A kiberbiztonsági audit rendje

Hatósági nyilvántartás és felügyelet

Hatósági nyilvántartásban való szereplés

A Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg 2. és 3. melléklet szerinti szervezetnek minősülő szervezet, valamint az 1. § (1) bekezdés d) és e) pontja szerinti szervezet köteles a működése megkezdését követő vagy az e törvény hatálya alá kerülést követő 30 napon belül a Kiberbiztonsági tv.-ben meghatározott adatokat megküldeni az SZTFH részére a nyilvántartásba vétel érdekében.

- **Többségi állami tulajdonban lévő szervezet,**
  - **amely nem minősül a közigazgatási ágazathoz tartozó szervezetnek,**
  - **összes foglalkoztatotti létszáma eléri vagy meghaladja az 50 főt, vagy éves nettó árbevétele és mérlegfőösszege meghaladja a 10 millió eurónak megfelelő forintösszeget, és**
  - **kiemelten kockázatos vagy kockázatos ágazat szerinti tevékenység végzésére jogosult.**
- **Kiemelten kockázatos és kockázatos ágazat szerinti tevékenység végzésére jogosult szervezetek, amennyiben a Kkvtv. szerint a szervezet középvállalkozásnak minősül.**
- **Méretkorlát nélkül:**
  - **elektronikus hírközlési szolgáltató,**
  - **bizalmi szolgáltató,**
  - **DNS-szolgáltató,**
  - **legfelső szintű doménnév-nyilvántartó,**
  - **doménnév-regisztrációt végző szolgáltató**

Kiberbiztonsági felügyelet

A Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti – az a) pont hatálya alá nem tartozó – szervezetek elektronikus információs rendszerei esetében a kiberbiztonsági felügyeletet az SZTFH látja el.

- **Kiemelten kockázatos és kockázatos ágazat szerinti tevékenység végzésére jogosult szervezetek, amennyiben a Kkvtv. szerint a szervezet középvállalkozásnak minősül és nem minősül a közigazgatási ágazathoz tartozó szervezetnek.**
- **Méretkorlát nélkül:**
  - **elektronikus hírközlési szolgáltató,**
  - **bizalmi szolgáltató,**
  - **DNS-szolgáltató,**
  - **legfelső szintű doménnév-nyilvántartó,**
  - **doménnév-regisztrációt végző szolgáltató**

Hatósági nyilvántartás és felügyelet kötelezettségei

Hatósági nyilvántartásban szereplő szervezet kötelezettségei

- **Kiberbiztonsági felügyeleti díj fizetése**
  - **Nyilatkozattétel a vállalatcsoportba való tartozásról az SZTFH-422 elektronikus űrlapon benyújtott tárgyév január 31. napjáig.**

  Kivéve:
  - **költségvetési szervek**

- **Kiberbiztonsági auditra vonatkozó megállapodás megkötése a kiberbiztonsági audit lefolytatására jogosult auditorral**

- **Kiberbiztonsági audit lefolytatása**

  Kivéve:
  - **mikrovállalkozások**

- **Kiberbiztonsági incidensek jelentése a Nemzeti Kibervédelmi Intézet felé a Kiberbiztonsági tv. rendelkezései alapján**

- **Nyilvántartásban szereplő adatokkal kapcsolatos változások bejelentése az SZTFH – 421 elektronikus űrlapon**

- **Kockázatmenedzsment keretrendszer létrehozása és működtetése**

Kiberbiztonsági felügyeletben érintett szervezet kötelezettségei

Nyilvántartásban való szereplés kötelezettségei kiegészülve az alábbiakkal

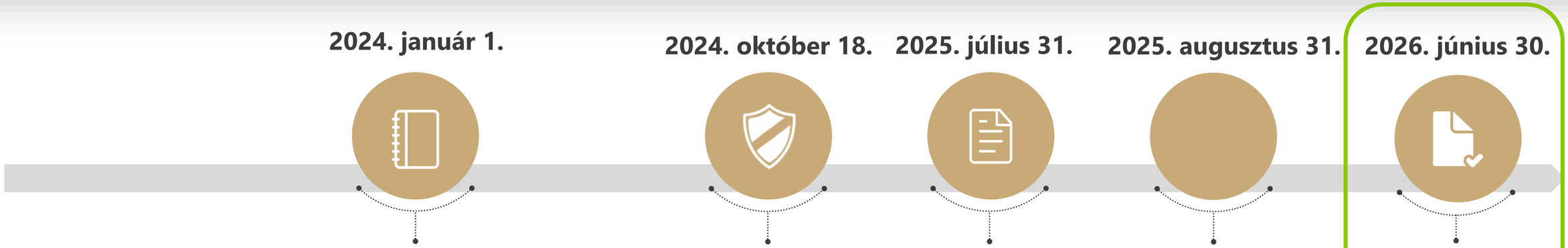
- **Együttműködés a 3/2025 SZTFH rendelet szerinti hatósági ellenőrzésekben, amelynek keretében az SZTFH jogosult:**
- **a biztonsági osztályba sorolást, a védelmi intézkedéseket és az ezekhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,**
- **a szervezet által meghatározott biztonsági osztályhoz tartozó védelmi intézkedéseken túl további biztonsági követelményeket meghatározni,**
- **a szervezet által elfogadott kiberbiztonsági kockázatkezelési értékeléséhez, valamint az információk bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatást kérni,**
- **a védelmi intézkedések és az ezekhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,**
- **rendszeres, eseti és célzott biztonsági ellenőrzéseket végezni,**
- **a felügyeleti feladatai ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz hozzáférni és ezeket bekérni, illetve a megküldött dokumentumok felülvizsgálatát elrendelni,**
- **az ellenőrzés során feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,**
- **a kiberbiztonsági audit eredményeképp előállított auditjelentést megalapozó bizonyítékokhoz hozzáférni és ezeket bekérni, ezek tartalmát felülvizsgálni,**
- **a meglévő auditjelentés eredménye alapján a következő audit célkitűzését meghatározni,**
- **rendkívüli auditot elrendelni.**

Kiberbiztonsági audit lefolytatására kötelezettek

A Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja szerinti azon szervezet, amely egyúttal a 2. és 3. melléklet szerinti szervezet is, valamint az 1. § (1) bekezdés d) pontja és – a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerinti mikrovállalkozás kivételével – az 1. § (1) bekezdés e) pontja szerinti szervezet az e törvény szerinti kiberbiztonsági követelményeknek való megfelelés bizonyítására köteles kétévente, illetve az SZTFH általi elrendelés esetén kiberbiztonsági auditot végeztetni.

- **Többségi állami tulajdonban lévő szervezet,**
  - **amely nem minősül a közigazgatási ágazathoz tartozó szervezetnek,**
  - **összes foglalkoztatotti létszáma eléri vagy meghaladja az 50 főt, vagy éves nettó árbevétele és mérlegfőösszege meghaladja a 10 millió eurónak megfelelő forintösszeget, és**
  - **kiemelten kockázatos vagy kockázatos ágazat szerinti tevékenység végzésére jogosult.**
- **Kiemelten kockázatos és kockázatos ágazat szerinti tevékenység végzésére jogosult szervezetek, amennyiben a Kkvtv. szerint a szervezet középvállalkozásnak minősül.**
- **Méretkorlát nélkül:**
  - **elektronikus hírközlési szolgáltató,**
  - **bizalmi szolgáltató,**
  - **DNS-szolgáltató,**
  - **legfelső szintű doménnév-nyilvántartó,**
  - **doménnév-regisztrációt végző szolgáltató**

Az audit lefolytatásnak határideje, amennyiben a szervezet 2025.01.01. előtt kezdte meg működését



	2024. január 1.	2024. október 18.	2025. július 31.	2025. augusztus 31.	2026. június 30.
SZTFH	• Érintett szervezetek nyilvántartásba vétele • Auditorok nyilvántartásba vétele	• Felügyeleti tevékenység • Ellenőrzési tevékenység			
Érintett szervezet	• Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig; • Szervezet EIR-jeinek azonosítása, biztonsági osztályba sorolás • Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése.	• Védelmi intézkedések alkalmazása	• Kiberbiztonsági felügyeleti díj megfizetése	• Első kiberbiztonsági auditra vonatkozó szerződéskötés az auditorral	• Első kiberbiztonsági audit lefolytatásának határideje

Az audit lefolytatásának határideje, amennyiben a szervezet 2025.01.01. után kezdte meg működését

	Kiberbiztonsági tv. hatálya alá tartozás napja	Nyilvántartásba vételt követő 30 nap	Nyilvántartásba vételt követő 120 nap	Nyilvántartásba vételt követő 2 éven belül
SZTFH	• Érintett szervezetek nyilvántartásba vétele		• Felügyeleti tevékenység • Ellenőrzési tevékenység	
Érintett szervezet	• Önazonosítás, nyilvántartásba vételre bejelentkezés • Szervezet EIR-jeinek azonosítása, biztonsági osztályba sorolás • Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése	• Kiberbiztonsági felügyeleti díj megfizetése	• Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral	• Első kiberbiztonsági audit lefolytatásának határideje

Az auditorok

Auditor	Vizsgálható biztonsági osztály
Alverad Technology Focus Korlátolt Felelősségű Társaság	Alap
Andrews IT Engineering Mérnöki, Információtechnikai és Szolgáltató Korlátolt Felelősségű Társaság	Alap
Certop Informatikai Tanúsítási Szolgáltatások Korlátolt Felelősségű Társaság	Alap, Jelentős
Ernst & Young Tanácsadó Korlátolt Felelősségű Társaság	Alap
HUNGUARD Számítástechnikai-, informatikai kutató - fejlesztő és általános szolgáltató Korlátolt Felelősségű Társaság	Alap, Jelentős, Magas
KÜRT Információbiztonsági és Adatmentő Zrt.	Alap, Jelentős
Mikroháló Távközlési, Szolgáltató Korlátolt Felelősségű Társaság	Alap
NETI Informatikai Tanácsadó Kft.	Alap
VALILAB IT Biztonsági Vizsgálólaboratórium Korlátolt Felelősségű Társaság	Alap
VERITAN Hírközlési és Informatikai Tanúsító Kft.	Alap

A kiberbiztonsági audit terjedelme

A kiberbiztonsági audit kiterjed:

- **a kockázatmenedzsment keretrendszer és a biztonsági osztályba sorolás,**
- **az elektronikus információs rendszerekhez kapcsolódó, a szervezet elektronikus információs rendszereinek védelmével összefüggő dokumentumok – ideértve a szervezet belső szabályozó eszközeit, szerződéseket –, illetve eljárások,**
- **az elektronikus információs rendszerekben alkalmazott hardver, szoftver vagy firmware elemekben megvalósított funkciók, kezelésükre vonatkozó bizonyítékok, a kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltatóval szembeni elvárások,**
- **az elektronikus információs rendszerek védelmét támogató folyamatokban részt vevő valamennyi természetes személy ilyen irányú tevékenysége,**
- **az elektronikus információs rendszerek védelme tekintetében a személyi feltételek és az ehhez kapcsolódó munkaköri felelősségek, valamint**
- **a szervezet által meghatározott eljárások gyakorlati megvalósulása**

vizsgálatára.

A szervezet rendelkezésében lévő EIR

Kiberbiztonsági tv. 6. § (1) bekezdése értelmében: A szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert.

A passzus nyelvtani értelmezése értelmében egy rendszer akkor van a rendelkezésében, amennyiben az érintett szervezet ténylegesen hozzáfér az adott elektronikus információs rendszerhez, jogosult azt irányítani, menedzselni, használni, azzal rendelkezni, vagy annak működésére hatást gyakorolni, függetlenül attól, hogy az elektronikus információs rendszer a szervezet tulajdonában van-e.

Rendelkezés alatt érteni kell különösen

a) a rendszer működésének irányítását;
b) a rendszer konfigurálását, felügyeletét;
c) a rendszer biztonságáért való felelősséget;
d) a rendszerrel összefüggő hardverekhez, szoftverekhez, illetve adatokhoz való hozzáférést;
e) a rendszerhez kapcsolódó jogosultságkezelési feladatok ellátását;
f) a rendszer használatával, fenntartásával kapcsolatos döntéshozatali jogosultságot.

Az elektronikus információs rendszerrel való rendelkezés lehet fizikai és logikai egyaránt.

Biztonsági osztályba sorolás

Az EIR biztonsági osztályba sorolását az EIR-ben kezelt adatok és az EIR funkciói határozzák meg és amely alapján az EIR:

- **Alap;**
- **Jelentős, illetve**
- **Magas biztonsági osztályba sorolható.**

A biztonsági osztályba sorolás elvégzése a szervezet felelőssége, melynek eredményét a szervezet vezetője hagyja jóvá.

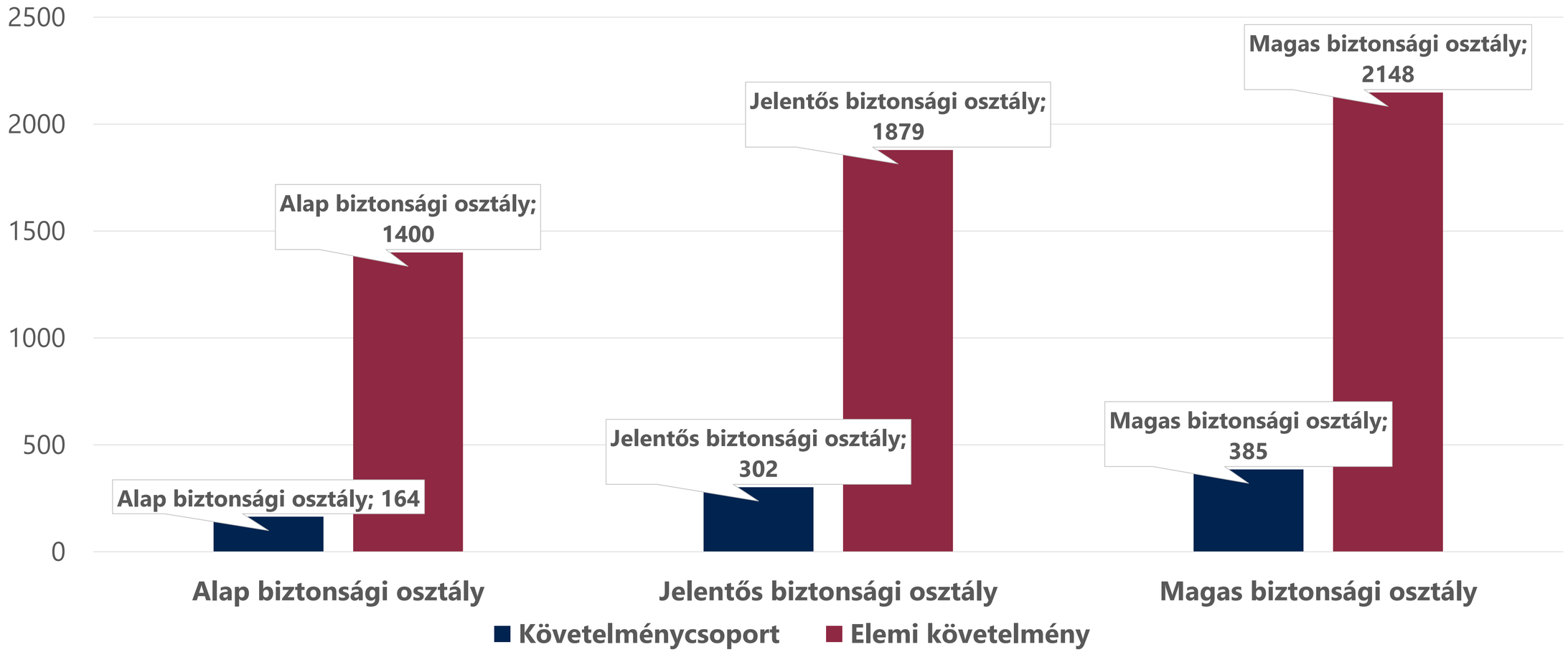
Az EIR biztonsági osztályba sorolása határozza meg a szükséges védelmi intézkedéseket, valamint azt, hogy a szervezet esetében mely auditor jogosult kiberbiztonsági auditot végezni.

A szervezet a 7/2024 (IV.24.) MK rendelet alapján beazonosítja a biztonsági osztályhoz tartozó védelmi intézkedéseket, majd a beazonosított intézkedéseket a kockázatelemzés alapján testre szabhatja.

Nem a teljes megfelelés, hanem a kockázatokkal arányos védelem kialakítása a cél.

Követelmények

Vizsgálandó követelménycsoportok és elemi követelmények szám szerinti megoszlása az egyes biztonsági osztályok esetén



Az audit maximális díja - 1/2025. (I.31.) SZTFH rendelet

Előző üzleti évi nettó árbevétel

Szorzószám az árbevétel függvénye:

0,9-4

EIR darabszáma

Darabszám függvénye a szorzószám

- 1-5 EIR: 1
- 6-15 EIR: 2,5
- 16 vagy több: 4

EIR biztonsági osztálya

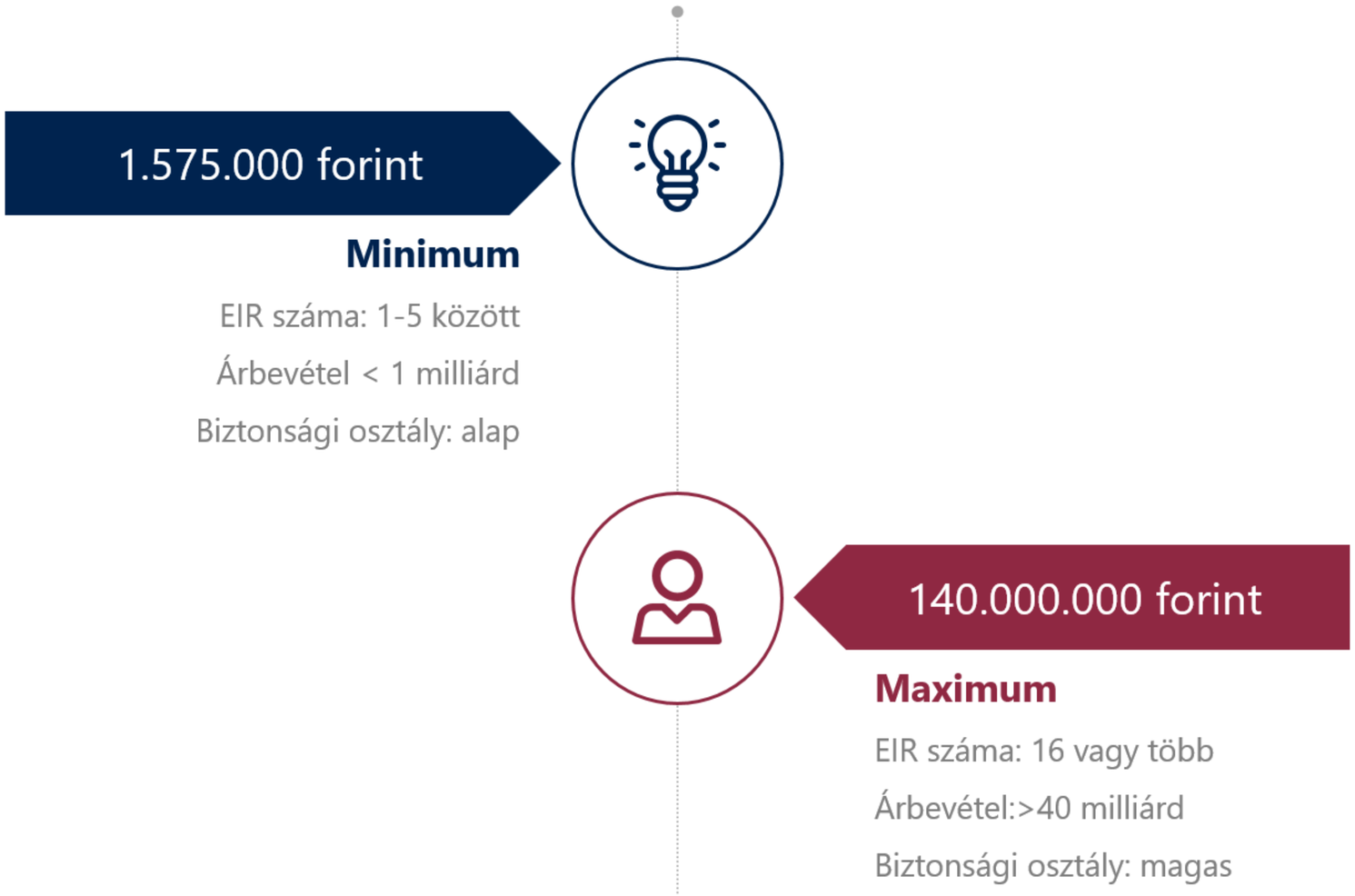
Szorzószám biztonsági osztályonként:

- alap: 1
- jelentős: 3
- magas: 5

1 750 000 forint

alapdíj

Az audit díja



Audit eredménye – VMI

VMI:

$$VMI = 100 - 100 * \frac{2*\sum_{i=1}^{n} b_i + \sum_{j=1}^{m} t_j}{20n+10m}$$

A „Biztosító” típusú követelménycsoportok kétszeres, míg a „Támogató” típusú követelménycsoportok teljesítése egyszeres súlyozással számítódik a képlet alapján és amely alapján az eltérés mértéke az alábbiak szerint alakul:

Eltérés mértéke	Az EIR-nek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő értékelése
VMI ≥ 95	megfelel
90 ≤ VMI < 95	alacsony kockázattal megfelel
80 ≤ VMI < 90	jelentős kockázattal megfelel
70 ≤ VMI < 80	magas kockázattal megfelel
VMI < 70	nem felel meg

Audit eredménye – SZEKI

SZEKI: $$szervezet\ ellenálló - képességi\ indexe = \frac{\sum_{i=1}^{n} VMI_i}{n}$$

A VMI értékek számtani átlaga, amely alapján a szervezet minősítése az alábbiak szerint alakul:

A szervezet értékelése	A szervezetnek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő minősítése	Értékelés eredménye
SZEKI ≥ 95	elhanyagolható kockázattal megfelel	megfelelt
90 ≤ SZEKI < 95	alacsony kockázattal megfelel	auditált
80 ≤ SZEKI < 90	közepes kockázattal megfelel	
70 ≤ SZEKI < 80	magas kockázattal megfelel	
SZEKI < 70	kritikus kockázattal nem felel meg	nem megfelelt

Mi a teendő, amennyiben egy szervezet nem rendelkezik EIR-rel ?

Azon szervezetek vonatkozásában, amelyeknek nem áll rendelkezésében elektronikus információs rendszer, nem tudják elvégezni az auditot az elektronikus információs rendszerek vonatkozásában, azonban az egyéb követelmények tekintetében (például: szervezeti követelmények, szabályzatok kialakítása, oktatások, fizikai biztonság, stb.) meg kell felelni a vonatkozó védelmi intézkedéseknek és ezt bizonyítandó az auditkötelezettség is fennáll.

Bár az elvi lehetősége fennáll annak, hogy egy szervezet rendelkezésében nincs elektronikus információs rendszer, a hatóság tapasztalatai alapján ez rendkívül ritka, kivételes esetekben fordulhat elő.

Amennyiben a szervezet akár csak egy olyan eszközzel rendelkezik, amely egy szoftver segítségével képes digitális adatok feldolgozására, tárolására vagy továbbítására, az megalapozza az elektronikus információs rendszer létét, így azt – vagy azokat – a 7/2024. (VI.24.) MK rendeletben foglaltak szerint biztonsági osztályba kell sorolni és az ennek megfelelő követelményeket teljesíteni szükséges.

Vonatkozó bírságtételek

A szabálytalanságok esetén kiszabható minimális és maximális bírságtételeket a 418/2024. (XII.23.) kormányrendelet 3. melléklete tartalmazza.

A szabálytalanság megnevezése	A bírság legkisebb mértéke	A bírság legnagyobb mértéke
A kiberbiztonsági auditra vonatkozó megállapodás határidőben történő megkötésére vonatkozó kötelezettség teljesítésének elmulasztása	1 000 000 forint	15 000 000 forint
A kiberbiztonsági audit határidőn belüli lefolytatásának elmulasztása	1 000 000 forint	50 000 000 forint

További hasznos információkat a Hatóság honlapján érhet el.