# IT-üzemeltetési megfelelés

Amit az audit ellenőriz – nem csak EDR, VPN, MFA....

**Deim Ágoston – Kockaképző**

# A lényeg egy mondatban

Az IT audit - akár a NIS2 - nem csak tűzfalat és EDR-t keres – hanem dokumentált eszközleltárt, licencnyilvántartást, incidens-ticketeket és változásnaplókat is.

**🔍 Az audit bizonyítékot kér – nem csak szabályzatot**

**📋 Az IT-üzemeltetési dokumentáció önálló auditpont**

**⚠️ A „kemény" security eszközök önmagukban nem elegendők**

# Jogi keret – mi vonatkozik Magyarországra

## Kulcsfontosságú jogszabályok:

- 2024. évi LXIX. törvény (Kiberbiztonsági tv.) – hatályos 2025. jan. 1-től
- Felügyeleti hatóság: SZTFH
- Módszertani háttér: NBSZ-NKI (914 intézkedés, NIST SP 800-53 rev5 alapján)

## Kritikus határidők (NIS2):

1. **2025. aug. 31.** → Auditorral szerződés kötelező
2. **2026. jún. 30.** → Első audit elvégzése (2025 előtt indult szervezetek)
3. **2 évente** → Audit megismétlése kötelező

3 biztonsági osztály: Alap | Jelentős | Magas

# Mit ellenőriz az auditor? – Az 5 legfontosabb IT-üzemeltetési terület

Eszközleltár (HW/SW) — CM-8: Naprakész, dokumentált leltár minden rendszerelemről, felelős-hozzárendeléssel

Licencmenedzsment — CM-10: Engedélyezett vs. ténylegesen használt licencszám nyilvántartása

Konfigurációkezelés — CM-2/3: Alapkonfiguráció-dokumentum + változásnapló

Incidenskezelés — IR: Ticketek, eszkalációs mátrix, 24/72/30 órás hatósági bejelentés

Naplózás & patch-állapot — AU/SI: Admin-tevékenység naplók, patch-összesítő, nyitott CVE-k

# Eszközkategóriák és NIS2-lefedettség

| Eszközkategória | NIS2 területek | Lefedettség |
| --- | --- | --- |
| ITAM-eszköz | CM-8 leltár, CM-10 licenc, CM-11 szoftverkorlátozás | ✅ Erős |
| Helpdesk / ITSM | IR incidenskezelés, MA karbantartás, AU napló | ✅ Erős |
| Felhasználói aktivitás-monitoring | AU naplózás, AC hozzáférés | ✅ Erős |
| Patch management / Vulnerability scanner | SI sértetlenség, RA kockázat | ⚠️ Leggyakrabban hiányzik |
| GRC / ISMS-platform | RA kockázat, SR ellátási lánc, PL tervezés | ⚠️ Részleges / külön eszköz |
| Backup / DR platform | CP üzletmenet-folytonosság | 🔲 Teljesen különálló |

A patch management a leggyakrabban hiányzó elem az auditon.

# A 6 leggyakoribb hiányosság az auditon

### 🔴 Patch-/sérülékenységkezelés hiánya

A leggyakrabban hiányzó elem; az ITAM önmagában nem helyettesíti a dedikált vulnerability scannert.

### 🔴 ISMS/GRC-dokumentáció hiánya

Kockázati nyilvántartás, SoA és szabályzatkezelés külön eszközt vagy strukturált folyamatot igényel.

### 🟠 Ellátási lánc / szállítói kockázat

Nincs elterjedt KKV-eszköz; jellemzően manuális nyilvántartás szükséges.

### 🟠 Backup/DR-dokumentáció

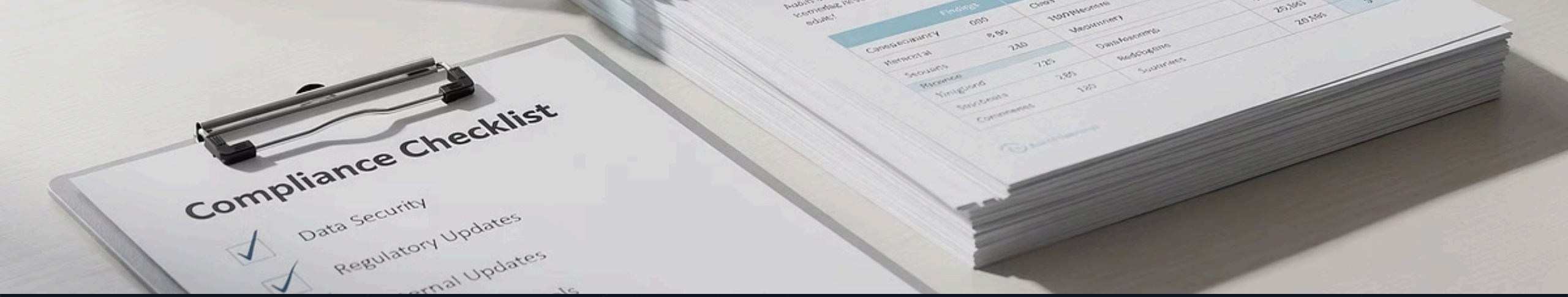
Az ITAM azonosítja a kritikus eszközöket, de a DR-terv és tesztek külön területet képeznek.

### 🟡 Hatósági incidens-bejelentés

A 24/72/30 órás SZTFH-bejelentés jellemzően manuális folyamat – eljárásrendben kell szabályozni.

### 🟡 Jogosulatlan szoftver tiltásának kikényszerítése

A CM-7/CM-11 technikai tiltás bizonyítékát kéri, nem csak a szabályzat meglétét.




# Mit kér az auditor konkrétan? – Bizonyíték-lista (I.)

- **Eszközleltár (HW)**
  exportált, dátummal ellátott lista; felelős, típus, életciklus vége
- **Szoftverleltár**
  telepített szoftverek listája gépenként, rendszeresen karbantartva
- **Licencleltár**
  engedélyezett vs. ténylegesen használt licencszám
- **Alapkonfiguráció-dokumentum**
  verziószámmal, egy vagy több rendszertípusra

# Mit kér az auditor konkrétan? – Bizonyíték-lista (II.)

- [ ] **Változásnapló**
  HW/SW konfiguráció-változások naplója dátumokkal
- [ ] **Incidens-napló / ticketek**
  legalább 12 hónapra visszamenőleg
- [ ] **Admin hozzáférési napló**
  privilegizált műveletek, visszakereshető formában

# Mit kér az auditor konkrétan? – Bizonyíték-lista (III.)

- [ ] **Patch-állapot-kimutatás**
  hány eszköz karbantartott, milyen CVE-k nyitottak
- [ ] **Backup/DR-terv és legutóbbi teszt dokumentációja**
- [ ] **Tudatossági képzés nyilvántartása**
  ki, mikor, milyen képzésen vett részt

# Biztonsági osztály szerint – mikor elég az ITAM?

| Biztonsági osztály | Tipikus profil | ITAM elegendő? | Mi kell még? |
|---|---|---|---|
| Alap | Kis szervezet, alacsony kockázat | ✅ Lényegében igen | Backup/DR-dokumentáció, manuális kockázatkezelés, awareness-képzés |
| Jelentős | Közepes szervezet, fontosabb szektor | ⚠️ Részben | Dedikált patch/VM-eszköz, SIEM/Syslog, formális ISMS-folyamat |
| Magas | Alapvető szolgáltató, kritikus infrastruktúra | ❌ Nem elegendő | Teljes SOC-képesség (SIEM/XDR), automatizált patch, GRC-platform, formális ISMS, IR-terv teszteléssel |

# Mit érdemes használni?

### A szervezet mérete és erőforrásai határozzák meg

- pénzügyi
- emberi

### Kereskedelmi eszközök

- Előnyök: kész riportok, adatok feldolgozása, célorientáltság
- Hátrányok: pénzügyi erőforrást igényel, némelyik megköti a lehetőségeket

### Open source eszközök

- Előnyök: licencdíj-mentesség, testreszabhatóság
- Hátrányok: a testreszabás gyakran nehézkes, és kódmódosítást igényelhet vagy nagyon bonyolult a használat

### Operációs rendszer szkriptek (pl. PowerShell, bash)

- Előnyök: teljesen testre szabható, csak annyit csinál, ami szükséges
- Hátrányok: limitációk a lefedett területekben, külső eszközökön múlik az összehasonlítás (pl. táblázatkezelő, SQL ritkán használt)

# Összefoglalás – 3 kulcstanulság

**Egy IT audit az IT-üzemeltetési dokumentációt ugyanolyan szigorúan ellenőrzi, mint a biztonsági eszközöket.**

**A patch-/sérülékenységkezelés a leggyakrabban hiányzó elem – ezt külön kell kezelni.**

**A megfelelés bizonyítékon alapul: naprakész leltár, ticketek, naplók és dokumentált folyamatok nélkül nincs sikeres audit.**