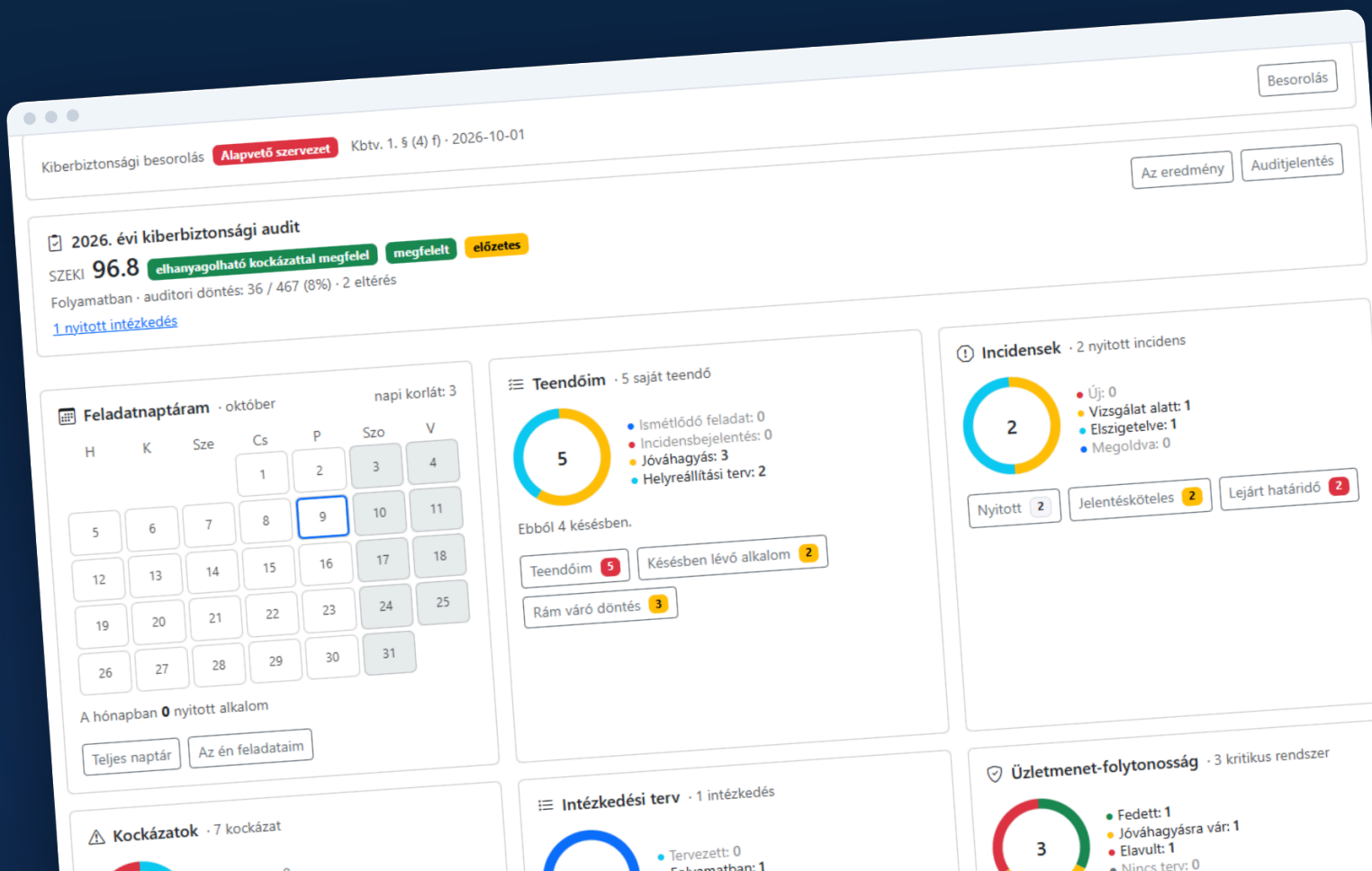
NISNavigator

Termékbemutató
2026

NIS2-megfelelés, ami működik – és bizonyítható.

Egyetlen rendszer a kiberbiztonsági törvény teljes körforgására: a besorolástól a kockázatkezelésen és az incidensek határidőin át a hivatalos audit eredményéig. Minden lépéshez dátum, felelős és visszakereshető nyomvonal tartozik.

- 2024. évi LXIX. törvény (Kbtv.)
- 7/2024. MK rendelet
- 1/2025. SZTFH rendelet
- (EU) 2022/2555 – NIS2



A KIHÍVÁS

A NIS2 nem egyszeri projekt, hanem évről évre ismétlődő kör

A kiberbiztonsági törvény hatálya alá eső szervezeteknek kockázatarányos intézkedéseket kell bevezetniük, jelentős incidensről órákon belül értesíteniük kell a hatóságot, és kétévente független audit méri, hogy mindez a gyakorlatban is működik-e. A felelősség a vezetőé.

19
fejezetes követelménykatalógus, amelynek a szervezetnek meg kell felelnie

24 óra
alatt kell egy jelentős incidensről a korai figyelmeztetést elküldeni

2 év
a kötelező kiberbiztonsági audit gyakorisága az alapvető és fontos szervezeteknél

> **Az auditor nem azt kérdezi, van-e szabályzatuk, hanem azt, hogy működik-e: ki hagyta jóvá, mikor vizsgálták felül, mikor tesztelték, és mi lett az eredmény.**

A NISNAVIGATOR VÁLASZA

A teljes megfelelési kör egyetlen rendszerben

A modulok egymásra épülnek, ezért a rendszer nemcsak tárol, hanem végig is vezet: kockázatot ismert eszközre, tervet ismert szolgáltatásra írhat. A bizonyítás nem külön munka, hanem a mindennapi munka melléktermék.

01
Besorolás
Vonatkozik-e ránk a törvény, alapvető vagy fontos szervezetként?

02
Nyilvántartás
Szolgáltatások, eszközök, beszállítók és tanúsítványok egy helyen.

03
Kockázatelemzés
Értékelés, kezelési terv, MITRE ATT&CK támadási vektorok.

04
Szabályok és jóváhagyás
Verziózott dokumentumtár, vezetői döntés négy szem elvvel.

05
Rendszeres feladatok
Felülvizsgálat, képzés, mentési próba – a rendszer ütemez és emlékeztet.

06
Üzletmenet-folytonosság
Helyreállítási tervek, tesztek, lefedettség és KPI-k.

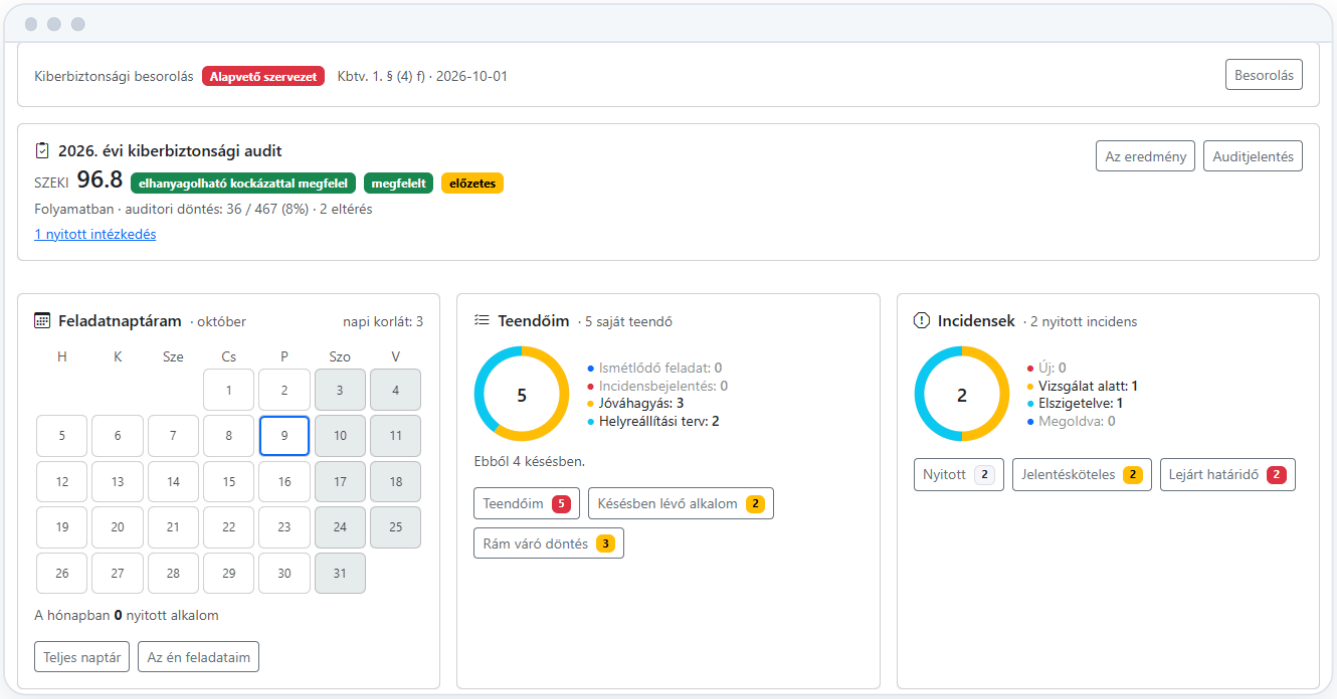
07
Incidenskezelés
24 órás, 72 órás és egyhónapos határidők valós időben.

08
Bizonyítás és audit
Megfelelőségi tábla, SZTFH-módszertan szerinti audit, auditjelentés.

ÁTTEKINTÉS ÉS NAPI MUNKA

Egy képernyő, és látja, hol tart a szervezet

A kezdőlap minden modulnak egy kártyát ad: a diagram megmutatja, miből mennyi van, a gombok pedig pontosan azt a szűrt listát nyitják meg, amelyből a szám származik. Lejárt határidő, elavult terv, jóváhagyásra váró döntés – semmi nem marad rejtve.

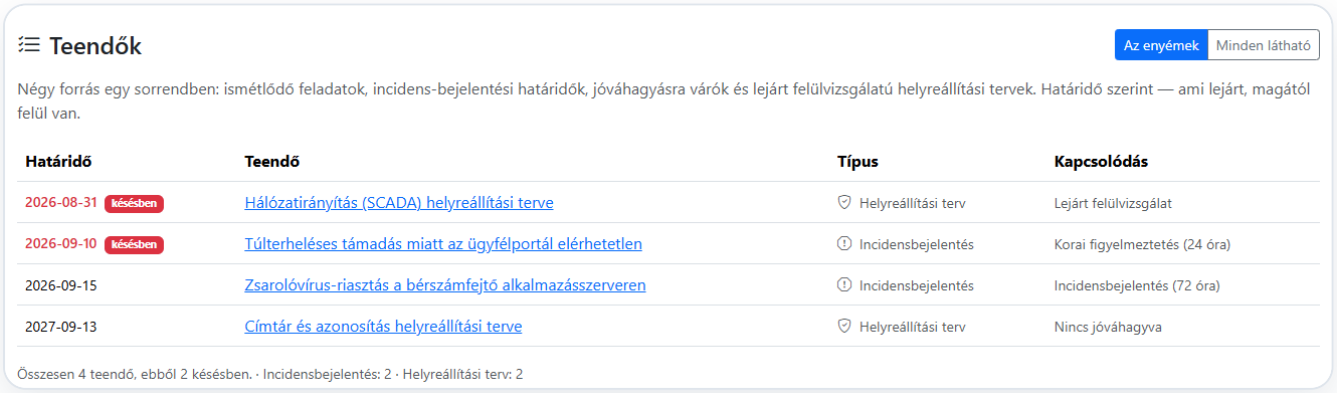


Az áttekintő oldal: besorolás, az aktuális audit indexe, feladatnaptár, teendők és incidensek egy pillantásra – alatta kockázatok, intézkedések, folytonosság, tanúsítványok, eszközök és beszállítók kártyái.

Teendők: egyetlen lista, határidő szerint

Az ismétlődő feladatok, az incidens-bejelentési határidők, a jóváhagyásra váró döntések és a felülvizsgálatra szoruló tervek egy közös listába kerülnek. Ami lejárt, az magától a lista tetejére ugrik.

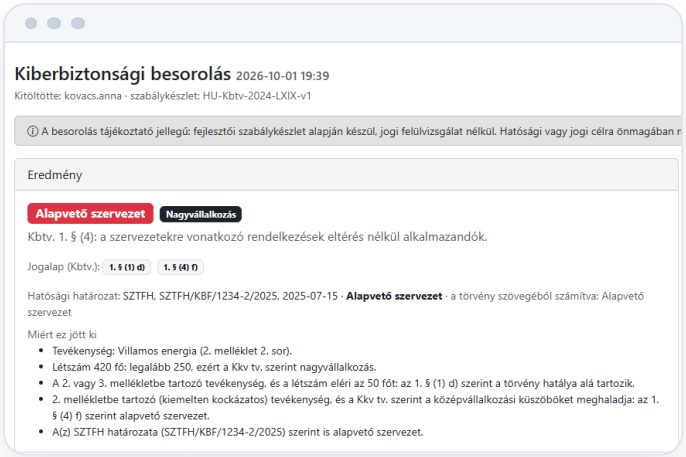
- Napi e-mail összefoglaló a saját teendőkről
- Mindenki a saját felelősségi körét látja



BESOROLÁS ÉS MEGFELELŐSÉG

Tudja meg percek alatt, mit vár el Öntől a törvény

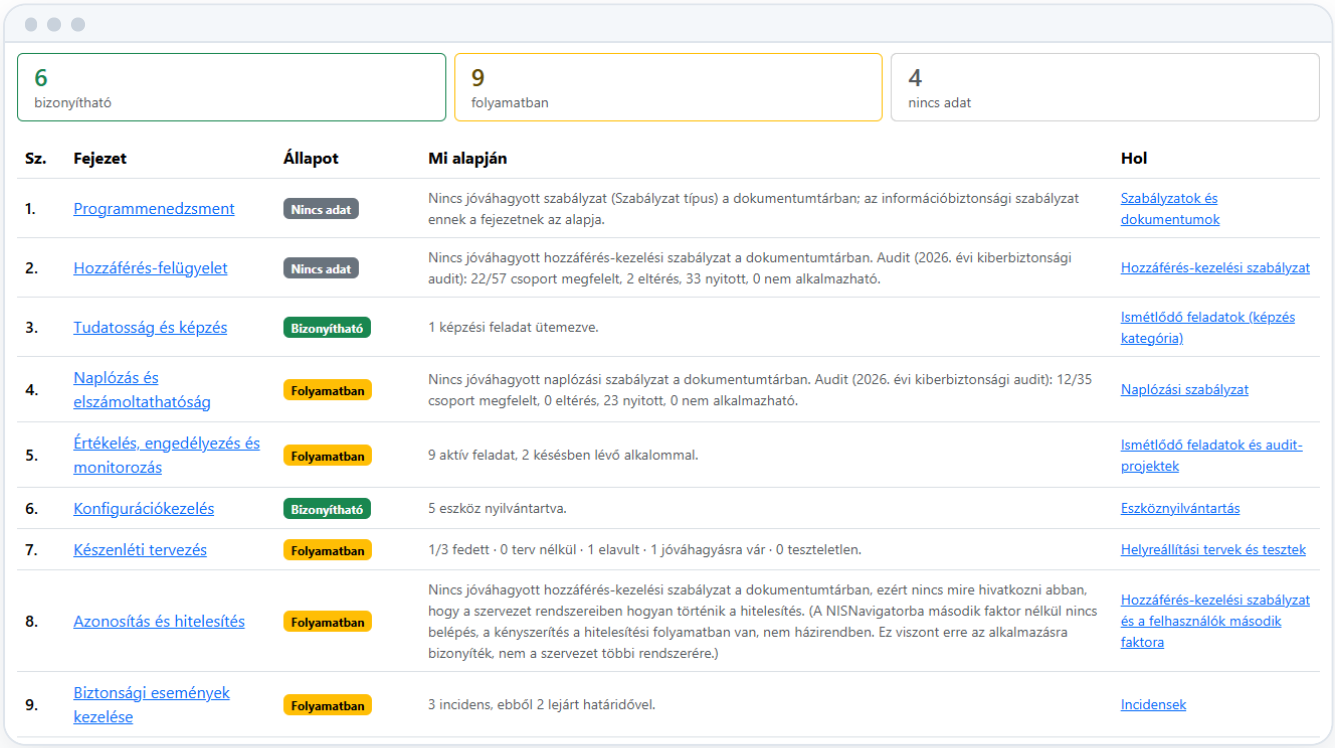
Egy négylépéses kérdőív rögzített jogszabályi küszöbökkel állapítja meg, hogy a szervezet a Kbtv. hatálya alá tartozik-e, és ha igen, alapvető vagy fontos szervezetként, melyik hatályi pont alapján. Az eredmény mellé a rendszer azt is leírja, miért ez jött ki, és mit jelent a gyakorlatban.



- **Indokolt eredmény** – tevékenység, létszám, árbevétel alapján, jogszabályhelyre hivatkozva
- **Konkrét kötelezettségek** – nyilvántartásba vétel, audit, felügyeleti díj határidőkkel
- **PDF-riport** a vezetésnek és a dokumentációhoz
- **Rendszerszintű osztályba sorolás** – 16 szempont alapján, vezetői jóváhagyással

Megfelelőségi tábla: amit az auditor elsőként kér

A 7/2024. MK rendelet követelménykatalógusának mind a 19 fejezetét összeveti a nyilvántartással, és fejezetenként megmondja, van-e mit felmutatni – Bizonyítható Folyamatban Nincs adat –, és pontosan mi alapján. A havi vezetői beszámoló alapja.



KOCKÁZATKEZELÉS

A kockázattól a vezetői döntésig, egyetlen láncban

A törvény szerint minden intézkedésnek kockázatarányosnak kell lennie. A NISNavigator egyben tartja a láncot: mi történhet, mennyire súlyos, mit teszünk ellene, mennyi marad utána, és ki hagyta jóvá.



Egy kockázat adatlapja: inherens és maradványérték, kezelési stratégia, felelős, határidő és a teljes jóváhagyási nyomvonal.

Kockázati mátrix

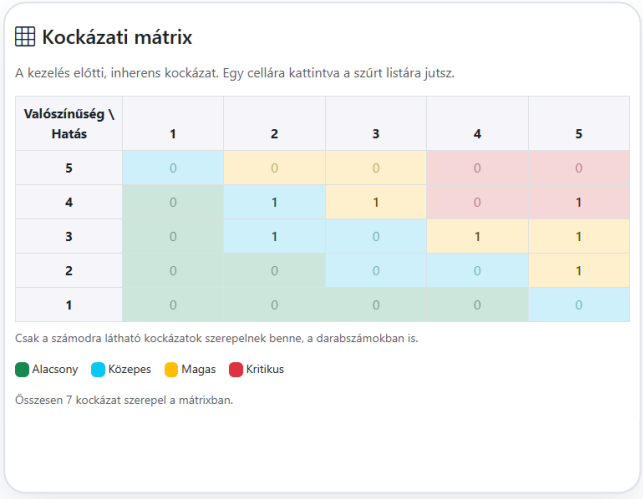
Inherens és maradvány nézet; egy cellára kattintva a szűrt listára jut.

MITRE ATT&CK támadási vektorok

Eszközszintű fenyegetettségi elemzés a nemzetközi technikakatalógus alapján – a kockázatértékelés műszaki megalapozása.

Négy szem elve a jóváhagyásban

Kockázat, szabályzatverzió és helyreállítási terv ugyanazon a jóváhagyási folyamaton megy át; saját beadványát senki nem hagyhatja jóvá.



INCIDENSKEZELÉS

Ha baj van, a rendszer órákra pontosan számol

Jelentős incidensnél a jogszabály órákban méri a teljesítést. A NISNavigator a tudomásszerzés pillanatától számolja a határidőket, e-mailben emlékeztet, és bizonyíthatóan rögzíti, mi, mikor és kinek a döntésével történt.

24 óra
Korai figyelmeztetés

72 óra
Incidensbejelentés

1 hónap
Zárójelentés



Az incidens adatlapja visszaszámlálással, iktatószámmal, állapotkövetéssel és időrendi naplóval.

ÜZLETMENET-FOLYTONOSSÁG

A terv a szándék, a teszt a bizonyíték

Helyreállítási tervek RTO- és RPO-célértékkel, dokumentált helyreállítási tesztek, és egy nézet, amely nem rögzít, hanem a hiányt mutatja: melyik kritikus szolgáltatás mögött nincs érvényes terv.

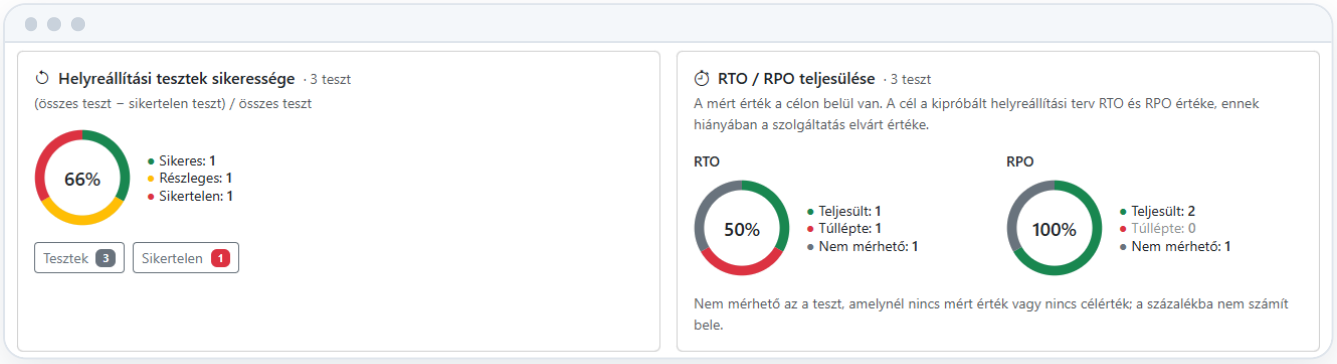


A lefedettségi nézet: a problémás sorok mindig felül, a lejárt felülvizsgálat és az RTO-eltérés pirossal. A tesztek eredményéből a rendszer KPI-ket is számol – erről a következő oldal szól.

MÉRHETŐ FOLYTONOSSÁG

Két szám, ami a helyreállítást méri

Húsz teszt adatlapjából nehéz megmondani, hogy a szervezet jobban vagy rosszabbul áll-e, mint egy éve. A KPI oldal erre felel két mutatóval, választható időszakra (3, 6, 12 hónap vagy a teljes időszak), mindig ugyanazzal a képlettel – így a trend is olvasható.



A KPI oldal: a százalék mellett mindig ott a tesztek száma, és egy kattintással elérhetők a mögöttes próbák.

1. KPI

Helyreállítási tesztek sikeressége

```
(összes − sikertelen) / összes
```

Minden visszatöltési próba és DR-gyakorlat beleszámít. A részleges eredmény nem hiba: a szervezet képes volt helyreállni – azt, hogy elég gyorsan-e, a második mutató méri.

2. KPI

RTO- és RPO-teljesülés

```
mért érték ≤ célérték → teljesült
```

Külön számolva, mert mást jeleznek: a túllépett RTO lassú folyamatra, a túllépett RPO ritka mentésre utal. A célérték a jóváhagyott tervből vagy a szolgáltatás elvárt értékéből jön; a nem mérhető teszt látszik, de nem torzítja a százalékot.

Bevált célértékek induláshoz

≥ 90%
Sikeresség
Évi 8–12 próbánál egy sikertelen még belefér, a második már vizsgálatot indít.

≥ 80%
RTO-teljesülés
A helyreállítási idő sok tényezőtől függ; a tartós túllépés irreális célt jelez.

100%
RPO-teljesülés
A mentés gyakorisága beállítás kérdése – itt nincs tűréshatár.

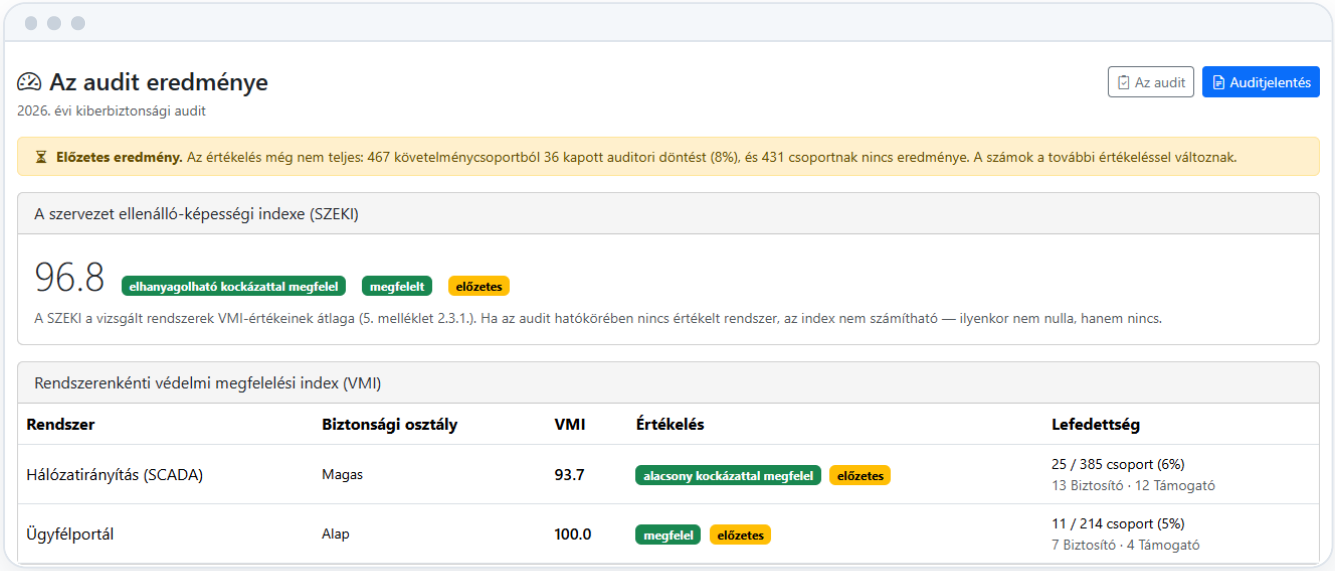
Javasolt negyedéves KPI-áttekintés

1. **Ütemezés** – Ismétlődő feladatként, a visszatöltési próbák után.
2. **Összevetés** – 12 hónapos nézet az előző negyedévhez mérve.
3. **Okfeltárás** – Célon kívül: a mögöttes próbák tapasztalatai.
4. **Intézkedés** – Tervjavítás, reálisabb cél, sűrűbb mentés.
5. **Beszámoló** – A vezetésnek, bizonyítékként csatolva.

KIBERBIZTONSÁGI AUDIT

Auditra készen – az SZTFH módszertana szerint

Az audit projekt összeköti a besorolt rendszereket a követelménykatalógussal, és követelménycsoportonként végigvezet: vonatkozik-e ránk, teljesül-e, és ha nem, mennyire súlyos. A szervezet önértékelése és az auditor megállapítása két külön sávon fut, és soha nem írják felül egymást.



Automatikusan számolt védelmi megfelelési index (VMI) rendszerenként és a szervezet ellenálló képességi indexe (SZEKI).

Audit-előkészítés

Szervezeti kérdőív és díjkalkuláció a már rögzített adatokból – ajánlatkéréshez készen.

Eltérések

Minden tudatos eltérés írásban, indokolva, vezetői jóváhagyással – átadható nyilvántartásban.

Intézkedési terv

Hiányosságból javítás: felelős, határidő, mérföldkövek és bizonyított lezárás.

És ami még a mindennapokat segíti

Ismétlődő feladatok és naptár

Egyszer leírt szabályból ütemezett alkalmak, emlékeztetők és megőrzött bizonyítékok.

Verziózott dokumentumtár

Titkosított tárolás, minden verziónak saját jóváhagyása; mindig tudható, mi volt hatályban.

Beszállítók és ellátási lánc

Kitől függünk, mit vállalt, mikor értékeltük – dokumentumbekéréssel.

Tanúsítványok

Lejárat előtti többlépcsős e-mail figyelmeztetés – nincs több váratlan leállás.

Háttértár-megsemmisítés

A kiszereléstől a fényképekkel igazolt megsemmisítésig követett adathordozók.

Követelménykatalógus

A teljes jogszabályi katalógus kereshető, szűrhető formában – audit nélkül is.

BEÉPÍTETT BIZTONSÁG

A legérzékenyebb adatai jó kezekben

A rendszer a szervezet biztonsági térképét őrzi – ezért maga is a katalógus elvárásai szerint épült.

Kötelező kétlépcsős belépés
Jelszó és hitelesítő alkalmazás, helyreállító kódokkal.

Need-to-know láthatóság
Mindenki csak a sajátját és a hozzá rendeltet látja – adatbázis szinten kikényszerítve.

Lepecsételt audit-napló
Minden művelet sorszámozva; az integritás-ellenőrzés kimutatja a közvetlen beavatkozást.

Titkosítás és védett belépés
Titkosított bizalmas mezők és fájlok, címletiltás jelszótalálgatás ellen, titkosított költöztetőcsomag.

GYORS BEVEZETÉS

Működő megfelelés 90 nap alatt

Bevált sorrend egy 300–500 fős szervezetre – a kézikönyv lépésről lépésre végigvezet.

1–2. hét	**Alapok** – felhasználók, levelezés, első belépés
2–4. hét	**Besorolás** és szolgáltatások RTO/RPO-val
3–6. hét	**Eszközök** – az eszközgazdák rögzítik
5–9. hét	**Kockázatok** és támadási vektorok
7–11. hét	**Szabályzatok** jóváhagyatása
9–13. hét	**Ritmus és folytonosság** – feladatok, tervek, első teszt
13. hét	**Vezetői áttekintés** PDF-riporttal

Mindenkinek a saját szerepe

Rendszergazda
Admin

Felhasználók, beállítások, licenc, audit-napló és hozzárendelések.

Megfelelőségi felelős
ComplianceManager

Besorol, kockázatot, dokumentumot, tervet kezel, jóváhagy, incidenst minősít.

Eszközgazda
AssetOwner

Rögzíti saját rendszereit, ütemezi és teljesíti a feladatokat.

Auditor
Auditor

Mindent lát, semmit nem módosíthat – csak az audit idejére.

Próbálja ki kockázat nélkül

A NISNavigator licenc nélkül is teljes funkcionalitással működik – egy kisebb szervezet vagy egy részleg bevezetéséhez elég. A licenc csak a mennyiségi korlátokat oldja fel; minden funkció az első naptól elérhető.

5 eszköz

5 szolgáltatás

5 felhasználó

A képernyőképek egy kitalált szervezettel (Zöldmező Energia Zrt.) készültek; a nevek és adatok kitaláltak. A besorolás tájékoztató jellegű, jogi felülvizsgálatot nem helyettesít. Az incidensmodul a hatósági bejelentést nem küldi el, de a határidőket számolja és dokumentálja.