

NIS2 felkészülés - - égető határidő közeleg

2024 június 12.



legal
services &
consulting





Miért érdekel bennünket pont most a kiberbiztonság?

Alapvető követelmények a NIS2 EU irányelvet implementáló, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény alapján:

- Regisztrációs és bejelentkezési kötelezettség a Hatóság felé
- Az információs rendszerek biztonságáért felelős személy szerepének és felelősségi körének meghatározása
- Az elektronikus információs rendszerek felhasználóira vonatkozó szabályok meghatározása
- Információbiztonsági képzés

Mely ágazatok szervezeteire terjed ki a NIS2?

Kiemelten kockázatos ágazatok:

- **Energetika** (villamos energia, távfűtés és -hűtés, kőolaj, földgáz, hidrogén)
- **Közlekedés** (légi, vasúti, vízi és tömegközlekedés)
- **Egészségügy**
- **Ivóvíz, szennyvíz** (víziközmű)
- **Hírközlési szolgáltatás** (elektronikus hírközlési szolgáltató, adatkicserélő szolgáltatást nyújtó)
- **Digitális infrastruktúra** (felhőszolgáltató, adatközpont szolgáltató, legfelső szintű domainnév nyilvántartó, DNS szolgáltató, tartalomszolgáltató hálózat szolgáltató)
- **Kihelyezett infokommunikációs technológiai szolgáltatások**
- **Úralapú szolgáltatás** nyújtását támogató földi infrastruktúra

Kockázatos ágazatok:

- **Postai és futárszolgálatok**
- **Élelmiszer előállítása**, feldolgozása, forgalmazása
- **Hulladékgazdálkodás**
- **Vegyszerek előállítása és forgalmazása**
- **Gyártás**: orvostechikai és diagnosztikai eszközök; számítógépek; elektronikai, optikai termékek; villamos berendezések; máshova nem sorolt gépek és berendezések ; gépjárművek, pótkocsik és félpótkocsik; egyéb szállítóeszközök; cement-, mész-, gipszgyártás
- **Digitális szolgáltatók** (online piactér, keresőszolgáltató, közösségi média, domainnév regisztrációt végző szolgáltató)
- **Kutatás**

Mely ágazatok szervezeteire terjed ki a NIS2?

50 ≤ foglalkoztatotti
létszám VAGY

10 millió EUR <
éves nettó árbevétel
VAGY

NIS2 kötelezett
szervezet
beszállítója VAGY

- Elektronikus hírközlési szolgáltató,
- Bizalmi szolgáltató,
- DNS-szolgáltatást nyújtó szolgáltató,
- Legfelső szintű domainnév-nyilvántartó vagy
- Domainnév-regisztrációt végző szolgáltató

Uniós kiberbiztonsági irányelvek

Nemzeti hatóságok

MNB

DORA

irányelv a
pénzügyi ágazat
rezilienciájáról

SZTFH

NIS2

irányelv
a magas szintű
kiberbiztonságot
biztosító
intézkedésekről

NBSZ

közigazgatás,
kritikus
szervezetek

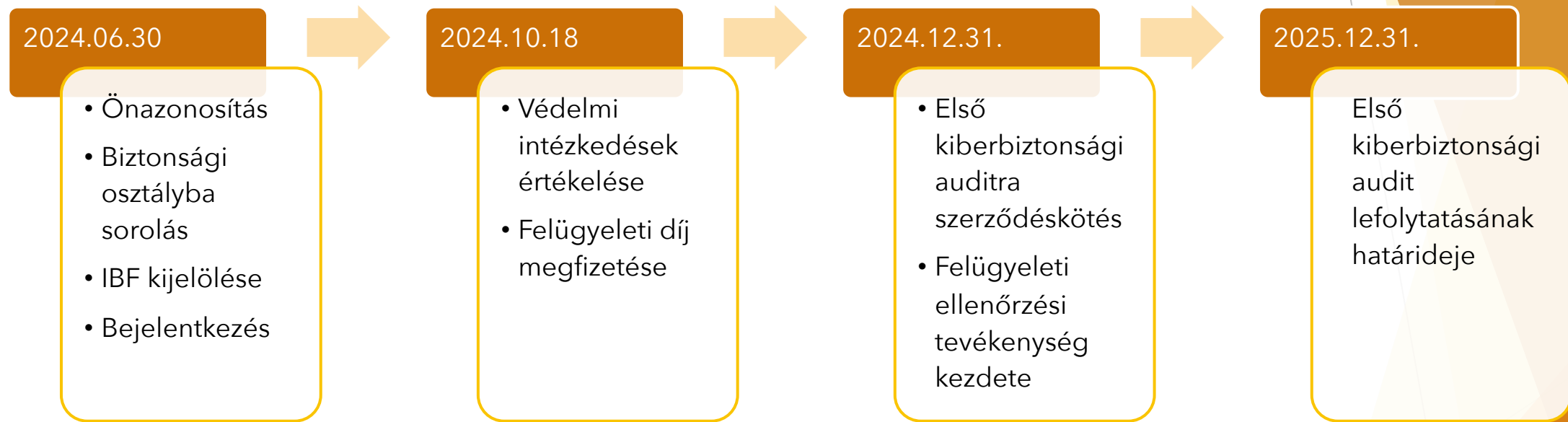
KNBSZ

honvédelmi
ágazat

CER

irányelv
a kritikus
szervezetek
rezilienciájáról

Fontosabb határidők és feladatok



Felkészülés a kiberbiztonsági auditra

Feladatok a felkészülés során 2024.06.30-ig

Elektronikus információs rendszerek biztonsági osztályba sorolása

- 1. "Alap", "jelentős" és "magas" biztonsági osztályok
- 2. A kezelt adatok bizalmasságának, sértetlenségének, rendelkezésre állásának követelményeinek súlyozása a funkciókra tekintettel
- 3. A biztonsági osztályba sorolást a kezelt adatok és az adott rendszer funkciói határozzák meg
- 4. A besorolást a szervezet vezetője hagyja jóvá és hatáselemzés alapján kell elvégezni
- 5. Egy szervezeten belül lehetségesek különböző besorolású rendszerek
- 6. Megfelelő osztályba sorolás jelentősége a későbbi költségek és potenciális bírság elkerülése miatt

Osztályba sorolás szempontjai*

Biztonsági osztály	Személyes adat	Szervezet üzleti vagy ügymenete	Lehetséges társadalmi-politikai hatás	Anyagi kár
Alap	Legfeljebb kis mennyiségű személyes adat	Csekély értékű, vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet	Szervezetten belül kezelhető	Éves költségvetés vagy nettó árbevétel $1\% \geq x$
Jelentős	Nagy mennyiségű adat, illetve különleges adat is sérülhet	Érzékeny folyamatokat kezelő rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet	Szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása, vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni	Éves költségvetés vagy nettó árbevétel $1\% \leq x \leq 10\%$
Magas	Különleges személyes adat nagy mennyiségben sérülhet/nemzeti adatvagyon helyreállíthatatlanul megsérülhet	Nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet	Nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet/ súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek	Éves költségvetés vagy nettó árbevétel $10\% \leq x$

* Még el nem fogadott jogszabálytervezet alapján.

Feladatok a felkészülés során 2024.10.18-ig*

Védelmi intézkedések értékelése - Gap analízis

Védelmi intézkedések témakörei	Követelmények (db)	Alap	Jelentős	Magas
Programmenedzsment	23	20	20	20
Hozzáférés-felügyelet	129	11	39	46
Tudatosság és képzés	14	5	6	6
Naplózás és elszámoltathatóság	52	10	16	25
Értékelés, engedélyezés és monitorozás	26	9	11	14
Konfigurációkezelés	53	9	21	30
Készenléti tervezés	49	5	22	35
Azonosítás és hitelesítés	50	12	21	23
Biztonsági események kezelése	38	7	13	18
Karbantartás	25	4	9	12
Adathordozók védelme	18	4	7	10
Fizikai és környezeti védelem	49	10	18	25
Tervezés	11	6	7	7
Személyi biztonság	13	9	9	10
Kockázatkezelés	22	7	12	12
Rendszer- és szolgáltatásbeszerzés	100	9	16	20
Rendszer- és kommunikációvédelem	132	10	25	30
Rendszer- és információsértetlenség	83	6	18	28
Ellátási lánc kockázatkezelése	27	11	12	14
Összesen	914	164	302	385

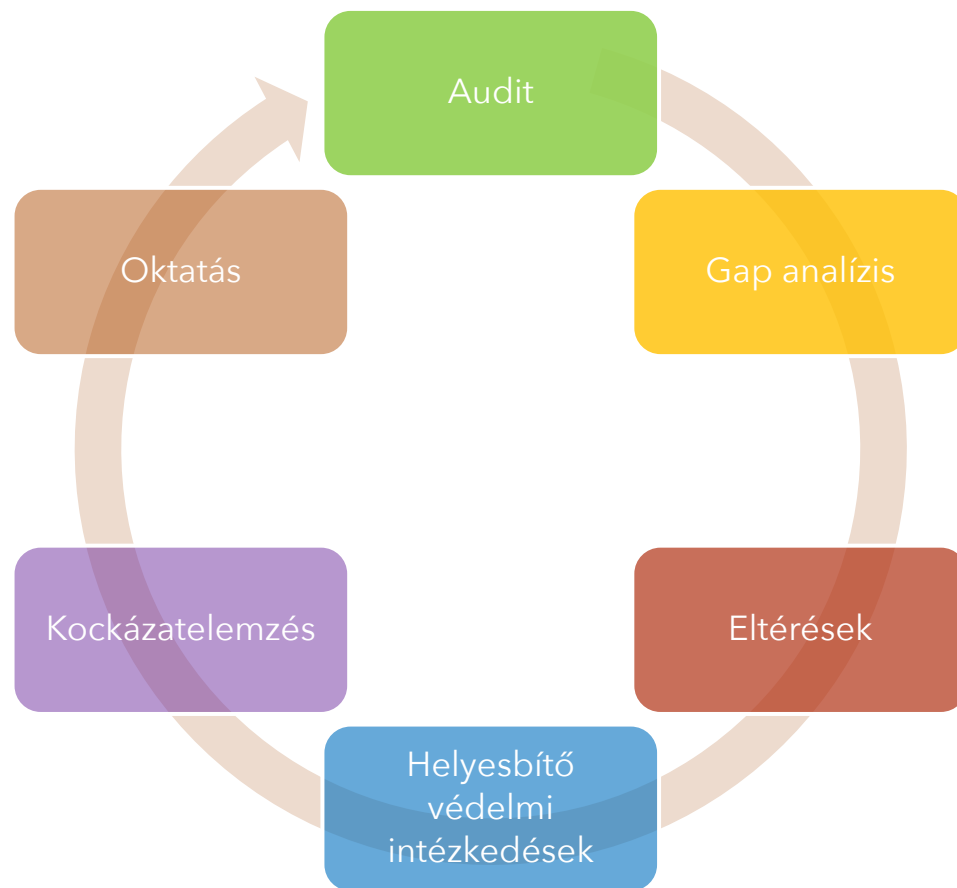
* Még el nem fogadott jogszabálytervezet alapján.

Feladatok az audit megkezdéséig

A Gap analízst követő lépések: a kockázatelemzés

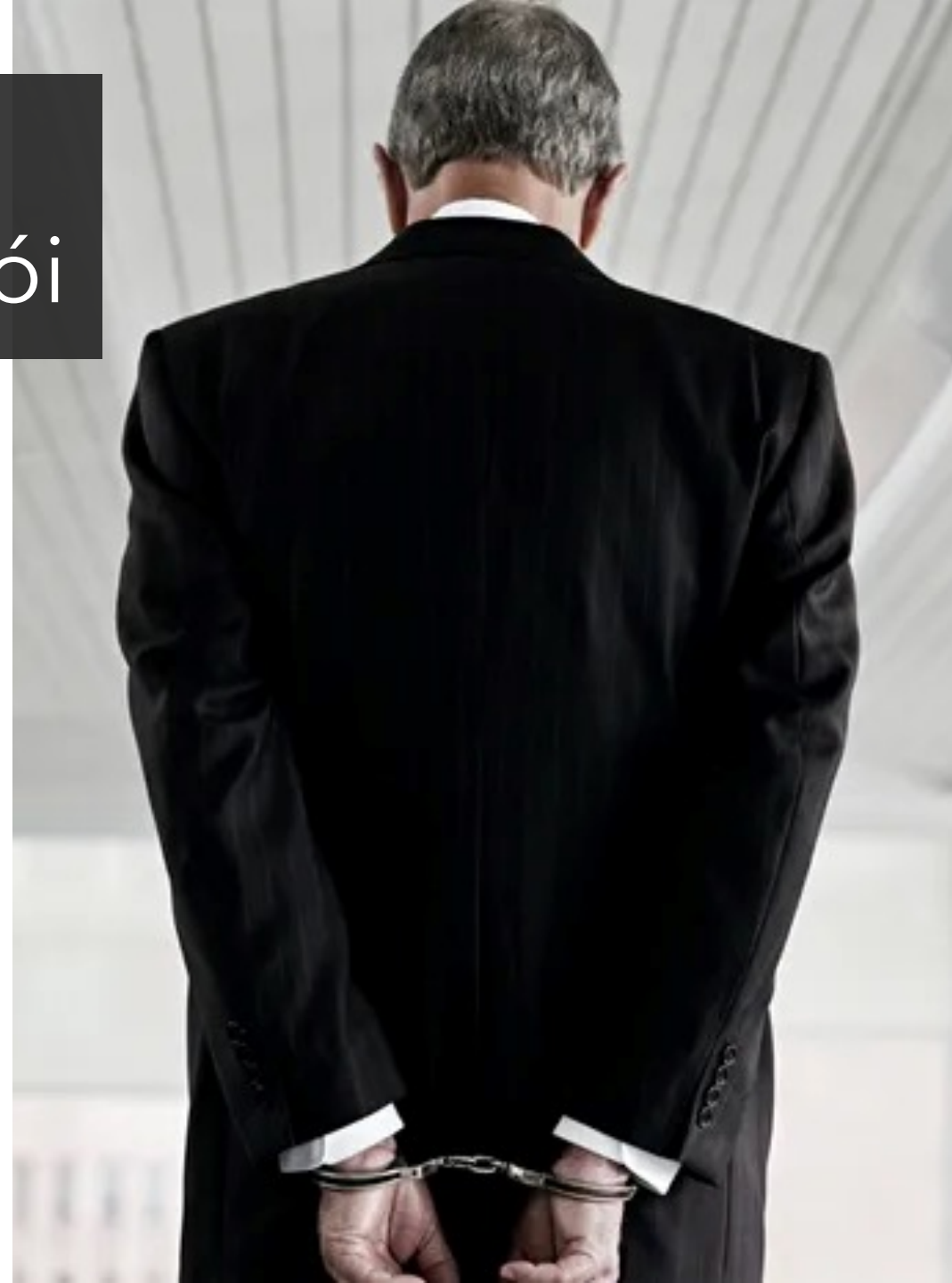


Készen állunk az auditra



NIS2 megfelelés elmulasztásának szankciói

- 10.000.000 EUR vagy a teljes éves világszintű forgalom 2%-ának megfelelő bírság kiemelten kockázatos ágazatok szervezetei esetén
- 7.000.000 EUR vagy a vállalkozás előző évi forgalma 1,4%-ának megfelelő bírság kockázatos ágazatok szervezetei esetén
- Súlyos esetben a társaság eltiltása az adott tevékenységtől, vezető tisztségviselő eltiltása





Tanácsadói támogatás

- ✓ A tanácsadóval belső – egyébként is leterhelt – erőforrások takaríthatók meg
- ✓ Speciális kiberbiztonsági és adatvédelmi szaktudás és tapasztalat biztosítása
- ✓ Jogszabályok értelmezése
- ✓ Pontos biztonsági osztályba sorolással későbbi költségek takaríthatók meg, illetve bírság kerülhető el
- ✓ Belső szabályzatok, folyamatleírások elkészítése
- ✓ Javaslat a költségesebb technológiai megoldások helyettesítésére folyamatszabályozással
- ✓ A szoftver alapú szimulációk, tesztek és a szabályozói feladatok koordinációja

Tapasztalt tanácsadók

Több évtizednyi tapasztalat a nemzetközi jogi, adatvédelmi és IT biztonsági compliance és tanácsadás területén



Energetika



Gyártás



IT,
telekommunikáció



Közigazgatás



Fuvarozás



Egészségügy



Pénzügyi
intézmények



Élelmiszeripar

Közel 100 sikeres projekt



Magyar Tudományos
Akadémia



GEDEON RICHTER LTD.



- ✓ Auditok (MNB, ISO27001)
- ✓ Adatvagyon felmérés, GDPR tanácsadás
- ✓ Üzleti hatáselemzés
- ✓ Kockázatelemzés
- ✓ Üzletmenet-folytonosság tervezés
- ✓ IBF/ CISO tevékenységek
- ✓ Biztonsági rendszerek tervezése
- ✓ Biztonsági szabályzatok készítése, biztonsági folyamatok kialakítása

Kapcsolat és további információ

nis2.rvdpartners.com

dr. Rövid Levente

+36 30 466 6018

nis2@rvdpartners.com