Milyen szoftverdokumentációt várjon el egy NIS2 kötelezett szervezet a beszállítóitól on-premise szoftver esetén?

VFP3 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/16

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.11.17	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

Megjelent a Magyar Kereskedelmi és Iparkamara (MKIK) NIS2-Tudástárában. A témához kapcsolódó alkalmakat a workshopok oldala sorolja fel. A dokumentum oldala a Tudástárban.

1. VEZETŐI ÖSSZEFOGLALÓ

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) hatálya alá tartozó, NIS2-kötelezett szervezet a saját infrastruktúráján futó szoftver szállítójától a biztonsági osztályhoz igazodó, a 7/2024. (VI. 24.) MK rendeletből (a továbbiakban: Rendelet) levezethető dokumentációt köteles megkövetelni. A dokumentáció a Szervezet saját megfelelésének bizonyítéka, hiányát dokumentálni, kockázatát kezelni kell.

- A dokumentáció a Szervezet kötelezettsége, egyedi fejlesztésnél a szállító készíti el, dobozos terméknél a Szervezet szerzi be és egészíti ki. A Rendelet minden biztonsági osztályban előírja az adminisztrátori, üzemeltetői és felhasználói dokumentáció kidolgozását vagy beszerzését, a beszerzési szerződésben pedig a dokumentációs követelmények rögzítését. Ami a szerződésből kimarad, azt később csak jóindulatból vagy felár ellenében kapja meg a Szervezet, nem kikényszeríthető.

- Alap biztonsági osztályban a működtetéshez szükséges dokumentáció az elvárás. Felhasználói és adminisztrátori kézikönyv, a biztonsági funkciók és a biztonságos konfiguráció leírása, telepítési útmutató, az ismert sérülékenységek és a támogatási feltételek közlése, valamint a rendszerelem-leltárhoz szükséges platform- és összetevőadatok. A használt portok és protokollok jegyzékét a Szervezet már ebben a biztonságiosztályban maga elkészíti.
- Jelentős biztonsági osztályban a tervezési és fejlesztési bizonyítékok is kellenek. A rendszerterv és az interfészek, a funkciók, portok és protokollok jegyzéke, a fejlesztői változáskövetés, a biztonsági tesztelés és a dokumentált fejlesztési folyamat bemutatása. Egyedi fejlesztésnél ezek a szerződésben teljes körűen előírhatók, dobozos terméknél a Szervezet a ténylegesen gyakorolható körben kéri és értékeli őket, a teljesíthetetlen részt pedig eltérésként rögzíti.
- Magas biztonsági osztályban a biztonsági architektúra és a szállítási konfiguráció is a csomag része. A fejlesztő tervezési specifikációt és biztonsági architektúrát készít, a szoftvert meghatározott biztonsági konfigurációval szállítja, a saját szoftverfejlesztőit képzi a biztonsági funkciók helyes használatáról, és a Szervezet a külső fejlesztők háttérellenőrzését is megköveteli.
- Dobozos szoftvernél a gyártói dokumentációt értékelni, a hiányt saját dokumentációval pótolni kell. A gyártói kézikönyv, a biztonsági útmutató és a kiadási jegyzék átvehető, a Szervezetre szabott konfigurációt és az üzemeltetési rendet a Szervezet maga dokumentálja. A kiberrezilienciáról szóló rendelet[1] 2027 végétől a gyártótól felhasználói tájékoztatást és szoftverösszetevő-jegyzék készítését várja el, a jegyzék átadásáról azonban a gyártó dönt, a korábban forgalomba hozott termékekre pedig csak lényeges módosítás esetén vonatkozik. Ha a dobozos alaptermékre partneri testreszabás épül, a testreszabott rétegre az egyedi fejlesztés szabályai irányadók.
- A hiányzó dokumentáció nem jelent automatikus meg nem felelést, a dokumentálatlan hiány viszont igen. A beszerzési kísérleteket dokumentálni, a hiányt saját dokumentációval és a Szervezet által meghatározott kiegészítő intézkedéssel pótolni kell, a nem együttműködő szállító kockázatát pedig kiegészítő intézkedésekkel és kilépési tervvel kell csökkenteni. A csere akkor indokolt, ha a kockázat így sem tartható elfogadható szinten.

[1] Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről (kiberrezilienciáról szóló rendelet, CRA). A rendelet a gyártóra, és nem a terméket használó Szervezetre állapít meg kötelezettséget, a kereskedelmi forgalomban beszerzett on-premise szoftver pedig jellemzően digitális elemeket tartalmazó terméknek minősül. A követelmények főszabály szerint 2027. december 11-től alkalmazandók, az ezt megelőzően forgalomba hozott termékekre csak akkor, ha azokat ezt követően lényegesen módosítják (69. cikk (2) bekezdés, 71. cikk (2) bekezdés). A gyártó bejelentési kötelezettsége az aktívan kihasznált sérülékenységekről és a súlyos incidensekről (14. cikk) ettől eltérően már 2026. szeptember 11-től alkalmazandó, a korábban forgalomba hozott termékekre is (69. cikk (3) bekezdés). A szoftverösszetevő-jegyzéket a gyártó köteles elkészíteni (I. melléklet II. rész 1. pont), a felhasználó számára való hozzáférhetővé tételéről azonban maga dönt (II. melléklet 9. pont). A gyártói megfelelés a Szervezet saját, a Kiberbiztonsági tv. és a Rendelet szerinti megfelelését nem helyettesíti.

- A nem értelmezhető dokumentációt indokolással kell kizárni, nem hallgatással. Ha a szoftvernek nincs adminisztrátori felülete, a követelmény az érintett részre nem vonatkozik, ezt azonban a rendszerbiztonsági tervben és az eltérések nyilvántartásában rögzíteni kell.
- A rendszerbiztonsági terv keretet ad a pótlásnak, de nem helyettesíti a szállítói dokumentációt. A saját architektúra, a szoftverkörnyezet, az interfészek, a portok és az alapkonfiguráció az NKI rendszerbiztonsági terv sablonja szerint a Szervezet saját dokumentumaként rögzíthető, a fejlesztői bizonyítékok hiánya viszont csak eltérésként.
- A meglévő szoftvereknél a dokumentációs kikötéseket a következő megújításkor kell bevezetni. Addig a hiányt fel kell mérni, dokumentáltan be kell kérni, és határidős intézkedési tervben kell kezelni.

2. A VIZSGÁLANDÓ KÉRDÉS

A vizsgálandó kérdés az, hogy a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban „Kiberbiztonsági tv.”) és a 7/2024. (VI. 24.) MK rendelet (a továbbiakban „Rendelet”) hatálya alá tartozó szervezet (a továbbiakban „Szervezet”) milyen szoftverdokumentációt köteles és milyen dokumentációt célszerű megkövetelnie a szállítóitól, ha a szoftver a saját infrastruktúráján fut. Az iránymutatás a kérdést az Alap, a Jelentős és a Magas biztonsági osztály szerint külön vizsgálja, mert a Rendelet 2. melléklete a dokumentációval összefüggő követelmények jelentős részét csak a magasabb osztályokhoz rendeli.

Az iránymutatás két szállítási modellt különböztet meg. Az egyedi fejlesztésű szoftvernél a Szervezet a megrendelő, ezért a dokumentáció tartalmát a szerződésben maga határozhatja meg. A dobozos, kereskedelmi forgalomban kapható szoftvernél a gyártói dokumentáció adott, a Szervezet értékelni és kiegészíteni tudja. A gyakorlatban gyakori a vegyes modell is, amelyben dobozos alaptermékre partneri testreszabás és harmadik féltől származó kiegészítő modul épül, ennek kezelését a 3.3. pont tárgyalja. A szoftverként nyújtott szolgáltatás (SaaS) dokumentációját **az MKIK 2026/17. számú iránymutatása** tárgyalja, a nyílt forráskódú szoftverét pedig **a 2026/15. számú iránymutatás**, ezért ezekre a jelen anyag csak utal.

3. GYAKORLATI JAVASLATOK

3.1 A dokumentációs követelményjegyzék összeállítása

A dokumentációs elvárást a beszerzés előkészítésekor, a biztonsági osztály ismeretében javasoljuk összeállítani, és a szerződés mellékleteként rögzíteni. A jegyzéket az alábbi lépésekben célszerű elkészíteni. Meglévő szoftvernél és szerződésnél a 3.6. pont szerint kell eljárni.

a) **Az érintett EIR és biztonsági osztály azonosítása.** Meg kell állapítani, melyik elektronikus információs rendszer (a továbbiakban: EIR) része lesz a szoftver, és az milyen biztonsági osztályba tartozik. A biztonsági osztályt a szerződésben közölni kell, mert a Rendelet 16.7.4. pontja (A) ezt kötelező szerződéses tartalomként írja elő.

Dobozos terméknél a közlés a partnerrel vagy a viszonteladóval kötött szerződésben vagy a megrendelésben történik. Ha a beszerzés kizárólag a gyártó egységes licencfeltételeivel jön létre, ezt a tényt és a gyártói dokumentáció értékelését a rendszerbiztonsági tervben kell rögzíteni. A szállítóval a biztonsági osztályt kell közölni, a kockázatelemzést nem.

b) **Az elkészítendő dokumentumtípusok meghatározása.** Meg kell határozni az adott szoftverhez elkészítendő dokumentumokat, igazodva a szoftver biztonsági osztályához.

c) **Formátum, nyelv, határidő és frissítés rögzítése.** A szerződésben meg kell határozni a dokumentáció nyelvét, formátumát, a mérföldkőhöz kötött határidejét és a változtatásokat követő frissítés rendjét.

d) **Átvételi vizsgálat.** A dokumentációt az átadás-átvétel részeként, az elektronikus információs rendszer biztonságáért felelős személy (a továbbiakban: IBF) bevonásával ellenőrizni kell.

e) **Nyilvántartásba vétel és védelem.** Az átvett dokumentumokat a rendszerelem-leltárhoz és a rendszerbiztonsági tervhez kell kapcsolni, a biztonsági dokumentumokat a jogosulatlan hozzáféréstől védeni kell. A gyártói és szállítói dokumentumokról jegyzéket kell vezetni (cím, internetes elérhetőség, termékverzió, letöltés dátuma, archivált példány helye, felelős), amely a rendszerbiztonsági terv kapcsolódó dokumentumokról szóló részében, az NKI-sablonban a 7.2. pontban vagy annak mellékletében vezethető. Online gyártói dokumentációnál a releváns változatot a licencfeltételek tiszteletben tartásával (6.47.1. pont, A) archiválni, főverzió-váltáskor felülvizsgálni, és a 16.15.4. pont (A) szerint a meghatározott szerepkörökhöz eljuttatni kell, mert az auditkor a hivatkozott weboldal tartalma már eltérhet.

A követelményjegyzék a **2026/10. számú iránymutatásban** leírt közreműködői szerződés dokumentációs fejezetének részletezése.

3.2 Egyedi fejlesztésű szoftver dokumentációja biztonsági osztályonként

Egyedi fejlesztésnél a jegyzéknek álláspontunk szerint legalább a Rendelet által nevesített, illetve a Szervezet saját kötelezettségeinek teljesítéséhez szükséges dokumentumokat tartalmaznia kell. A magasabb osztály az alacsonyabb osztály elvárásait is magában foglalja. Alap osztályban az alábbi dokumentumokat javasoljuk megkövetelni.

a) **Felhasználói kézikönyv.** A felhasználók számára elérhető biztonsági funkciókat, a biztonságos használat módját és a felhasználó felelősségét tartalmazza.

b) **Adminisztrátori és üzemeltetői kézikönyv.** A biztonságos konfigurációt, telepítést és üzemeltetést, a biztonsági funkciók karbantartását és a privilegizált funkciókkal kapcsolatos ismert sérülékenységeket írja le. Ez az alapkonfiguráció és a konfigurációs beállítások kiindulópontja.

c) **A biztonsági funkciók leírása.** A fejlesztő leírja a védelmi intézkedések funkcionális tulajdonságait. Ebből derül ki, hogy a szoftver mely követelményeket teljesíti saját funkcióval, és melyeket kell a Szervezetnek más eszközzel pótolnia.

d) **Telepítési és konfigurációs leírás.** A biztonságos alapbeállítások jegyzékével, az alapkonfiguráció és a konfigurációs beállítások dokumentálásához.

e) **Rendszerelem- és összetevőjegyzék.** A rendszerelem-leltár csak a szoftver összetevőinek, verzióinak és függőségeinek ismeretében lehet pontos. Alap osztályban ajánlott a fő platform- és futtatókörnyezeti összetevők (adatbázismotor, futtatókörnyezet, beágyazott harmadik féltől származó komponens) és verzióik közlése, ha ez hiányzik, a Szervezet saját felméréssel pótolja. Géppel olvasható szoftverösszetevő-jegyzéket (SBOM) a Rendelet egyik osztályban sem ír elő, a magasabb biztonsági osztályokban ajánlásként javasoljuk. Az összetevőadatok helye az NKI rendszerbiztonsági terv sablonjában az 5.2.3. szoftverkörnyezet-táblázat.

f) **Támogatási és életciklus-tájékoztató.** A támogatás nélkül maradt rendszerelemek kezelése és a hibajavítás megkívánja a támogatott verziók, a támogatás lejárata, a frissítési rend és a sérülékenység-bejelentési csatorna ismeretét. Az életciklus-adatokat az NKI-sablon 5.2.3. táblázatában célszerű vezetni, a táblázatot a támogatás vége és a támogatási forrás (gyártó, partner, alternatív támogatás) oszlopával kiegészítve.

g) **Interfészleírás.** Az információcsere a rendszerkapcsolatok dokumentálására vonatkozó követelmény az interfészek dokumentálását kívánja meg. A Szervezet ténylegesen használt kapcsolatainak jegyzéke az NKI-sablon 5.2.4. táblázata, amelyet az 5.7.2. pont (A) szerinti biztonsági követelményekkel és felelősségi körrel kell kiegészíteni.

h) **Portok, protokollok és szolgáltatások saját jegyzéke.** Ezt a jegyzéket Alap biztonsági osztályban a Szervezet saját felmérése alapján maga készíti el (6.26. pont, A), az NKI-sablonban az 5.3. pontban. Jelentős osztálytól ezen felül a Jelentős osztályra vonatkozó felsorolás b) pontja szerint a fejlesztőtől vagy a szállítótól is meg kell követelni, a kettő összevetésének helye ugyancsak az 5.3. táblázat.

i) **Licenc- és felhasználási feltételek.** A szoftverhasználat korlátozásainak dokumentálása tipikusan a szerződés része szokott lenni.

A fenti lista az elvárt tartalmat rögzíti, ezeknek természetesen nem kell önálló dokumentumoknak lenniük, a b), c) és d) pont szerinti tartalom az üzemeltetési dokumentáció része lehet.

Jelentős biztonsági osztályban a fentieken túl az alábbi dokumentumok szükségesek.

a) **Tervezési és megvalósítási dokumentáció.** A biztonsági szempontból releváns külső interfészek, a magas és az alacsony szintű rendszerterv, valamint a forráskód vagy a Szervezet által meghatározott részletes információk. Ha a Szervezet a forráskód helyett letéti megállapodást vagy megbízott harmadik fél vizsgálati jogát fogadja el, az az 1. melléklet 3.1.2. pontja szerinti eltérés, amelyet kockázatelemzéssel indokolni és a 3.1.3. pont szerint jóváhagyatni kell.

b) **Funkciók, portok, protokollok és szolgáltatások jegyzéke.** A 16.13. pont (J) ezt szerződéses rendelkezésként írja elő, a legszűkebb funkcionalitás és a határvédelem beállításának alapja. Dobozos terméknél a jegyzéket a telepítést végző partner a tényleges konfigurációra készíti el.

c) **Fejlesztői változáskezelési dokumentáció.** A 16.58. pont (J) alapján kiadási jegyzék a biztonsági hatások megjelölésével, változásnapló és a biztonsági hibák nyilvántartása.

d) **Biztonsági tesztelési dokumentáció.** A 16.66. pont (J) szerint biztonságértékelési terv, tesztjelentés és a hibajavítás igazolása.

e) **A fejlesztési folyamat leírása és kritikussági elemzés.** A 16.76. pont (J) dokumentált, a biztonsági követelményeket kiemelten kezelő fejlesztési folyamatot, a 16.79. pont (J) a döntési pontokon végzett kritikussági elemzést követel meg. A szállítói adatfolyam-leírás a Szervezet 6.52. pont (J) szerinti saját nyilvántartásának bemenete. Az NKI rendszerbiztonsági terv sablon 2025-ös változata a 16.76. és a 16.79. pontot nem tartalmazza, ezeket a sablon 8. fejezetének bevezetője szerint kiegészítő pontként, a sablon űrlapjával kell felvenni. A Szervezet saját kritikussági elemzését (15.21. pont, J) a sablon 8.7.8. pontja tartalmazza.

Magas osztályban az alábbi dokumentumokkal egészül ki a jegyzék.

a) **Tervezési specifikáció és biztonsági architektúra.** A 16.87. pont (M) alapján a Szervezet architektúrájához illeszkedő, a biztonsági funkciók megosztását és együttműködését bemutató dokumentum. A Szervezet saját architektúraleírása az NKI-sablon 5.1. és 5.2. pontjában a fejlesztői specifikációt nem helyettesíti, de az illeszkedés vizsgálatának alapja.

b) **Szállítási konfiguráció leírása.** A 16.11. pont (M) megköveteli, hogy a szállítás a meghatározott biztonsági konfigurációval történjen, és újratelepítéskor vagy frissítéskor az alapkonfigurációt alkalmazzák (16.11.1. és 16.11.2. pont). A konfiguráció leírását és ellenőrzési módját javasoljuk kikötni.

c) **Fejlesztői képzés és átvilágítási nyilatkozat.** A 16.86. pont (M) azt követeli meg, hogy a fejlesztő a saját szoftverfejlesztőit képezze a megvalósított biztonsági funkciók helyes használatáról, a 16.98. pont (M) a külső fejlesztők háttérellenőrzését írja elő. Ha a Szervezet a saját felhasználóinak vagy üzemeltetőinek képzését igényli, azt külön szerződéses elemként kell kikötni. A különálló tesztkörnyezet kialakítása a Szervezet kötelezettsége (6.16. pont, M), ezért beszerzéskor a teszt- és fejlesztői licenc feltételeit is tisztázni kell. Az NKI rendszerbiztonsági terv sablon a 16.86., 16.87. és 16.98. pontot nem tartalmazza, ezeket kiegészítő pontként kell felvenni.

Egyik biztonsági osztályban sem kötelező, de a kockázatelemzés (15.5. pont, A) alapján indokolt lehet a fenyegetésmodellezés (16.68. pont, O), a behatolásvizsgálat (16.71. pont, O), az automatizált sérülékenységelemzés (16.82. pont, O), a kiadás archiválása (16.85. pont, O) és a sértetlenség ellenőrzését lehetővé tevő aláírás (16.59. pont, O).

3.3 Dobozos szoftver esetén követendő eljárás

Dobozos szoftvernél a Szervezet a gyártói dokumentációt nem tudja alakítani, a Rendelet követelményei azonban rá is vonatkoznak. A 16.15. pont (A) a dokumentáció kidolgozását és beszerzését egyaránt elfogadja, ezért az eljárás a következő. A Jelentős és Magas biztonsági osztály fejlesztői követelményeit dobozos terméknél a Szervezet a ténylegesen gyakorolható körben teljesíti, vagyis dokumentáltan kéri, értékeli a gyártó nyilvános bizonyítékait, a teljesíthetetlen részt pedig kockázatelemzéssel alátámasztott eltérésként rögzíti. Az elfogadható bizonyítékokat a pont végén lévő táblázat foglalja össze.

a) **A gyártói dokumentáció átvétele és értékelése.** A beszerzés előtt meg kell vizsgálni a gyártó kézikönyveit, biztonsági útmutatóját, kiadási jegyzékét, az életciklus-közleményt és a sérülékenységi tájékoztató csatornáját, és az elvárt tartalmi minimummal össze kell

vetni, megállapítva, hogy esetlegesen mi hiányzik. Kisebb gyártónál a hiányzó adatok beszerzésének egyszerű eszköze a 2. melléklet szerinti gyártói kérdőív. Az átvett dokumentumokat a 3.1. e) pont szerinti jegyzékbe kell felvenni.

b) **A hiányzó elemek saját dokumentálása.** A Szervezetre szabott konfigurációt, az üzemeltetési eljárásrendet, a jogosultsági modellt és a rendszerkapcsolatokat a Szervezet maga dokumentálja, az NKI rendszerbiztonsági terv sablonja szerint. Az architektúra, a határok és a topológia az 5.1. és az 5.2.1. pontba, a szoftverösszetevők gyártóval, verzióval és patchszinttel az 5.2.3. pontba, a rendszerkapcsolatok az 5.2.4. pontba, a portok, protokollok és szolgáltatások az 5.3. pontba, az alapkonfiguráció és a biztonsági beállítások a 8.4. fejezet megfelelő pontjaiba, a jogosultsági modell a 3.8. pontba és a 8.1. fejezetbe kerül. A gyártói kézikönyv ezekhez forrás, a kitöltött fejezet a Szervezet saját bizonyítéka.

c) **A viszonteladó és az integrátor bevonása.** A bevezetési dokumentáció, a testre szabott konfiguráció és a tesztjegyzőkönyv a bevezetést végző közreműködőtől követelhető meg. A globális gyártók (például Microsoft, SAP) a középvállalattal jellemzően nem állnak közvetlen szerződésben, a licencet és a támogatást viszonteladó vagy implementációs partner nyújtja, ilyenkor a közreműködő a partner. A partnerszerződésben előírható a gyártói dokumentáció és a biztonsági közlemények továbbítása, a telepített konfigurációra vonatkozó funkció-, port- és protokolljegyzék elkészítése (16.13. pont, J), a bevezetési és tesztdokumentáció, valamint a Kiberbiztonsági tv. 11. § (9) bekezdése szerinti tájékoztatás. A gyártóval szemben a Szervezet a nyilvános dokumentációra és a jogszabályi gyártói kötelezettségekre támaszkodik. A külső szereplőket (gyártó, viszonteladó, implementációs partner, üzemeltető vagy támogató közreműködő) feladatukkal, szerződésük azonosítójával és kapcsolattartójukkal az NKI-sablon 3.7. táblázatába is fel kell venni, a partner távoli hozzáférését és annak portjait pedig az 5.2.4. és az 5.3. táblázatban jelölni kell.

d) **Gyártói tanúsítványok felhasználása.** A gyártó tanúsítványa vagy független értékelése a 16.8. pont (A) szerinti leírást és a magasabb osztályok tesztelési bizonyítékát részben kiválthatja, ha a Szervezet dokumentálja, mire terjed ki. A Kiberbiztonsági tv. 6. § (8) bekezdése csak az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer szerinti tanúsítványra (például EUCC) vonatkozik. Az ISO/IEC 27001, a SOC 2 vagy a Common Criteria (CC) tanúsítvány e körön kívül esik, bizonyítékként azonban mérlegelhető, ha a Szervezet dokumentálja, hogy a vizsgált termékre és verzióra kiterjed.

e) **A gyártói kötelezettségek figyelembevétele.** A kiberrezilienciáról szóló (EU) 2024/2847 rendelet (CRA) 2027. december 11-től a gyártótól felhasználói tájékoztatást, szoftverösszetevő-jegyzéket, sérülékenységkezelést és a támogatási időszak közlését követeli meg.[2] A szoftverösszetevő-jegyzéket a gyártónak el kell készítenie, a felhasználónak való átadásáról azonban maga dönt (II. melléklet 9. pont). A követelmények a 2027. december 11. után forgalomba hozott termékekre vonatkoznak, a korábbiakra csak lényeges módosítás esetén, ezért a meglévő szoftverállományon nem

[2] Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete, 13. cikk (18) bekezdés, 31. cikk, I. melléklet II. rész 1. pont, II. és VII. melléklet. A sérülékenységjelentési kötelezettség 2026. szeptember 11-től alkalmazandó.

segítenek. A már 2026. szeptember 11-től alkalmazandó bejelentési kötelezettség keretében a gyártó az aktívan kihasznált sérülékenységről az érintett felhasználókat is tájékoztatja, ezért a Szervezet tartsa naprakészen a gyártói kapcsolattartási adatait. Az adatokat a Szervezet a gyártótól kérheti, saját megfelelését azonban továbbra is a Rendelet szerint igazolja.

A vegyes (hibrid) modell. A gyakorlatban gyakori, hogy dobozos alaptermékre partneri testreszabás és harmadik féltől származó kiegészítő modul épül (például ügyviteli rendszer magyar lokalizációval és kiegészítőkkel). A követelményjegyzéket ilyenkor rétegenként kell alkalmazni. Az alaptermékre a jelen pontot, a Szervezet megrendelésére készült testreszabásra és bővítményre a 3.2. pontot teljes körűen, a forráskód átadását is beleértve, a kiegészítő modulra pedig gyártójának szerződéses helyzetétől függően az egyiket vagy a másikat. A legtöbb biztonsági kockázat a testreszabott rétegben jelenik meg, ott a Szervezet megrendelő, ezért a dokumentációs elvárást a bevezetési szerződésben kell rögzíteni.

Jogszabályváltozás miatti kötelező frissítések. A könyvelő-, bér- és adóprogramok jogszabályváltozás miatt kötelező, határidős frissítéseit a Szervezet előre jóváhagyott szabványos változásként kezelheti. Ennek elemei a telepítés előtti mentés, a visszaállítási terv, a kiadási jegyzék biztonsági szempontú átnézése és a telepítés utáni ellenőrzés, így a biztonsági hatásvizsgálat (6.15. pont, A) és a frissítések telepítés előtti tesztelése (18.2.2. pont, A) arányosan teljesül. Különálló tesztkörnyezetet a 6.16. pont csak Magas osztályban követel meg.

Fejlesztői követelmények dobozos szoftvernél. A Jelentős és Magas biztonsági osztály fejlesztői követelményeinél dobozos szoftver esetén az alábbi bizonyítékokat tartjuk elfogadhatónak. Az utolsó oszlop az NKI rendszerbiztonsági terv sablonjának azt a pontját jelöli, ahol a teljesítést vagy az eltérést rögzíteni kell.

Pont	Követelmény	Osztály	Dobozos szoftvernél elfogadható bizonyíték	NKI RBT-sablon
16.9.	Tervezési és megvalósítási információk	J	Gyártói architektúra-leírás és nyilvános protokollspecifikáció, saját integrációs architektúra. A forráskódra eltérés, kivéve, ha hozzáférhető (például egyes ügyviteli rendszerek alkalmazásrétege).	8.8.3. (J, M); 5.1., 5.2.
16.13.	Funkciók, portok, protokollok és szolgáltatások	J	Gyártói portdokumentáció, valamint a partner vagy a Szervezet portfelmérése a telepített példányon.	8.8.4. (J), 8.8.5. (M); 5.3.
16.58.	Fejlesztői változáskövetés	J	Kiadási jegyzék és biztonsági közlemények. A 16.58.3. pont dobozos terméknél úgy értelmezhető, hogy a Szervezet a frissítés telepítését hagyja jóvá a saját változáskezelésében.	8.8.7. (J), 8.8.8. (M); 8.4.6.
16.66.	Fejlesztői biztonsági tesztelés	J	A gyártó dokumentált biztonságos fejlesztési életciklusa vagy ISO/IEC 27001 tanúsítványa, EUCC vagy Common Criteria tanúsítvány, valamint saját sérülékenységvizsgálat a telepített példányon.	8.8.8. (J), 8.8.9. (M); 8.7.1.
16.76.	Fejlesztési folyamat, szabványok és eszközök	J	A gyártó nyilvános biztonságos fejlesztési életciklus leírása vagy az ISO/IEC 27001 tanúsítvány hatálya.	A sablon nem tartalmazza, kiegészítendő.

Pont	Követelmény	Osztály	Dobozos szoftvernél elfogadható bizonyíték	NKI RBT-sablon
16.79.	Kritikussági elemzés	J	A Szervezet saját kritikussági elemzése (15.21. pont), a fejlesztői elemzésre eltérés.	Kiegészítendő; saját elemzés 8.7.8.
16.87.	Fejlesztői biztonsági architektúra és tervezés	M	Gyártói architektúra-leírás és a Szervezet saját integrációs architektúrája.	Kiegészítendő; 5.1., 5.2.
16.11.	Rendszer, rendszerelem és szolgáltatás konfigurációk	M	Gyártói hardening-útmutató és a Szervezet saját alapkonfigurációja.	8.8.4. (M); 8.4.2.
16.86., 16.98.	Fejlesztői képzés, külső fejlesztők háttérellenőrzése	M	Gyártói nyilatkozat vagy ISO/IEC 27001 tanúsítvány, ha egyik sincs, eltérés.	Kiegészítendő.
6.52., 6.16.	Információ helye, különálló tesztkörnyezet	J, M	Szervezeti teendő, a szállítói adat csak bemenet.	8.4.21. (J), 8.4.30. (M); 8.4.11. (M)

3.4 Hiányzó dokumentáció és nem együttműködő szállító

Ha valamely dokumentáció nem áll rendelkezésre, az alábbi, a Rendelet 16.15.3. pontjából (A) és az MKIK-28. számú jogi állásfoglalásából következő sorrendet javasoljuk.

a) **A beszerzési kísérlet dokumentálása.** Írásban rögzíteni kell, mikor, kitől, milyen dokumentumot kért a Szervezet, és milyen választ kapott. Ez a Rendelet követelménye és az audit során a jóhiszemű eljárás bizonyítéka. A kísérlet és az eredménye az NKI rendszerbiztonsági terv sablon dokumentációs pontjában (Alap 8.8.3., Jelentős 8.8.5., Magas 8.8.6. pont) részben megvalósított státusszal, a részletek mezőben rögzíthető. A kitöltött vagy megtagadott gyártói kérdőív (2. melléklet) e kísérlet bizonyítéka.

b) **Szerződéses eszközök.** Ha a szerződés a dokumentációt kifejezetten előírja, a hiány szerződésszegés, amelyre kötbér, díjvisszatartás vagy felmondás alkalmazható. Dobozos termék egységes licencfeltételeinél és régebbi szerződéseknél ilyen kikötés rendszerint nincs, ilyenkor a megújítás és a partnerszerződés a tárgyalási pont. Az IBF a Kiberbiztonsági tv. 11. § (9) bekezdése alapján a közreműködőtől tájékoztatást kérhet, és megismerheti az ott meglévő, a biztonság tárgyában keletkezett dokumentumokat. A jogosultság új dokumentum elkészítésére nem kötelez, és közvetlen hatósági szankció sem kapcsolódik hozzá (MKIK-28), ezért a kötelezettséget a szerződésben kell rögzíteni.

c) **A hiány pótlása saját erőből vagy harmadik féllel.** Az üzemeltetési dokumentáció a rendszer felmérésével, az összetevőjegyzék automatizált eszközzel, a tesztelési bizonyíték független sérülékenységvizsgálattal pótolható, a költség a mulasztó szállítóra hárítható, ha a szerződés erre lehetőséget ad.

d) **Pótló intézkedés, eltérés és helyettesítés.** Az adminisztrátori, üzemeltetői és felhasználói dokumentáció hiányát a 16.15.3. pont (A) szerinti eljárás, vagyis a kísérletek dokumentálása és a Szervezet által meghatározott intézkedések végrehajtása maga kezeli, ehhez külön helyettesítési eljárás nem szükséges. Az intézkedés lehet fokozott felügyelet, hálózati elkülönítés, szigorúbb változáskezelés és kilépési terv. A pótló intézkedéseket és határidejüket az NKI-sablon intézkedési tervről szóló pontja (Alap 8.3.5., Jelentős 8.3.6., Magas 8.3.8. pont) tartalmazza. Az 1. melléklet 3. és 4. pontja szerinti eltérést vagy helyettesítést akkor kell alkalmazni, ha a Szervezet egy fejlesztői követelményt (például a

16.9., 16.66. vagy 16.76. pontot) nem tud teljesíteni. Az NKI-sablon külön eltérés-nyilvántartást nem tartalmaz, ezért az eltéréseket és a helyettesítő intézkedéseket az 1/2025. (I. 31.) SZTFH rendelet 4. melléklete szerinti nyilvántartásban kell vezetni, a vezetővel jóváhagyatni, és a rendszerbiztonsági terv érintett pontjában erre hivatkozni.

e) **A szállító értékelése és cseréje.** A nem együttműködő szállítót az ellátási lánc kockázatelemzésében (15.5. pont, A, Jelentős osztálytól a 19.16. pont, J) magasabb kockázatúként kell értékelni. A kockázatot kiegészítő intézkedésekkel (hálózati elkülönítés, fokozott felügyelet, szigorúbb változáskezelés) és kilépési tervvel kell csökkenteni, a szállítót pedig a következő megújításkor újra kell értékelni. A csere akkor indokolt, ha a kockázat így sem tartható elfogadható szinten, alaprendszernél (ügyviteli, bérszámfejtő rendszer) ez jellemzően több évre ütemezett projekt. A használat folytatásáról a vezető a Kiberbiztonsági tv. 6. § (3) bekezdés 12. pontja alapján dokumentáltan dönt.

3.5 A nem értelmezhető dokumentációs követelmény kezelése

A parancssori eszköznek nincs felhasználói felülete, a beágyazott könyvtárnak nincs adminisztrátori felülete. Ilyenkor a dokumentum nem hiányzik, hanem tárgytalan, ezt azonban bizonyíthatóan meg kell állapítani. Az IBF a szállító nyilatkozata illetve saját vizsgálata alapján rögzíti, mely dokumentum mely része tárgytalan, az indokolást a rendszerbiztonsági tervben és az eltérések nyilvántartásában rögzíti (az NKI-sablonban az érintett követelménynél a nem alkalmazható jelölővel és a részletek mezőben megadott indokkal, megjelölve, hogy a követelmény mely része tárgytalan és mely része nem), mert az auditor a „nem alkalmazható” minősítést csak az átadott nyilvántartás alapján adhatja meg.[3] A nem relevancia rendszerint részleges, az adminisztrátori felület nélküli szoftvernek is van konfigurációja, frissítési rendje és naplója, ezekre a dokumentáció továbbra is szükséges. Új funkció bevezetésekor ezt a vizsgálatot a biztonsági hatásvizsgálat keretében újra el kell végezni.

3.6 Meglévő szoftverek és szerződések kezelése

A fenti eljárás az új beszerzésre épül. A meglévő szoftvereknél a régebbi szerződések dokumentációs kikötést rendszerint nem tartalmaznak, és a nem támogatott verziók is gyakoriak. Ilyenkor az alábbi sorrendet javasoljuk.

a) **Felmérés.** A Szervezet felméri a meglévő dokumentációt és a hiányokat, az eredményt pedig az NKI-sablon szerinti rendszerbiztonsági tervben rögzíti.

b) **Dokumentált bekérés.** A hiányzó dokumentumokat a 16.15.3. pont (A) szerint dokumentáltan bekéri, kisebb gyártónál a 2. melléklet szerinti kérdőívvel.

c) **Kikötés a megújításkor.** A dokumentációs kikötéseket a következő támogatási vagy licencmegújításkor, illetve a partnerszerződés módosításakor vezeti be.

d) **Nem támogatott verziók.** A támogatás nélküli rendszerelemet a 16.99. pont (A) szerint lecseréli vagy alternatív támogatást biztosít hozzá, a támogatás végét és forrását pedig a terv 5.2.3. táblázatában vezeti.

[3] 1/2025. (I. 31.) SZTFH rendelet 5. § (1) bekezdés c) pont, 4. melléklet és 5. melléklet 2.2.2. pont.

e) **Intézkedési terv.** A fennmaradó hiányokat határidős intézkedési tervben kezeli (5.10. pont, A), amely az NKI-sablonban az Alap osztályban a 8.3.5., Jelentős osztályban a 8.3.6., Magas osztályban a 8.3.8. pont.

A fokozatos bevezetésre a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet nem hivatkozhat, ezért az átmenetet eltérésként és intézkedési tervvel kell kezelni. Dokumentáltan elkülönített régi rendszerelemnél az 1. melléklet 3.2.7. pontja szerinti egyedi eltérés is alkalmazható, ha az elkülönített elemek közötti határvédelemről gondoskodtak (lásd az iránymutatás 4.8. pontját).

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

Az iránymutatás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) vagy e) pontja alá tartozik, felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el, és rendszereit biztonsági osztályba sorolta. A szoftverszállító közreműködő, ha az EIR létrehozásában, karbantartásában vagy javításában vesz részt, a dobozos szoftver gyártója pedig akkor, ha a Szervezettel támogatási szerződésben áll. A globális gyártók a középvállalattal jellemzően nem állnak közvetlen szerződésben, ilyenkor a licencet és a támogatást nyújtó viszonteladó vagy implementációs partner a közreműködő. A fogalmat az **MKIK-30. számú jogi állásfoglalás**, a szerződés tartalmát a **2026/10. számú iránymutatás** tárgyalja. A dokumentáció egyszerre védelmi intézkedés és audit bizonyíték, az auditor a dokumentumvizsgálat során a rendszerbiztonsági tervet, a rendszertervet, a rendszerleltárt és a szoftverleltárt is vizsgálja, és bizonyíték hiányában a követelményt nem teljesítettnek minősíti.[4]

4.2 A dokumentáció helye a törvény rendszerében

A Kiberbiztonsági tv. a szoftverdokumentációt nem nevesíti, a közreműködő igénybevételének szerződéses feltételeit azonban a vezető kötelezettségévé teszi.

> *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. tv. 6. § (5) bekezdés d) pont]*

A vezető felelőssége a közreműködő igénybevétele esetén is fennmarad a 6. § (6) bekezdése szerint. A dokumentáció megszerzésének törvényi eszköze az IBF tájékoztatáskérési joga.

> *(9) Az elektronikus információs rendszer biztonságáért felelős személy jogosult a szervezet elektronikus információbiztonsági kötelezettségeinek,*

[4] 1/2025. (I. 31.) SZTFH rendelet 4. § (2) bekezdés, 5. melléklet 1.1.4. és 1.2.1. pont.

> *feladatainak teljesítésében közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében jogosult megismerni a követelményeknek való megfelelőség alátámasztásához szükséges közreműködői tevékenységgel kapcsolatos adatot, valamint az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. [2024. évi LXIX. tv. 11. § (9) bekezdés]*

A jogosultság közvetlenül a törvényből fakad, de csak a közreműködővel szemben él, a meglévő adatok és dokumentumok megismerésére terjed ki, új dokumentum elkészítésére nem kötelez, és szankció sem kapcsolódik hozzá. A szerződéses rögzítés ezért szükséges, mert a dokumentáció elkészítésének kötelezettsége, formátuma, határideje és a jogkövetkezmény csak a szerződésből következik. A dokumentáció a használatbavételi döntés feltétele is, mert a Rendelet 1. mellékletének 1.1.6. pontja szerint a vezető a rendszerbiztonsági terv, az értékelési jelentés és a kockázatelemzés alapján dönt, ezek pedig a szállítói dokumentáció nélkül nem készíthetők el megalapozottan.

4.3 A Rendelet dokumentációs követelményei

A Rendelet 2. melléklete a szoftverdokumentációt minden osztályban megköveteli, a hiány esetére pedig kifejezett szabályt ad.

> *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. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.15.1. pont, A]*
> *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 [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.15.3. pont, A]*

A felhasználói dokumentáció tartalmát a 16.15.2. pont (A) határozza meg. A beszerzési szerződés kötelező tartalmát a 16.7. pont (A) írja elő, amely a dokumentációs követelményeket és a dokumentumok védelmét külön nevesíti.

> *16.7.5. A biztonsággal kapcsolatos dokumentációs követelményeket.*
> *16.7.6. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7.5. és 16.7.6. pont, A]*

A biztonsági funkciók leírását a 16.8. pont (A) minden osztályban a fejlesztőtől követeli meg. Jelentős és Magas osztályban a tervezési és megvalósítási információk is a fejlesztő kötelezettségévé válnak.

> *16.9. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője biztosítson tervezési és megvalósítási információkat a védelmi intézkedésekhez. Ezek az információk tartalmazzák a biztonsági szempontból releváns külső rendszerinterfészeket, a magas szintű rendszertervet, az alacsony szintű rendszertervet, a forráskódot vagy a hardversémákat, valamint a szervezet által meghatározott részletes tervezési és megvalósítási információkat. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.9. pont, J]*

A követelményben a forráskód a hardversémával vagylagos, nem a letéttel. Ha a Szervezet a forráskód helyett letéti megállapodást vagy harmadik fél vizsgálati jogát fogadja el, az az 1. melléklet 3.1.2. pontja szerinti eltérés, amelyet kockázatelemzéssel indokolni és a 3.1.3. pont szerint jóváhagyatni kell. Ugyancsak Jelentős és Magas biztonsági osztályban kötelező a funkciók, portok és protokollok jegyzéke (16.13. pont), a fejlesztői változáskövetés (16.58. pont), a fejlesztői biztonsági tesztelés (16.66. pont), a dokumentált fejlesztési folyamat (16.76. pont) és a kritikussági elemzés (16.79. pont). Magas biztonsági osztályban a biztonsági architektúra (16.87. pont), a szállítási konfiguráció (16.11. pont), a fejlesztő saját szoftverfejlesztőinek képzése (16.86. pont) és a külső fejlesztők háttérellenőrzése (16.98. pont) egészíti ki a jegyzéket. A támogatás megszűnésének felismeréséhez a 16.99. pont (A) miatt az életciklus-tájékoztató Alap osztályban is a jegyzék része. Dobozos terméknél a fejlesztői követelmények a 3.3. pont szerinti, ténylegesen gyakorolható körben teljesíthetők, a teljesíthetetlen részre eltérés kell. Az NKI rendszerbiztonsági terv sablonjának 2025-ös változata a 16.76., 16.79., 16.86., 16.87. és 16.98. pontot nem tartalmazza, a sablon hiánya azonban a kötelezettség alól nem mentesít. A 16.86. pont a fejlesztő saját fejlesztőinek képzéséről szól, nem a Szervezet képzéséről.

> *16.86. A szervezet kötelezi a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztőknek a megvalósított biztonsági funkciók, szabályozások és mechanizmusok helyes használatáról és működéséről. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.86. pont, M]*

A fokozatosság a biztonsági osztályba sorolás logikájából következik. Alap biztonsági osztályban a Szervezet a kész termék viselkedését dokumentálja, Jelentős biztonsági osztályban a termék keletkezéséről is bizonyítékot kap, Magas biztonsági osztályban a tervezés szintjéig és a fejlesztő személyi megbízhatóságáig jut el. Az alacsonyabb osztályban nem kötelező követelményeket a Szervezet önként is előírhatja, a kötelezőktől csak az 1. melléklet 3. és 4. pontja szerinti dokumentált eltéréssel térhet el.

4.4 Dobozos szoftver és a gyártói kötelezettségek

A Rendelet a dokumentáció kidolgozását és beszerzését egyenrangúan kezeli, ezért a gyártói dokumentáció akkor fogadható el, ha a 16.15. pont tartalmi elemeit lefedi. A gyártói kézikönyv a szoftver általános viselkedését írja le, a Szervezet konkrét telepítését és kapcsolatait nem, ezért

ezeket mindig a Szervezet dokumentálja. A szoftverhasználat jogszerűségét a Rendelet a dokumentációra is kiterjeszti.

> *6.47.1. Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak. [7/2024. (VI. 24.) MK rendelet 2. melléklet 6.47.1. pont, A]*

A CRA a gyártót a felhasználó Szervezettől függetlenül kötelezi felhasználói tájékoztatásra és szoftverösszetevő-jegyzék készítésére, a jegyzék átadásáról azonban a gyártó dönt, és a követelmények csak a 2027. december 11. után forgalomba hozott termékekre vonatkoznak, a gyártói megfelelés azonban nem helyettesíti a Szervezet saját megfelelését. A Kiberbiztonsági tv. 6. § (8) bekezdése az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított terméket nevesíti.

> *(8) Az (1)–(5) bekezdés szerinti egyes követelményeknek való megfelelés igazolására – ha rendelkezésre áll – európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat alkalmazható. [2024. évi LXIX. tv. 6. § (8) bekezdés]*

Az ISO/IEC 27001, a SOC 2 vagy a Common Criteria (CC) szerinti tanúsítvány e körön kívül esik, bizonyítékként azonban szabadon mérlegelhető, ha a Szervezet dokumentálja, hogy a vizsgált termékre és verzióra kiterjed.

4.5 Hiányzó dokumentáció és helyettesítő védelmi intézkedés

A 16.15.3. pont szerint a beszerzési kísérletek dokumentálása és a Szervezet által meghatározott intézkedések végrehajtása együtt teljesíti a követelményt. Az intézkedés a gyakorlatban a saját dokumentáció és a Szervezet által meghatározott kiegészítő intézkedés, ehhez a helyettesítő intézkedés négy feltételének igazolása nem szükséges. Az 1. melléklet 3. és 4. pontja szerinti eltérés vagy helyettesítés a fejlesztői követelmények nem teljesíthető részénél alkalmazandó.

> *4.1. A helyettesítő védelmi intézkedés alkalmazása olyan eljárás, amelyet a szervezet az adott biztonsági osztályhoz tartozó védelmi intézkedés helyett kíván alkalmazni, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például jogszabályoknak vagy szervezeti szintű szabályozóknak) való megfelelést. [7/2024. (VI. 24.) MK rendelet 1. melléklet 4.1. pont]*

A helyettesítés négy együttes feltételét a 4.2. pont tartalmazza, ezek a katalógusbeli intézkedés alkalmazhatatlansága, a kockázat elfogadása, az egyenértékűség bemutatása és a vezetői jóváhagyás. Az eltérést a 3.1.2. és 3.1.3. pont szerint dokumentálni és jóváhagyatni kell, az SZTFH auditrendelete pedig az eltérések és helyettesítő intézkedések nyilvántartását az auditálási terv részeként kéri be. Az NKI rendszerbiztonsági terv sablonja ilyen nyilvántartást

nem tartalmaz, ezért azt külön kell vezetni, és a terv érintett pontjában rá kell hivatkozni. A nem együttműködő szállítóval szemben az MKIK-28. számú állásfoglalás szerint a hatóság a közreműködőt főszabály szerint közvetlenül nem bírságolhatja, a jogkövetkezményeket a Szervezet viseli, aki a szállítóval szemben polgári jogi úton léphet fel, ezért a dokumentáció hiányát a szerződésben kötbérrel, díjvisszatartással és felmondási joggal kell ellensúlyozni.

4.6 A nem értelmezhető követelmény

> *3.2.4.2. A védelmi intézkedések az elektronikus információs rendszer csak azon komponenseire vonatkoznak, amelyek az intézkedés által megcélzott biztonsági képességet biztosítják vagy támogatják, és az intézkedés által csökkenteni kívánt lehetséges kockázatok forrásai. [7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.4.2. pont]*

Ha a szoftvernek nincs adminisztrátori felülete, a dokumentáció felületre vonatkozó része tárgytalan, a biztonságos konfigurációra, telepítésre és az ismert sérülékenységekre vonatkozó része azonban nem. A megállapítás az 1. melléklet 3.2.4.2. pontja szerinti egyedi eltérés, amelyet a 3.1.3. pont szerint a vezető vagy a kockázatok felvállalására jogosult személy hagy jóvá, és amelyet az eltérések nyilvántartásába is át kell vezetni. A hiányzó és a nem releváns dokumentáció közötti különbség a dokumentált indokolásban áll, a hallgatás mindkettőt hiányként jeleníti meg. Az NKI rendszerbiztonsági terv sablonjában a nem alkalmazható jelölő a követelmény teljes kizárását jelenti, a részleges tárgytalanságot ezért a részletek mezőben kell leírni, a jelölő pedig önmagában az eltérések nyilvántartását nem pótolja.

4.7 Az 1. § (1) bekezdés a), b), c) és f) pontja szerinti szervezetek

A Kiberbiztonsági tv. 1. § (1) bekezdés a), b), c) és f) pontja szerinti szervezetekre a 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Korm.rendelet) is vonatkozik. A Kiberbiztonsági tv. 13. §-a az 1. § (1) bekezdés a) és c) pontja szerinti alapvető szervezetre, valamint a b) pont szerinti és egyben a 2. és 3. melléklet szerinti szervezetre vonatkozik, ezek a fejlesztési szerződésben rögzítik a hatóság által jóváhagyott osztályba sorolás követelményeit. A többi a), b) és c) pont szerinti szervezetre a 14. § vonatkozik. A Korm. rendelet a szerződés tartalmát és a hatósági jóváhagyás feltételét egészíti ki.

> *(4) A szervezet rögzíti a fejlesztésre irányuló szerződésben a nemzeti kiberbiztonsági hatóság által jóváhagyott osztályba soroláshoz kapcsolódó követelményeket és a fejlesztés során intézkedik azok megvalósulása iránt a fejlesztést végző szervezet felé. [2024. évi LXIX. tv. 13. § (4) bekezdés]*
> *(2) Az (1) bekezdés szerinti szervezet intézkedik a védelmi követelmények megvalósulása iránt a fejlesztést végző szervezet felé. [2024. évi LXIX. tv. 14. § (2) bekezdés]*
> *13. § (1) A szervezet az elektronikus információs rendszer fejlesztésére, továbbfejlesztésére (a továbbiakban együtt: fejlesztés) irányuló szerződésekben köteles meghatározni a fejlesztő részére a sérülékenységvizsgálat során feltárásra kerülő sérülékenységek*

> *javítására vonatkozó feltételeket. [418/2024. (XII. 23.) Korm. rendelet 13. § (1) bekezdés]*
> *(2) A kérelemnek tartalmaznia kell a biztonsági osztályba sorolás eredményeként kapott, elvárt védelmi intézkedések megvalósításáról készült valamennyi dokumentációt. [418/2024. (XII. 23.) Korm. rendelet 14. § (2) bekezdés]*

A 13. § hatálya alá tartozó Szervezet számára a szállítói dokumentáció ezért a használatbavétel hatósági jóváhagyásának feltétele is.

4.8 A rendszerbiztonsági terv és a szállítói dokumentáció viszonya

A rendszerbiztonsági terv a Szervezet saját dokumentuma, amelyet a vezető vagy az elektronikus információs rendszer biztonságáért felelős személy hagy jóvá.

> *A szervezet a biztonsági követelményeket a rendszerbiztonsági tervben dokumentálja, amelyet a szervezet vezetője vagy az elektronikus információs rendszer biztonságáért felelős szerepkört betöltő személy hagy jóvá. [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.3. pont]*

A terv a szállítói dokumentáció hiányát nem helyettesíti, hanem keretet ad a pótlásnak. Rögzíti, mely dokumentum áll rendelkezésre, mit dokumentált a Szervezet maga, mely követelmény tárgytalan, és melyik hiány milyen intézkedéssel, milyen határidőre kezelt. A kitöltéshez az NBSZ Nemzeti Kibervédelmi Intézet által a Rendelet alapján közzétett, biztonsági osztályonként külön rendszerbiztonsági terv sablont javasoljuk. A sablon ténylegesen pótolja a gyártótól be nem szerezhető dokumentáció egy részét, így a saját architektúrát és határokat (5.1. és 5.2.1. pont), a szoftverkörnyezetet és a verziókat (5.2.3. pont), az interfészjegyzéket (5.2.4. pont), a portok, protokollok és szolgáltatások jegyzékét (5.3. pont), az alapkonfigurációt és a beállításokat (8.4. fejezet), a sérülékenységkezelést (8.7. fejezet) és az intézkedési tervet. Nem pótolja viszont a gyártó biztonsági funkcióinak leírását (16.8. pont), a gyártói sérülékenységi ismeretet (16.15.1.3. pont), az alacsony szintű tervet és a forráskódot (16.9. pont), valamint a fejlesztési folyamatra és a fejlesztőkre vonatkozó bizonyítékokat, ezeknél a terv csak a hiány és az eltérés dokumentálásának helye. A sablon információbiztonsági felelős szerepköre a Kiberbiztonsági tv. 11. §-a szerinti, az elektronikus információs rendszer biztonságáért felelős személynek felel meg.

A portok, protokollok és szolgáltatások jegyzéke a sablon szerint már Alap biztonsági osztályban is a terv része, ami a Szervezet saját kötelezettségéből következik.

> *6.26.2. Meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat. [7/2024. (VI. 24.) MK rendelet 2. melléklet 6.26.2. pont, A]*

A tervet a tényleges megvalósítás és az eltérések alapján frissíteni kell, ezért főverzió-váltás vagy rendszerelem cseréje után a szoftverkörnyezet-táblázatot is aktualizálni kell.

> *Az intézkedések végrehajtása során a szervezet a rendszerbiztonsági tervet a védelmi intézkedések tényleges megvalósítása, valamint a tervtől*

> *való esetleges eltérések alapján frissíti; [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.4. pont]*

A meglévő szoftverállománynál (3.6. pont) a fokozatos bevezetés a d) és e) pont szerinti Szervezet számára nem áll rendelkezésre.

> *A Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet, valamint a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja szerinti és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezetnek minősülő szervezet tekintetében az 1. melléklet 3.2.6. pontjában foglalt rendelkezések nem alkalmazhatók. [7/2024. (VI. 24.) MK rendelet 3. §]*

Az átmenet eszköze ezért az intézkedési terv (5.10. pont, A), elszigetelt régi rendszerelemnél pedig az egyedi eltérés.

> *3.2.7. Az elektronikus információs rendszer dokumentáltan elkülönített, informatikai biztonsági szempontból önállóan értékelhető elemei tekintetében a védelmi intézkedések a szervezet által elfogadott kockázatmenedzsment eljárásrendben rögzített vizsgálatot követően, külön-külön egyedi eltérésekkel is alkalmazhatóak, ha az elkülönített elemek közötti határvédelemről gondoskodtak. A határvédelem megfelelőségét, valamint az egyedi eltérések okát és mértékét dokumentálni és meghatározott gyakorisággal felülvizsgálni szükséges. [7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.7. pont]*

5. GYAKORI KÉRDÉSEK

5.1 Kötelező-e szoftverdokumentációt megkövetelni a beszállítótól?

A dokumentáció a Szervezet kötelezettsége, egyedi fejlesztésnél a szállító készíti el, dobozos terméknél a Szervezet szerzi be és egészíti ki. A Rendelet minden biztonsági osztályban előírja az adminisztrátori, üzemeltetői és felhasználói dokumentáció kidolgozását vagy beszerzését, a beszerzési szerződésben pedig a dokumentációs követelmények rögzítését. (1. fejezet)

5.2 Milyen dokumentációt kell megkövetelni Alap biztonsági osztályban?

Alap biztonsági osztályban a működtetéshez szükséges dokumentáció az elvárás. Felhasználói és adminisztrátori kézikönyv, a biztonsági funkciók és a biztonságos konfiguráció leírása, telepítési útmutató, az ismert sérülékenységek és a támogatási feltételek közlése, valamint a rendszerelem-leltárhoz szükséges platform- és összetevőadatok. A használt portok és protokollok jegyzékét a Szervezet már ebben az osztályban maga elkészíti. (1. fejezet)

5.3 Miben több a Jelentős és a Magas osztály elvárása?

Jelentős biztonsági osztályban a tervezési és fejlesztési bizonyítékok is kellenek. A rendszerterv és az interfészek, a funkciók, portok és protokollok jegyzéke, a fejlesztői változáskövetés, a biztonsági tesztelés és a dokumentált fejlesztési folyamat bemutatása. Egyedi fejlesztésnél ezek a

szerződésben teljes körűen előírhatók, dobozos terméknél a Szervezet a ténylegesen gyakorolható körben kéri és értékeli őket, a teljesíthetetlen részt pedig eltérésként rögzíti. Magas osztályban a biztonsági architektúra és a szállítási konfiguráció is a csomag része. (1. fejezet)

5.4 Hogyan kell eljárni dobozos szoftver esetén?

Dobozos szoftvernél a gyártói dokumentációt értékelni, a hiányt saját dokumentációval pótolni kell. A gyártói kézikönyv, a biztonsági útmutató és a kiadási jegyzék átvehető, a Szervezetre szabott konfigurációt és az üzemeltetési rendet a Szervezet maga dokumentálja. A kiberrezilienciáról szóló rendelet 2027 végétől a gyártótól felhasználói tájékoztatást és szoftverösszetevő-jegyzék készítését várja el, a jegyzék átadásáról azonban a gyártó dönt, a korábban forgalomba hozott termékekre pedig csak lényeges módosítás esetén vonatkozik. Ha a dobozos alaptermékre partneri testreszabás épül, a testreszabott rétegre az egyedi fejlesztés szabályai irányadók. (1. fejezet)

5.5 Mi a teendő, ha a szállító nem ad dokumentációt?

A hiányzó dokumentáció nem jelent automatikus meg nem felelést, a dokumentálatlan hiány viszont igen. A beszerzési kísérleteket dokumentálni, a hiányt saját dokumentációval és a Szervezet által meghatározott kiegészítő intézkedéssel pótolni kell, a nem együttműködő szállító kockázatát pedig kiegészítő intézkedésekkel és kilépési tervvel kell csökkenteni. A csere akkor indokolt, ha a kockázat így sem tartható elfogadható szinten. (1. fejezet)

5.6 Mi a teendő, ha az adminisztrátori dokumentáció nem értelmezhető?

A nem értelmezhető dokumentációt indokolással kell kizárni, nem hallgatással. (1. fejezet) A nem relevancia rendszerint részleges, az adminisztrátori felület nélküli szoftvernek is van konfigurációja, frissítési rendje és naplója, ezekre a dokumentáció továbbra is szükséges. (3.5. pont)

5.7 Mi a teendő a már használt szoftvereknél?

A meglévő szoftvereknél a dokumentációs kikötéseket a következő megújításkor kell bevezetni. Addig a hiányt fel kell mérni, dokumentáltan be kell kérni, és határidős intézkedési tervben kell kezelni. (1. fejezet) A fokozatos bevezetésre a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet nem hivatkozhat, ezért az átmenetet eltérésként és intézkedési tervvel kell kezelni. (3.6. pont)

5.8 Kiválthatja-e a rendszerbiztonsági terv a hiányzó szállítói dokumentációt?

A rendszerbiztonsági terv keretet ad a pótlásnak, de nem helyettesíti a szállítói dokumentációt. A saját architektúra, a szoftverkörnyezet, az interfészek, a portok és az alapkonfiguráció az NKI rendszerbiztonsági terv sablonja szerint a Szervezet saját dokumentumaként rögzíthető, a fejlesztői bizonyítékok hiánya viszont csak eltérésként. (1. fejezet) A kitöltéshez az NBSZ Nemzeti Kibervédelmi Intézet által a Rendelet alapján közzétett, biztonsági osztályonként külön rendszerbiztonsági terv sablont javasoljuk. (4.8. pont)

6. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (kiberrezilienciáról szóló rendelet, CRA)
- 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
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- NBSZ Nemzeti Kibervédelmi Intézet, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, 16. Rendszer- és szolgáltatásbeszerzés
- NBSZ Nemzeti Kibervédelmi Intézet, A 7/2024. (VI. 24.) MK rendelet alapján aktualizált rendszerbiztonsági terv sablonok (Alap, Jelentős és Magas biztonsági osztály, V.1.0, 2025)
- ENISA, Technical implementation guidance on cybersecurity risk management measures (1.0 verzió, 2025. június)
- NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- BSI TR-03183, Cyber Resilience Requirements for Manufacturers and Products, Part 2 Software Bill of Materials (SBOM)
- MKIK-28 jogi állásfoglalás, Mit tehet egy NIS2 kötelezett cég, ha egy szerződött közreműködő megtagadja az együttműködést?
- MKIK-30 jogi állásfoglalás, A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása

7. KAPCSOLÓDÓ MKIK-ÁLLÁSFOGLALÁSOK ÉS IRÁNYMUTATÁSOK

- 2026/17, Milyen szoftverdokumentációra van szükség NIS2 kötelezett szervezetnél SaaS szolgáltatás igénybevétele esetén? (iránymutatás)
- MKIK-30, A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása
- MKIK-28, Mit tehet egy NIS2 kötelezett cég, ha egy szerződött közreműködő megtagadja az együttműködést?
- 2026/10, A közreműködővel kötött szerződés tartalma
- 2026/15, Nyílt forráskódú szoftverek használata NIS2-kötelezett szervezeteknél
- 2026/3, Mikor kell alkalmazni a tanúsított IKT-termékeket

MKIK Jogi állásfoglalások és MKIK Iránymutatások

8. AJÁNLOTT HIVATKOZÁS

Magyar Kereskedelmi és Iparkamara (2026). Milyen szoftverdokumentációt várjon el egy NIS2 kötelezett szervezet a beszállítóitól on-premise szoftver esetén? Iránymutatás, 2026/16. NIS2-Tudástár, https://nis2.mkik.hu/iranymutatasok/milyen-szoftverdokumentaciot-varjon-el-egy-nis2-kotelezett-szervezet-a-beszallitoitol-onpremise/

Közzétéve: 2026.11.17. További anyagok: https://nis2.mkik.hu/

1. MELLÉKLET

A szoftverdokumentációhoz kapcsolódó követelmények a 7/2024. (VI. 24.) MK rendelet 2. melléklete alapján

Az osztályjelölés azt a legalacsonyabb biztonsági osztályt mutatja, amelytől kezdve a követelmény kötelező. Az (A) jelölésű követelmény Alap, Jelentős és Magas biztonsági osztályban, a (J) jelölésű Jelentős és Magas biztonsági osztályban, az (M) jelölésű csak Magas biztonsági osztályban kötelező, az (O) jelölés pedig egyik osztályban sem kötelező, kiegészítő követelményt jelent. A táblázat a Rendelet 2025. január 2-től hatályos szövege alapján készült, és nem helyettesíti a teljes követelménykatalógus alkalmazását. Az utolsó oszlopban szereplő RBT-sablon hivatkozások az NKI rendszerbiztonsági terv sablonjainak 2025-ös, V.1.0 változatát követik (Alap, Jelentős és Magas biztonsági osztály sablon pontszáma), a számozás későbbi változatokban módosulhat.

Pont	Követelmény	Osztály	Iránymutatás pontja	Teljesítés a szoftverdokumentáció terén
Szervezeti keretek és tervezés				
1.5.	Elektronikus információs rendszerek nyilvántartása	A	3.1.	A szállítói dokumentáció az EIR nyilvántartási adatainak forrása.
5.7.	Információcsere	A	3.2.	Az interfészleírás a megállapodás melléklete. RBT-sablon 5.2.4.; 8.3.4. (A), 8.3.5. (J), 8.3.6. (M).
13.2.	Rendszerbiztonsági terv	A	3.3., 4.2., 4.8.	A szállítói dokumentumok a terv mellékletei. Kitöltéséhez az NKI osztályonkénti sablonja javasolt, a szállítói dokumentumok jegyzéke a sablon 7.2. pontjában vezethető.
15.5.	Kockázatelemzés, ellátási lánc	A	3.2., 3.4., 3.6.	A dokumentáció hiánya ellátási lánc kockázat.
15.21.	Rendszerelemek kritikusságának elemzése	J	3.2.	A Szervezet saját kritikussági elemzése, a 16.79. pont szerinti fejlesztői elemzés kiegészítése. RBT-sablon 8.7.8. (J, M).
Konfigurációkezelés				
6.2.	Alapkonfiguráció	A	3.2.	A telepítési és konfigurációs leírás az alapkonfiguráció kiindulópontja. RBT-sablon 8.4.2. (A, J, M).
6.15.	Biztonsági hatásvizsgálatok	A	3.5.	A nem relevancia felülvizsgálata változáskor. RBT-sablon 8.4.3. (A), 8.4.8. (J), 8.4.10. (M).
6.16.	Biztonsági hatásvizsgálatok, különálló tesztkörnyezetek	M	3.2.	Szervezeti kötelezettség, beszerzéskor a teszt- és fejlesztői licenc feltételeit tisztázni kell. RBT-sablon 8.4.11. (M).
6.23.	Konfigurációs beállítások	A	3.2.	A biztonságos beállítások jegyzéke. RBT-sablon 8.4.5. (A), 8.4.11. (J), 8.4.15. (M).

Pont	Követelmény	Osztály	Iránymutatás pontja	Teljesítés a szoftverdokumentáció terén
6.26.	Legszűkebb funkcionalitás	A	3.2., 4.8.	A portok, protokollok és szolgáltatások saját jegyzéke. RBT-sablon 5.3.; 8.4.6. (A), 8.4.12. (J), 8.4.18. (M).
6.36.	Rendszerelem leltár	A	3.2.	A szállítói összetevőadat a Szervezet saját leltárának egyik forrása. RBT-sablon 5.2.3.; 8.4.7. (A), 8.4.16. (J), 8.4.22. (M).
6.47.	A szoftverhasználat korlátozásai	A	3.2., 4.4.	A licenc- és felhasználási feltételek dokumentálása. RBT-sablon 8.4.8. (A), 8.4.19. (J), 8.4.28. (M).
6.52.	Információ helyének azonosítása és dokumentálása	J	3.2.	Szervezeti kötelezettség, a szállítói adatfolyam-leírás a nyilvántartás bemenete. RBT-sablon 4.1.; 8.4.21. (J), 8.4.30. (M).
6.53.	Aláírt rendszerelemek	O	3.2.	Aláírás vagy ellenőrző összeg.
Rendszer- és szolgáltatásbeszerzés				
16.7.	Beszerzések	A	3.1., 4.3.	A dokumentációs követelmények és a dokumentumok védelme szerződéses tartalom. RBT-sablon 8.8.1. (A, J, M).
16.8.	Alkalmazandó védelmi intézkedések funkcionális tulajdonságai	A	3.2., 4.3.	A biztonsági funkciók leírása. RBT-sablon 8.8.2. (A, J, M).
16.9.	Tervezési és megvalósítási információk	J	3.2., 4.3.	Rendszerterv, interfészek, forráskód, a letét eltérésként fogadható el. RBT-sablon 8.8.3. (J, M), saját architektúra 5.1., 5.2.
16.10.	Fejlesztési módszerek, technikák és gyakorlatok	O	3.2.	A fejlesztési életciklus bemutatása.
16.11.	Rendszer, rendszerelem és szolgáltatás konfigurációk	M	3.2., 4.3.	Szállítás a meghatározott biztonsági konfigurációval, újratelepítéskor az alapkonfiguráció alkalmazása. RBT-sablon 8.8.4. (M).
16.13.	Használatban lévő funkciók, portok, protokollok és szolgáltatások	J	3.2., 4.3.	A funkciók, portok és protokollok jegyzéke. RBT-sablon 5.3.; 8.8.4. (J), 8.8.5. (M).
16.15.	Az elektronikus információs rendszerre vonatkozó dokumentáció	A	3.2., 3.4., 4.3., 3.6.	Adminisztrátori, üzemeltetői és felhasználói dokumentáció, a hiány dokumentálása. RBT-sablon 8.8.3. (A), 8.8.5. (J), 8.8.6. (M).
16.58.	Fejlesztői változáskövetés	J	3.2., 4.3.	Kiadási jegyzék, változásnapló, hibanyilvántartás. RBT-sablon 8.8.7. (J), 8.8.8. (M).
16.59.	Szoftver és firmware sértetlenségének ellenőrzése	O	3.2.	Sértetlenség-ellenőrzés lehetővé tétele.
16.66.	Fejlesztői biztonsági tesztelés	J	3.2., 4.3.	Biztonságértékelési terv és tesztjelentés. RBT-sablon 8.8.8. (J), 8.8.9. (M).
16.68.	Fenyegetésmodellezés és sérülékenységelemzések	O	3.2.	Fenyegetésmodell eredménye.
16.71.	Behatolásvizsgálat	O	3.2.	A fejlesztői behatolásvizsgálat jelentése.

Pont	Követelmény	Osztály	Iránymutatás pontja	Teljesítés a szoftverdokumentáció terén
16.76.	Fejlesztési folyamat, szabványok és eszközök	J	3.2., 4.3.	A dokumentált fejlesztési folyamat leírása. Az NKI RBT-sablon nem tartalmazza, kiegészítő pontként kell felvenni.
16.79.	Kritikussági elemzés	J	3.2., 4.3.	A kritikussági elemzés eredménye. Az NKI RBT-sablon nem tartalmazza, kiegészítő pontként kell felvenni.
16.82.	Automatizált sérülékenységelemzés	O	3.2.	A sérülékenységelemzés jelentése.
16.85.	Rendszer vagy rendszerelem archiválása	O	3.2.	A kiadás archiválása a bizonyítékokkal.
16.86.	Szoftverfejlesztők oktatása	M	3.2., 4.3.	Nyilatkozat a fejlesztők biztonsági képzéséről. Az NKI RBT-sablon nem tartalmazza, kiegészítő pontként kell felvenni.
16.87.	Fejlesztői biztonsági architektúra és tervezés	M	3.2., 4.3.	Tervezési specifikáció és biztonsági architektúra. Az NKI RBT-sablon nem tartalmazza, kiegészítő pontként kell felvenni.
16.98.	Külső fejlesztők háttérellenőrzése	M	3.2., 4.3.	Nyilatkozat az átvilágítás megtörténtéről. Az NKI RBT-sablon nem tartalmazza, kiegészítő pontként kell felvenni.
16.99.	Támogatással nem rendelkező rendszerelemek	A	3.2., 4.3., 3.6.	Támogatási és életciklus-tájékoztató. RBT-sablon 5.2.3.; 8.8.4. (A), 8.8.9. (J), 8.8.10. (M).
Rendszer- és információsértetlenség, ellátási lánc				
18.2.	Hibajavítás	A	3.2.	A frissítések kiadási rendje és a sérülékenységi tájékoztató. RBT-sablon 8.10.2. (A, J, M).
19.7.	Alvállalkozók	A	3.1.	A továbbadott követelmények.
19.13.	Beszerzési stratégiák, eszközök és módszerek	A	3.1.	A követelményjegyzék a beszerzési módszer része.
19.16.	Beszállítók értékelése és felülvizsgálata	J	3.4.	A dokumentáció rendszeres felülvizsgálata. Alap osztályban a 15.5. pont szerinti kockázatelemzés az irányadó.
19.19.	Értesítési megállapodások	A	3.2.	Sérülékenység- és változásértesítés rendje.

2. MELLÉKLET

Gyártói kérdőív és nyilatkozatminta a szoftverdokumentáció beszerzéséhez

A kérdőív a 3.3. és a 3.4. pont szerinti beszerzési kísérlet eszköze, elsősorban kisebb gyártóknál és forgalmazóknál. A kitöltött vagy megtagadott kérdőív a 16.15.3. pont (A) szerinti beszerzési kísérlet bizonyítéka, a válaszokat a rendszerbiztonsági terv megjelölt pontjába kell átvezetni.

a) **Platformösszetevők.** Milyen adatbázismotor, futtatókörnyezet és beágyazott harmadik féltől származó komponens szükséges a termékhez, milyen verzióban? (RBT 5.2.3.)

b) **Támogatott változatok.** Mely termékévjáratok és platformverziók támogatottak, és mikor ér véget a támogatásuk? (RBT 5.2.3., 16.99. pont)

c) **Biztonsági frissítések.** Milyen csatornán és milyen gyakorisággal jelennek meg a biztonsági frissítések és közlemények, és jelöli-e a kiadási jegyzék a biztonsági hatást? (16.58. és 18.2. pont)

d) **Alapértelmezett fiókok.** Milyen alapértelmezett fiókokat és jelszavakat hoz létre a telepítés (például adatbázis-adminisztrátori fiók), és hogyan módosíthatók? (16.15.1.1. pont)

e) **Hálózati igény.** Mely portokat, protokollokat és hálózati megosztásokat használ a termék, és milyen minimális jogosultság szükséges a működéshez? (RBT 5.3., 16.13. pont)

f) **Jogosultsági modell.** Milyen szerepköröket és jogosultsági szinteket kezel a termék, és hogyan hitelesíti a felhasználókat? (16.8. pont, RBT 8.1.)

g) **Naplózás.** Milyen biztonsági eseményeket naplóz a termék, és hol tárolja a naplót? (16.8. pont)

h) **Mentés és visszaállítás.** Milyen mentési és visszaállítási eljárást javasol a gyártó? (16.15.1. pont)

i) **Adatok helye.** Hol tárolja a termék az adatokat, és továbbít-e adatot a gyártónak vagy harmadik félnek? (6.52. pont, RBT 4.1.)

j) **Sérülékenység-bejelentés.** Kihez lehet sérülékenységet bejelenteni, és hogyan tájékoztatja a gyártó a felhasználókat a kihasznált sérülékenységről? (16.15.1.3. pont)

k) **Fejlesztési folyamat és tanúsítványok.** Dokumentált biztonságos fejlesztési folyamat szerint készül-e a termék, rendelkezik-e a gyártó tanúsítvánnyal (például ISO/IEC 27001), és ha igen, mire terjed ki? (16.66. és 16.76. pont)

l) **Nyilatkozat a fejlesztőkről.** Nyilatkozik-e a gyártó a fejlesztők biztonsági képzéséről és átvilágításáról? (16.86. és 16.98. pont)

A kérdőívhez nyilatkozat csatolható, amelyben a gyártó vagy a forgalmazó képviselője aláírásával igazolja, hogy a válaszok a megjelölt termékverzióra vonatkoznak, és vállalja, hogy a lényeges változásokról a Szervezetet tájékoztatja.

Az MKIK a NIS2-kötelezett vállalkozásoknak díjmentes workshopokat és egyedi konzultációt kínál. Az időpontok és a jelentkezés a **workshopok oldalán** érhetők el, további állásfoglalások és iránymutatások pedig a **NIS2-Tudástárban**.