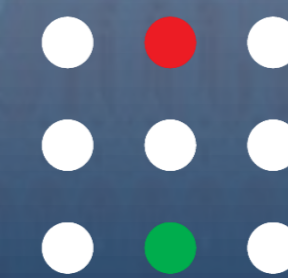


Hatósági tapasztalatok a NIS2 megfelelés tükrében

**Magyar Kapcsolt Energia
Társaság**

Mátraháza, 2026.03.11.

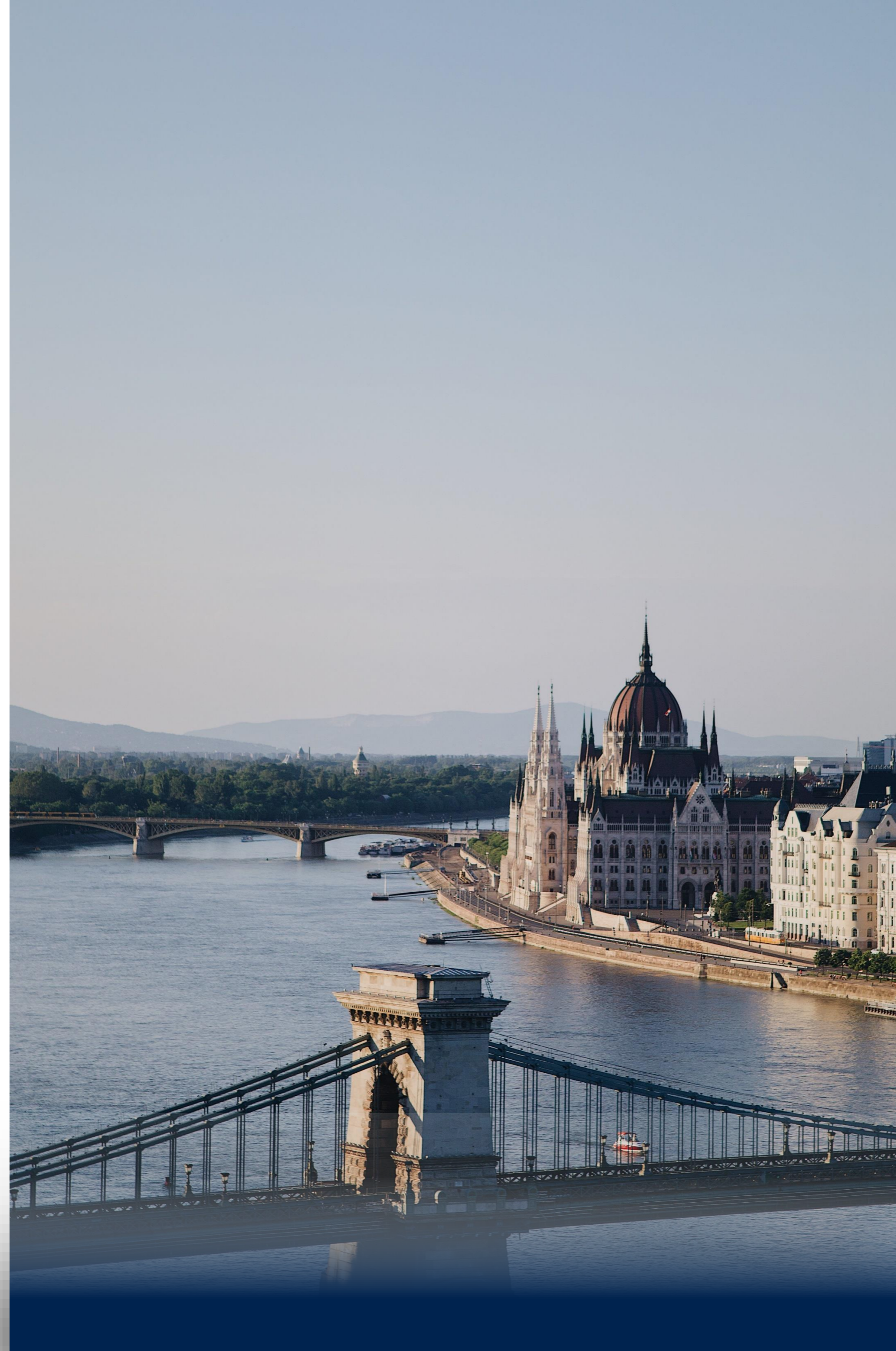
Dr. Szemeti Ferenc



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Az SZTFH szerepe a NIS2 irányelv alapján

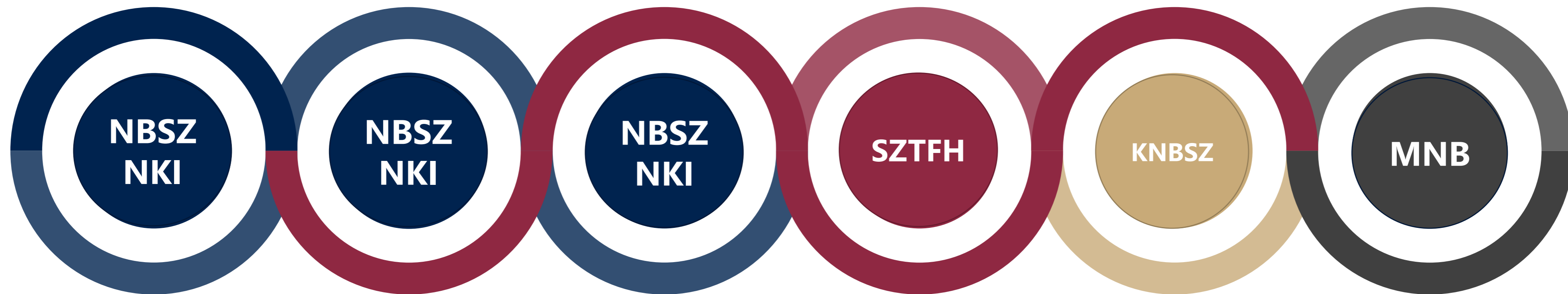


A kiberbiztonság hazai felügyelete

**Többségi állami befolyás
alatt álló gazdasági
szervezet**

**Kiemelten kockázatos és
kockázatos tevékenységet
folytató gazdálkodó
szervezetek**

Pénzügyi szervezetek



**Közigazgatási szervek és
önkormányzati hivatalok**

**Kritikus infrastruktúrák
alapvető
szolgáltatásában
közreműködő rendszerei**

**Honvédelmi célú
rendszerelemek**

Előzmények

- 2024-ben a magyar Országgyűlés elfogadta a Magyarország kiberbiztonságáról 2024. évi LXIX. Törvényt, amely 2025. január 1-jével lépett hatályba.
- A meglévő jogszabályi keretrendszer megszilárdításával és kibővítésével a törvény erősíti Magyarország kiberbiztonsági környezetét, és jobban összehangolja azt az uniós szabványokkal (NIS1 és NIS2 irányelvek).
- A jelenlegi rendelkezések értelmében a kiberbiztonsági hatóság feladatait több intézmény látja el Magyarországon, a felügyelt szervezettől (gazdasági szereplők, bankok és egyéb pénzügyi intézmények, közigazgatási szervezetek, kritikus infrastruktúrák) függően, amelyek egyike az SZTFH.
- **Kiberbiztonsági hatóságként az SZTFH látja el az IKT és IoT-termékek és-szolgáltatások nemzeti kiberbiztonsági tanúsító hatóságának feladatait, valamint kiberbiztonsági felügyeletet végez a NIS2 által érintett szervezetek felett.**

Az SZTFH szerepe a hazai kiberbiztonságban

SZTFH által felügyelt ágazatok (NIS2 irányelv alapján)



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 Kkv tv. szerint a szervezet közép vállalkozásnak 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 Kkv tv. szerint a szervezet közép vállalkozásnak 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**
Kivéve:
 - költségvetési szervek
- **Kiberbiztonsági audit lefolytatása**
Kivéve:
 - mikrovállalkozások

Kiberbiztonsági felügyeletben érintett szervezet kötelezettségei

Nyilvántartásban való szereplés kötelezettségei kiegészülve az alábbiakkal

A szervezet esetében 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 teljesülésének 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 felügyelet – érintett szervezetek mérete *



* Kivéve azon szervezetek, melyek a Kiberbiztonsági tv. 1. § (1) bekezdésének e) pontja alapján méretkötlet nélkül a törvény személyi hatálya alá tartoznak:

- elektronikus hírközlési szolgáltató,
 - bizalmi szolgáltató,
 - DNS-szolgáltató,
- legfelső szintű doménnév-nyilvántartó,
- doménnév-regisztrációt végző szolgáltató.

Szervezet mérete – kiemelten kockázatos és kockázatos ágazat esetében

	Szervezet mérete (Kkvtv.*)				
	mikrovállalkozás	kisvállalkozás	középvállalkozás	nagyvállalkozás	
foglalkoztatotti létszám	kevesebb, mint 10	kevesebb, mint 50	kevesebb, mint 250	több, mint 250	Fő
	és	és	és	és	
előző évi bevétel	legfeljebb 2	legfeljebb 10	legfeljebb 50	legalább 50	Millió €
			vagy	vagy	
mérlegfőösszeg			legfeljebb 43	legalább 43	Millió €

* A 2004. évi XXXIV. Törvény alapján a vállalkozás abban az esetben veszíti el, illetve nyeri el a KKV minősítést, **ha két egymást követő számviteli időszakban, illetve bevallási időszakban túllépi a fenti táblázatban meghatározott foglalkoztatotti létszámot vagy pénzügyi határértékeket, vagy elmarad azoktól.**

Energetika ágazat



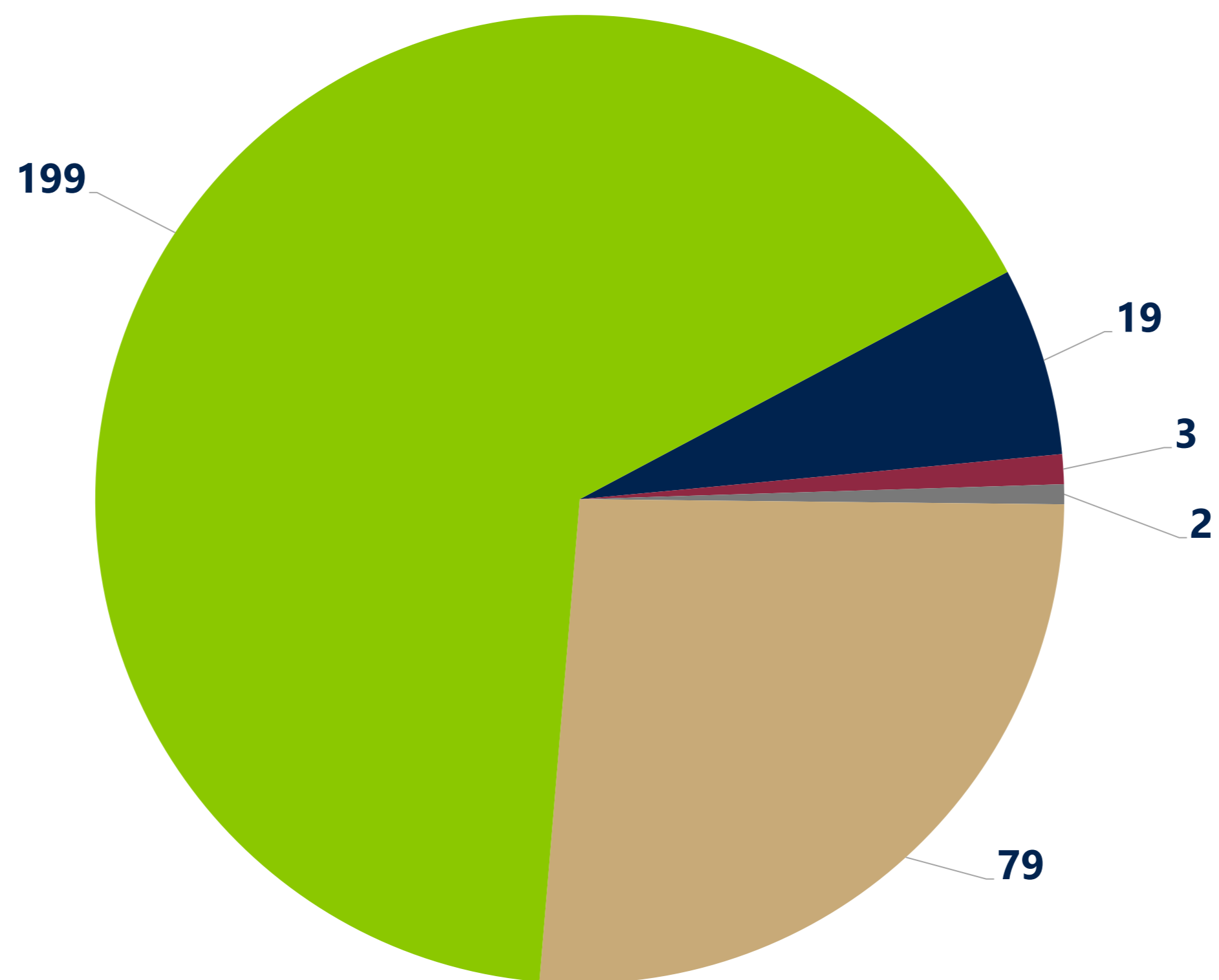
Nyilvántartásba vett szervezetek

A Kiberbiztonsági törvény 2. melléklete szerint:

- **Villamos energia alágazat:** a villamos energiáról szóló törvény szerinti **villamosenergia-ipari vállalkozás** a közvilágítási üzemeltetési engedélyes kivételével;
- **Távfűtés és hűtés alágazat:** a távhőszolgáltatásról szóló törvény szerinti engedélyes,
- **Kőolaj alágazat:** a bányászatról szóló törvény szerinti
 - szénhidrogén szállítóvezetékét létesítő és üzemben tartó engedélyes,
 - a kőolajfeldolgozásban, tárolásban használt létesítmény üzemeltetője,
 - a behozott kőolaj és kőolajtermékek biztonsági készletezéséről szóló törvény szerinti központi készletező szervezet.
- **Földgáz alágazat:** – az egyablakos kapacitásértékesítő, a szervezett földgázpiaci engedélyes és a vezetékes PB-gáz szolgáltató kivételével – a földgázellátásról szóló törvény szerinti engedélyes tevékenységet folytató földgázipari vállalkozás;
- **Hidrogén alágazat:** a hidrogéntermelés, -tárolás és -szállítás üzemeltetője

→ Jelenleg **302** szervezet szerepel a hatósági nyilvántartásban, mint „Energetika” ágazatban tevékenységet folytató szervezet.

Energetikai ágazat – alágazatok



■ Földgáz ■ Hidrogén ■ Kőolaj ■ Távfűtés és hűtés ■ Villamos energia

2026. Február 17-i állapot szerint.

A MEKH szerepe az SZTFH kiberbiztonsági eljárásaiban

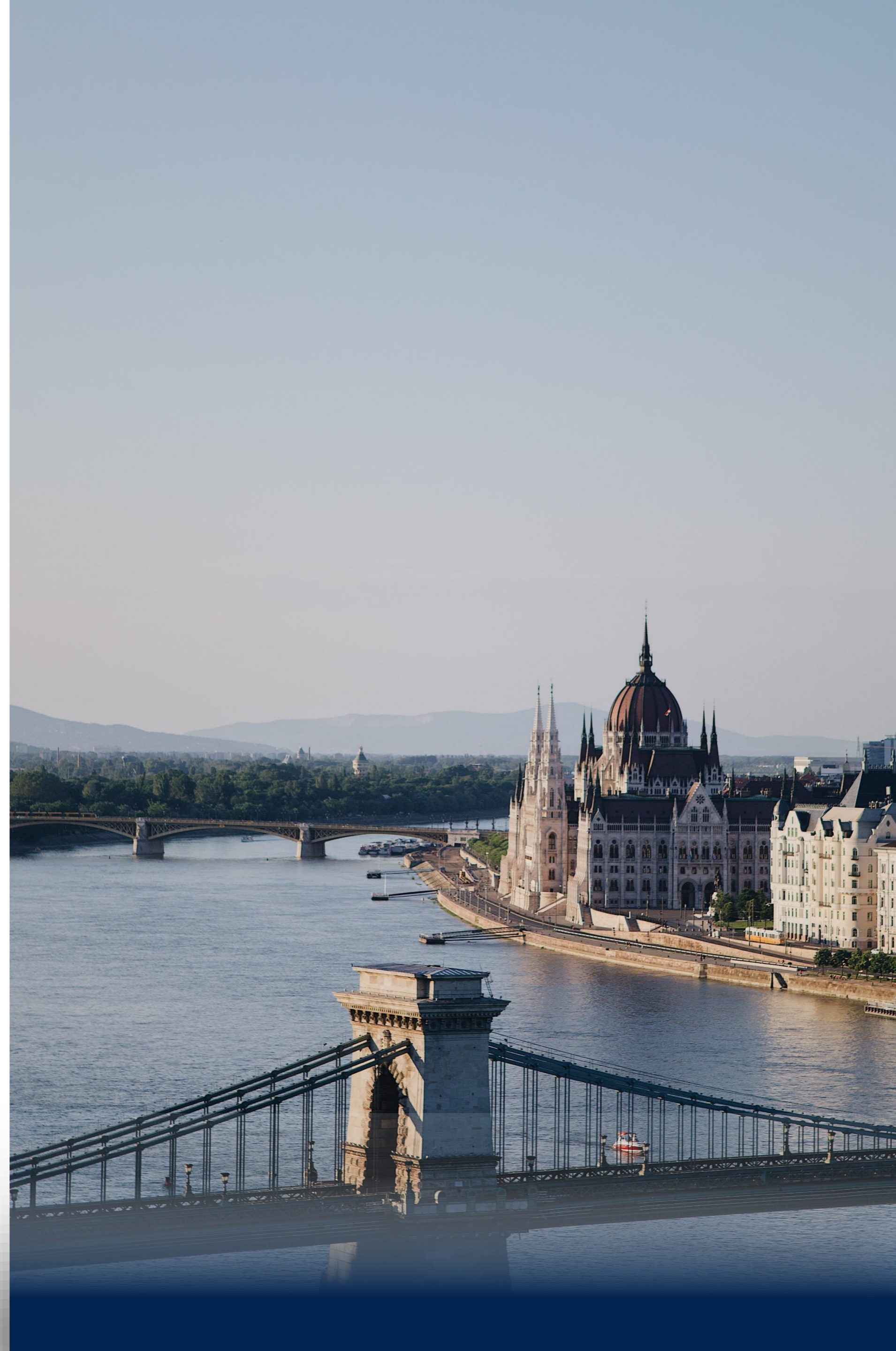
A Kiberbiztonsági törvény 2. és 3. melléklete alapján az alábbi kockázatos, valamint kiemelten kockázatos ágazatok esetében is jelentős szerepet töltenek be a **Magyar Energetikai és Közmű-szabályozási Hivatal** által vezetett nyilvántartások az SZTFH hatósági eljárásai során.

Az SZTFH a

- Villamosenergiái-ipari;
- Földgázipari;
- Távhőszolgáltató;
- Távhőtermelői;
- Víziközmű-szolgáltató;
- Hulladékgyártás

tevékenységekkel kapcsolatos nyilvántartásba vételi, illetve nyilvántartásból való törlési kérelmek elbírálásakor a MEKH által vezetett, adott ágazatra vonatkozó „Engedélyesek listája” alapján ellenőrzi, hogy a kérelmet benyújtott szervezet jogosult-e a fenti tevékenységek nyújtására.

Nyilvántartott szervezetek kötelezettségei



Vezetői felelősség

A szervezet vezetője köteles

Kockázatmenedzsment keretrendszert hoz létre és működtet.

Gondoskodik a szervezet által használt elektronikus információs rendszerek, központi szolgáltatások felméréséről és nyilvántartásba vételéről.

Legalább két évente, az információbiztonsági szabályzat felülvizsgálatával, illetve ennek következményeként a biztonsági osztályba sorolást.

Gondoskodni arról, hogy a szervezet együttműködjön a kiberbiztonsági hatósággal. (adatváltozások bejelentés)

Kijelöli az elektronikus információs rendszer biztonságáért felelős személyt vagy a szervezeten kívüli személlyel megállapodást köt.

Gondoskodik a biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során feltárt hiányosságok orvoslásáról.

Jóváhagyja az elektronikus információs rendszer esetében alkalmazott helyettesítő védelmi intézkedéseket és eltéréseket.

Kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a gyors és hatékony reagálásról

Vezetői felelősség

Ha a szervezet vezetője a jogszabályban előírt kötelezettségének nem tesz eleget, a nemzeti kiberbiztonsági hatóság az eset összes körülményének mérlegelésével **kormányrendeletben meghatározott mértékű bírsággal sújthatja, ismételt jogsértés esetén sújtani köteles.** → 418/2024. (XII. 23.) Korm. Rendelet alapján 15 millió forintig terjedő bírsággal sújthatja, illetve ismételt jogsértés esetén sújtja.

Ha a nem közigazgatási szervnek minősülő alapvető szervezet a kiberbiztonsági hatóság által szabott határidőn belül nem tesz eleget a hatósági kötelezésnek, a kiberbiztonsági hatóság

a) kezdeményezheti az illetékes hatóságnál az alapvető szervezet által nyújtott, a jogsértéssel érintett alapvető szolgáltatások vagy tevékenységek egészére vagy egy részére vonatkozó tanúsítás vagy engedély ideiglenes felfüggesztését és

b) kezdeményezheti a cégbíróságnál az alapvető szervezet vezetőjének az adott szervezetben betöltött vezető tisztségviselői feladatainak ellátásától való ideiglenes eltiltását.

Hatósággal való kommunikáció

Az SZTFH-val való kapcsolattartás elektronikusan és elektronikus űrlapokon keresztül valósul meg.

- **SZTFH – 420 űrlap: érintett szervezet nyilvántartásba vételére irányuló kérelem**
- **SZTFH – 421 űrlap: érintett szervezet adatváltozásának bejelentésére és törlésére irányuló kérelem**

Adatváltozásban érintett adat:

- **a szervezet azonosításához szükséges adatok,**
- **ha a szervezet nem az Európai Unióban letelepedett szervezet, de Magyarországon belül kínál szolgáltatásokat és magyarországi letelepedett képviselőt jelöl ki, a képviselő nevét vagy cégnevét, levelezési címét, telefonszámát és elektronikus levelezési címét,**
- **az elektronikus információs rendszer biztonságáért felelős személy természetes személyazonosító adatait, telefonszámát és elektronikus levelezési címét,**
- **azon európai uniós tagállamok listáját, amelyben a szervezet szolgáltatásokat nyújt,**
- **a 23/2023 (XII.19.) SZTFH elnökének rendeletében előírt további, személyes adatnak nem minősülő adatok.**

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.**

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 szöveg 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.

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.

Kiberbiztonsági audit



Audit kötelezettség

A Kiberbiztonsági törvény alapján:

Azon szervezetek, melyek a Kiberbiztonsági törvény 1. § (1) bekezdés b) pontja szerinti azon szervezetek, amelyek egyúttal a 2. és 3. melléklet szerinti szervezetek 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 szervezetek, kötelesek a kétévenkénti kiberbiztonsági audit lefolytatására.

Vagyis:

- a mikrovállalkozások mentesülnek az auditkötelezettség alól, de a felügyeleti díj fizetési kötelezettségük továbbra is fennáll, valamint
- **azon szervezetek, melyek többségi állami tulajdonban vannak, de az SZTFH nyilvántartásában is szerepelniük kell, – a költségvetési szervek kivételével – kiberbiztonsági felügyeleti díj fizetésére és a rendelkezésükben álló EIR-ek tekintetében auditra kötelezettek.**

A kiberbiztonsági audit során az audit lefolytatására jogosult, az SZTFH által nyilvántartásba vett auditorok

- **az elektronikus információs rendszerek (a továbbiakban: EIR) biztonsági osztályba sorolását, valamint**
- **a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségét ellenőrzik.**

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

Előző üzleti évi nettó árbevétel

Szorószám az árbevétel függvénye:
0,9-4

EIR darabszáma

Darabszám függvénye a szorószám

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



EIR biztonsági osztálya

Szorószám biztonsági osztályonként:

- alap: 1
- jelentős: 3
- magas: 5

1 750 000 forint
alapdíj

Az audit díja

1.575.000 forint

Minimum

EIR száma: 1-5 között
Árbevétel < 1 milliárd
Biztonsági osztály: alap



140.000.000 forint

Maximum

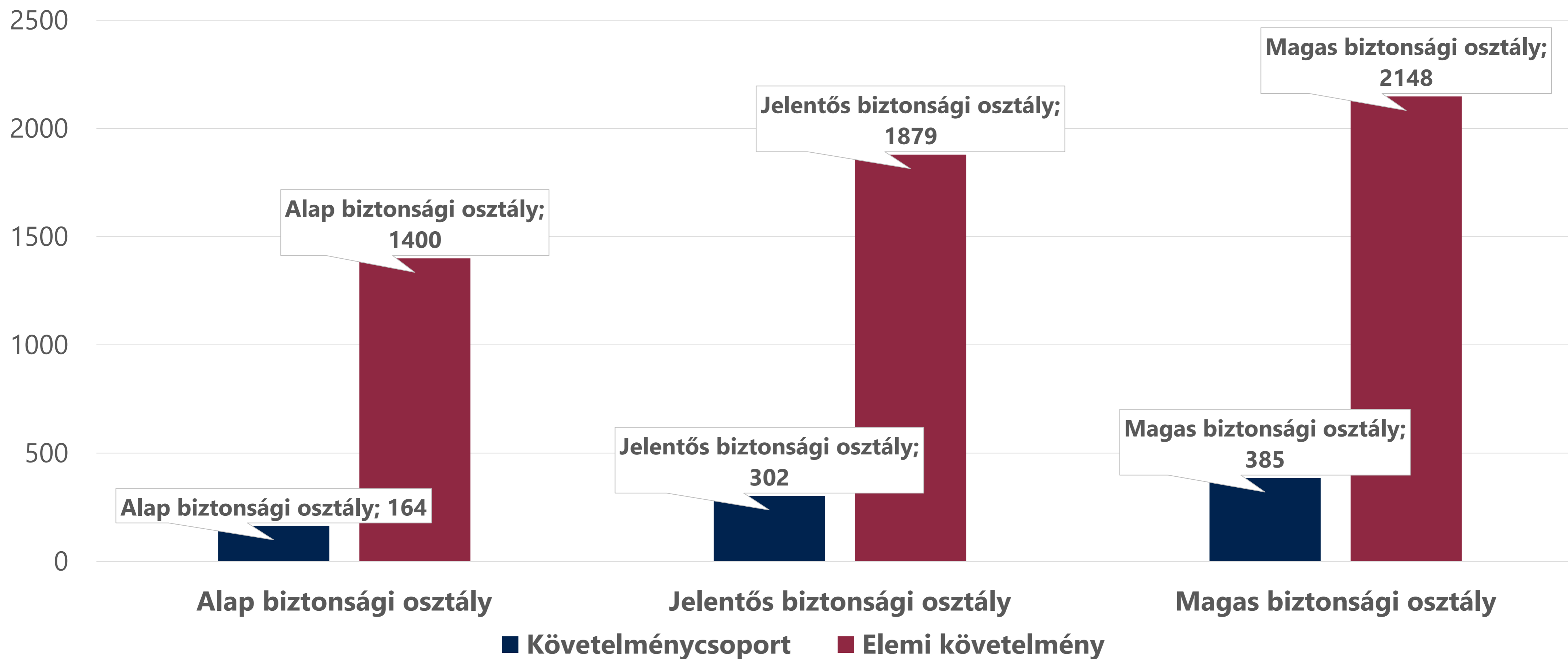
EIR száma: 16 vagy több
Árbevétel: >40 milliárd
Biztonsági osztály: magas

Az auditorok

Auditor	Vizsgálható biztonsági osztály
Alverad Technology Focus Korlátolt Felelősségű Társaság	Alap
Andrews IT Engineering Mérnöki, Informatikai és Szolgáltató Korlátolt Felelősségű Társaság	Alap
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
VantaSec Korlátolt Felelősségű Társaság (Jogelőd szervezet: Certop Informatikai Tanúsítási Szolgáltatások Korlátolt Felelősségű Társaság)	Alap, Jelentős
VERITAN Hírközlési és Informatikai Tanúsító Kft.	Alap

Követelmények

Vizsgálható követelménycsoportok és elemi követelmények számszerinti megoszlása az egyes biztonsági osztályok esetén



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 számítható 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
$VMI \geq 95$	megfelel
$90 \leq VMI < 95$	alacsony kockázattal megfelel
$80 \leq VMI < 90$	jelentős kockázattal megfelel
$70 \leq VMI < 80$	magas kockázattal megfelel
$VMI < 70$	nem felel meg

Audit eredménye – SZEKI

SZEKI:

$$\text{szervezet ellenálló – képességi indexe} = \frac{\sum_{i=1}^n VMI_i}{n}$$

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 \geq 95	elhanyagolható kockázattal megfelel	megfelelt
90 \leq SZEKI $<$ 95	alacsony kockázattal megfelel	auditált
80 \leq SZEKI $<$ 90	közepes kockázattal megfelel	
70 \leq SZEKI $<$ 80	magas kockázattal megfelel	
SZEKI $<$ 70	kritikus kockázattal nem felel meg	nem megfelelt

Az auditot követően

A kiberbiztonsági audit lezárásakor az auditor a kiberbiztonsági audit során keletkezett bizonyítékokat és az audit eredményét tartalmazó **magyar nyelvű auditjelentést nyomtatható, és gépi feldolgozást támogató formátumban** kell megküldi a Hatóság részére.

Az auditjelentés mellékleteként az auditor auditigazolást állít ki.

Az auditor a vizsgálati eredményeket és az azokhoz tartozó bizonyítékokat kizárólag a vizsgált szervezet és a Hatóság részére adhatja át.

A **szervezet** az auditor által átadott bizonyítékokat a kiberbiztonsági audit lezárásának időpontjától számított **5 évig megőrzi**. → a szervezet felelőssége, nem az auditoré!

Ha nem sikerül az audit

Ha a szervezet vagy a kiberbiztonsági audit során az auditor az adott elektronikus információs rendszerre vonatkozó biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során hiányosságot állapít meg, akkor a szervezet – a vizsgálat vagy a kiberbiztonsági audit eredményének kézhezvételét követő **90 napon belül – intézkedési tervet készít a hiányosság megszüntetésére, amelyet jóváhagyásra benyújt a nemzeti kiberbiztonsági hatóság részére.**

A Hatóság a 3/2025 (IV.17.) SZTFH rendelet alapján jogosult többek közt:

- a szervezet által meghatározott biztonsági osztályhoz tartozó védelmi intézkedéseken túl további biztonsági követelményeket meghatározni,
- a védelmi intézkedések és az ezekhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
- rendszeres, eseti és célzott biztonsági ellenőrzéseket végezni, ideértve a helyszíni ellenőrzéseket, a távoli felügyeleti intézkedéseket és a véletlenszerű ellenőrzéseket is,
- az ellenőrzés során feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,
- a meglévő auditjelentés eredménye alapján a következő audit célkitűzését meghatározni,
- rendkívüli auditot elrendelni,
- információbiztonsági felügyelőt kirendelni a Hatóság munkatársai közül.

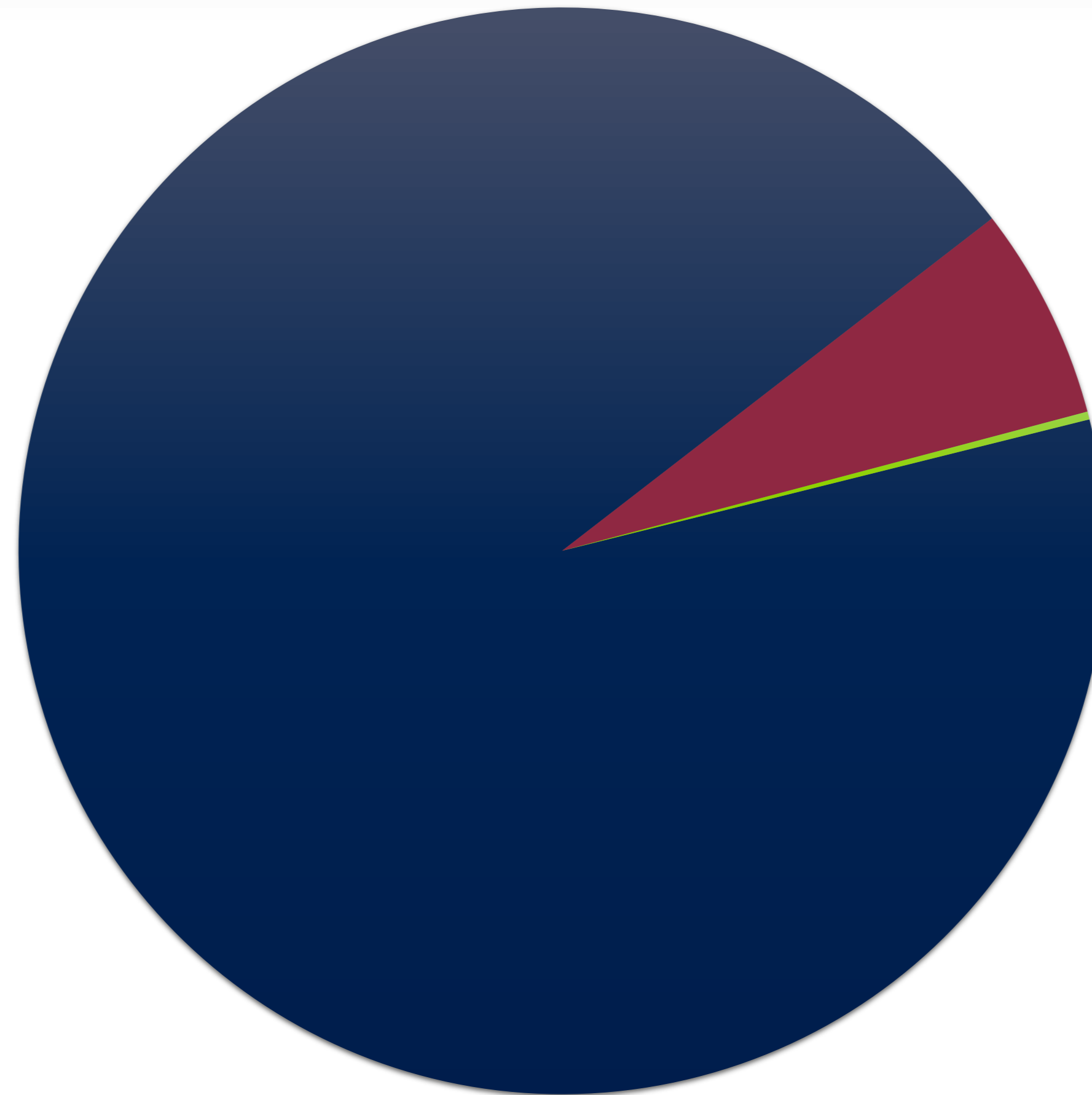
Bírságok

- 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 nyilvántartásba vétel érdekében történő adatszolgáltatás nem teljesítése	a szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának 0,5%-a, de legalább 1 000 000 forint	a szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának legfeljebb 2%-a, de legfeljebb 150 000 000 forint
A nyilvántartásba vétel érdekében történő adatszolgáltatás határidőn túl történő teljesítése	50 000 forint	a szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának legfeljebb 0,1%-a, de legfeljebb 15 000 000 forint
A felügyeleti díjfizetés elmulasztása	500 000 forint	a kiberbiztonsági éves felügyeleti díj maximum tízszerese
A nyilvántartásba vétel óta bekövetkezett adatváltozás megküldésének elmulasztása	50 000 forint	1 000 000 forint
A kockázatmenedzsment keretrendszer kialakítására és működtetésére vonatkozó kötelezettség nem teljesítése	1 000 000 forint	a) Ha a szervezet alapvető szervezetnek minősül 10 millió euronak megfelelő forintösszeg vagy, ha ez magasabb a szervezet előző pénzügyi évi globális éves forgalma teljes összege 2%-ának megfelelő összeg, b) Ha a szervezet fontos szervezetnek minősül 7 millió euronak megfelelő forintösszeg vagy, ha ez magasabb a szervezet előző pénzügyi évi globális éves forgalma teljes összege 1,4%-ának megfelelő összeg.
A kiberbiztonsági audit határidőn belüli lefolytatásának elmulasztása	1 000 000 forint	50 000 000 forint

Audit tapasztalatok – EIR darabszám

**1-5 darab EIR: 397
szervezet esetében**



**6-15 darab EIR: 27
szervezet esetében**

**15 darabnál több
EIR: 1 szervezet**

2026. Február 17-i állapot szerint.

Audit tapasztalatok – VMI megoszlása

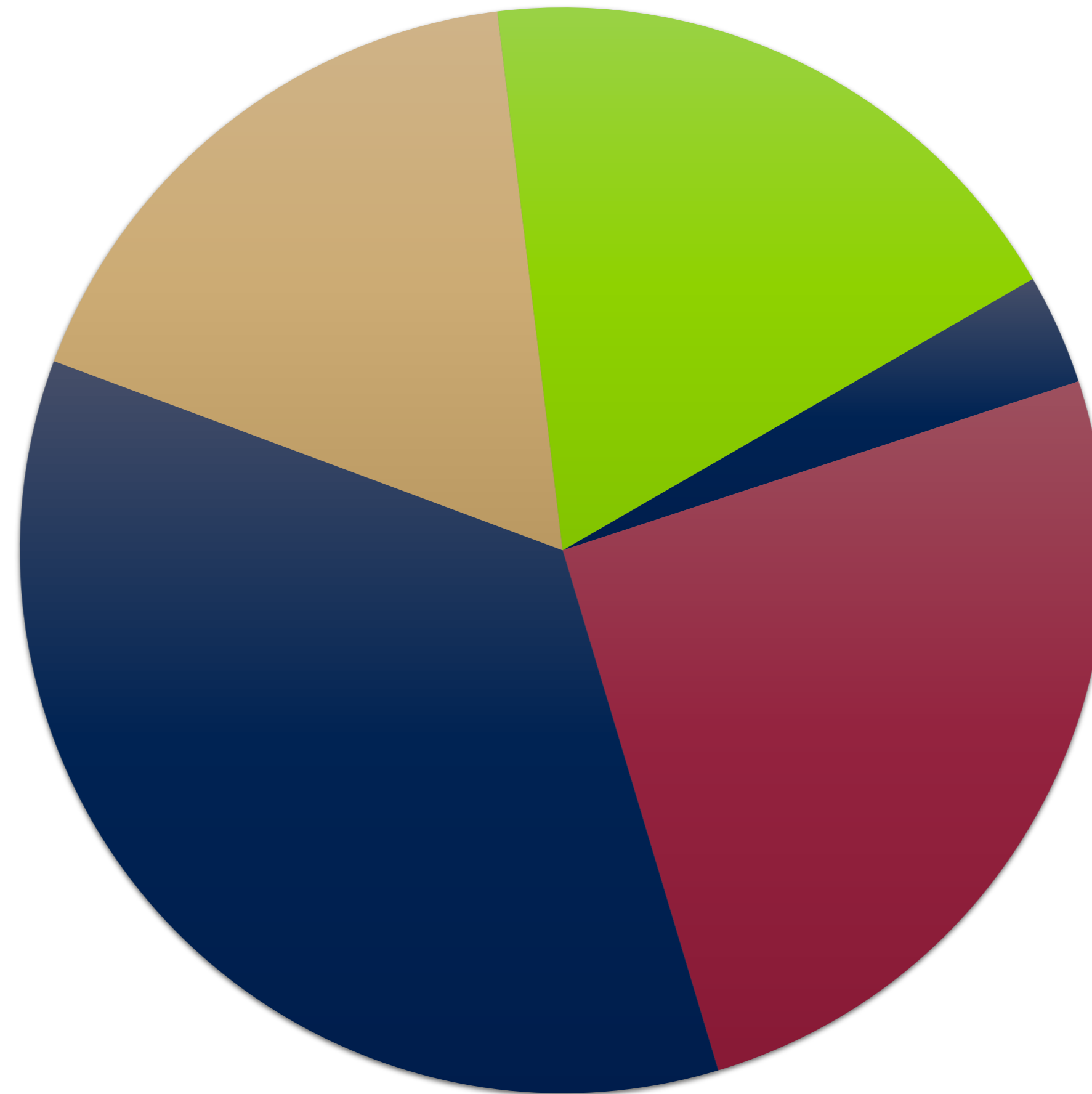
VMI 90-94:
74 szervezet

VMI 95-100:
79 szervezet

VMI <70:
14 szervezet

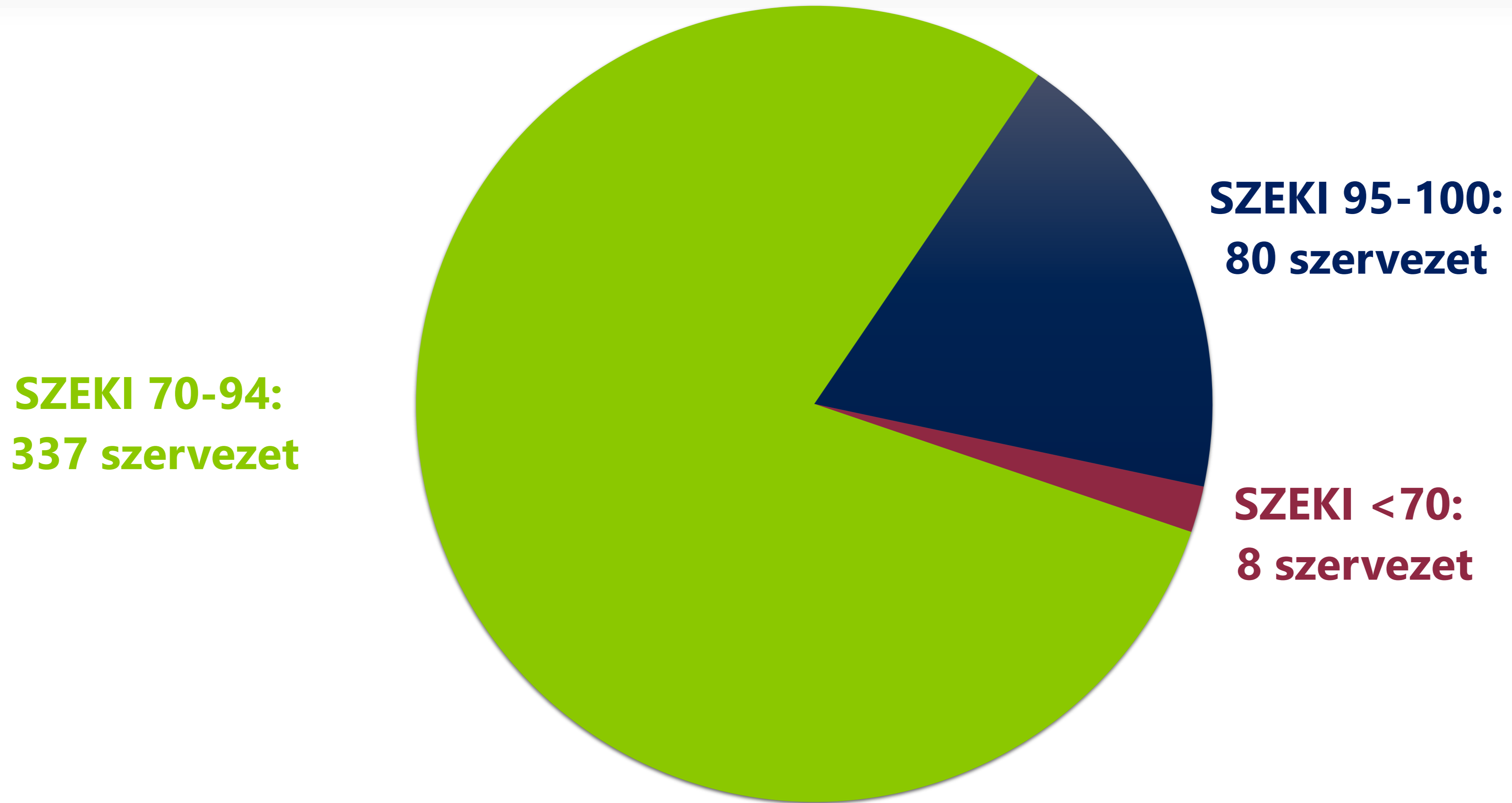
VMI 80-89:
150 szervezet

VMI 70-79:
108 szervezet



2026. Február 17-i állapot szerint.

Audit tapasztalatok – SZEKI megoszlása

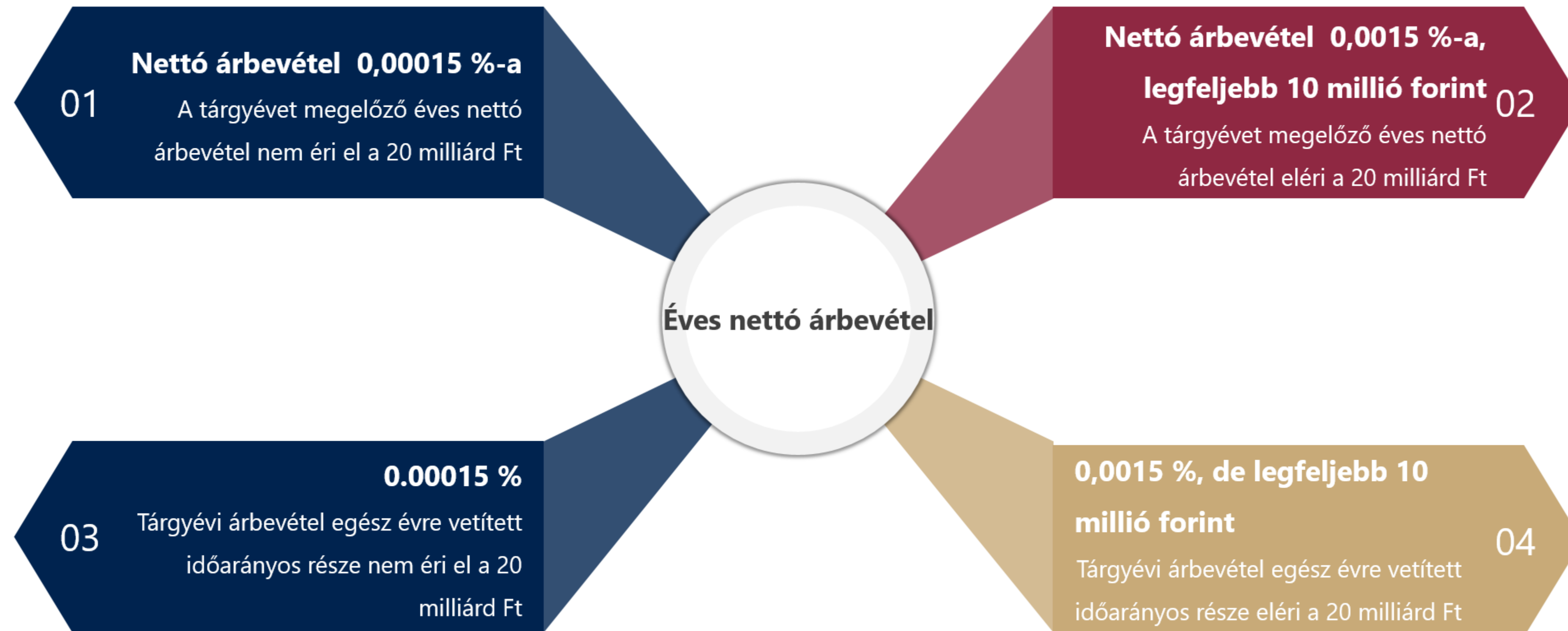


2026. Február 17-i állapot szerint.

Kiberbiztonsági felügyeleti díj



A kiberbiztonsági felügyeleti díj – 2/2025 (I.31.) SZTFH Rendelet



A kiberbiztonsági felügyeleti díj



*: 3,5 milliárd forint alatt nem éri el az 5000 forintot



*: kivéve vállalatcsoportok, melyek esetében maximum 50 millió forint

A minimális és maximális kiberbiztonsági felügyeleti díj



A kiberbiztonsági felügyeleti díj - határidők



Kiberbiztonsági felügyeleti díj kalkulátor

A Hatóság honlapján (www.sztfh.hu) elérhető funkció.

TOVÁBBI OLDALAK

- Kiberbiztonsági tanúsítások
- Kiberbiztonsági felügyelet
- Tudástár
- Kiberbiztonsági felügyeleti díj
- Kriptováltást validálók felügyelete
- Gyakran Ismételt Kérdések

Kiberbiztonsági felügyeleti díj

A kiberbiztonsági felügyeleti díjról szóló 2/2025. (I.31.) rendelet (a továbbiakban: Rendelet) értelmében az SZTFH az érintett szervezeteket 2025. május 31-ig tájékoztatja a felügyeleti díj mértékéről és a megfizetés módjáról. A felügyeleti díj magába foglalja a 2024. évre – 2024. október 18-tól 2024. december 31-ig tartó időszakra – vonatkozó felügyeleti díjat. A 2024. évi díjfizetés alapját a szervezet 2024. évet megelőző évben közzétett utolsó, a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Szt.) szerint beszámolója szerinti nettó árbevétele adja.

A 2025. évre megfizetendő kiberbiztonsági felügyeleti díj számítás alapját a 2025. évet megelőző évben közzétett utolsó, az Szt. szerint beszámolója szerinti nettó árbevétele adja.

A Kiberbiztonsági felügyeleti díj kalkulátor ügyféltájékoztatás elősegítése érdekében készült, az ügyfél által kiszámított összeg kötelező erővel nem bír, erre bíróság, vagy más hatóság előtt megalapozottan hivatkozni nem lehet.



Felügyeleti díj kalkulátor

Tárgyévet megelőző évben közzétett
nettó árbevétel*

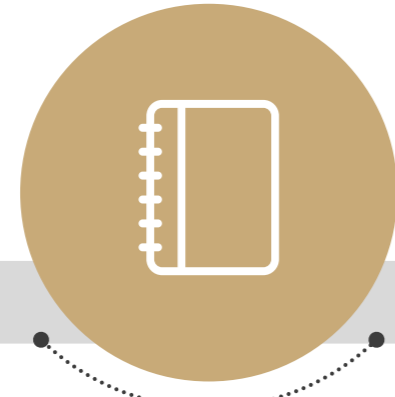
3 500 000 000 Ft

Fizetendő kiberbiztonsági felügyeleti díj

5 000 Ft

Határidők ütemezése amennyiben a szervezet 2025.01.01. előtt kezdte meg működését

2024. január 1.



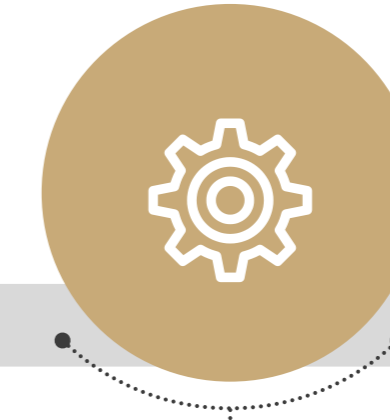
2024. október 18.



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**

Határidők ütemezése 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**

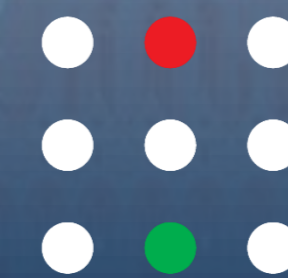
- **Kiberbiztonsági felügyeleti díj megfizetése**

- **Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral**

- **Első kiberbiztonsági audit lefolytatásának határideje**

Köszönöm a figyelmet!

kiberbiztonsag@sztfh.hu



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Az Alaptörvény és a jogalkotásról szóló 2010. évi CXXX. törvény hatályos rendelkezéseivel összhangban tájékoztatjuk, hogy ez az előadásanyag az ügyféltájékoztatás elősegítése érdekében készült, kötelező erővel nem bír, erre bíróság, vagy más hatóság előtt megalapozottan hivatkozni nem lehet.