

Új rendszer bevezetése, rendszerkivezetés, EIR-ek változásai auditok között

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/32

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.08.28	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Az elektronikus információs rendszerek környezete az audit lezárását követően is folyamatosan változik. Új rendszer bevezetése, meglévő rendszer jelentős módosítása, más rendszerrel történő integrációja vagy kivezetése nem tekinthető kizárólag informatikai feladatnak: ezek olyan szervezeti változások, amelyek információbiztonsági, adatvédelmi, üzemeltetési, beszerzési, szerződéses és üzletmenet-folytonossági következményekkel járhatnak.

A szervezetnek ezért szabályozott változáskezelési eljárást kell működtetnie. A változtatások magukba foglalják az érintett rendszer azonosítását, biztonsági és működési szempontból történő értékelését, szükség szerinti tesztelését, illetve a jóváhagyási folyamatot is

A jóváhagyási folyamatba – a változás jellegétől függően – be kell vonni az üzleti vagy szakmai folyamatgazdát, az informatikai vezetőt vagy üzemeltetőt, az információbiztonsági felelőst, az adatgazdát, az adatvédelmi tisztviselőt, valamint a kockázat elfogadására jogosult vezetőt.

A vezetés feladata annak biztosítása, hogy új vagy lényegesen módosított rendszer ne kerülhessen ellenőrizetlenül éles üzembe, illetve rendszer ne kerülhessen kivezetésre dokumentált lezárás nélkül. A cél nem indokolatlan adminisztráció létrehozása, hanem annak igazolhatósága, hogy a szervezet az auditált állapot változásait folyamatosan, kockázatarányosan és ellenőrzött módon kezeli.

2. A VIZSGÁLANDÓ KÉRDÉS

Mik a teendők új rendszer bevezetése, rendszerkivezetés, EIR-ek változásai auditok között? Milyen folyamatok szükségesek, mely területeket, és azok dokumentációt érintheti a változás?

3. VÁLASZ

3.1 Változások által érintett területek, dokumentációl

Egy új rendszer be- és kivezetése, az EIR változtatása (az EIR-t alkotó rendszerelemek változásai) az alábbi területeket és a hozzájuk kapcsolódó szabályzatokat, eljárásendeket befolyásolhatják:

Érintett követelménycsalád	Érintett dokumentum(ok)	Tipikusan érintett kontrollok (rendszerfüggő)
Információbiztonsági szabályozás	Információbiztonsági szabályzat	- Elektronikus információs rendszerek nyilvántartása
Hozzáférés-felügyelet	Szabályzat. és eljárásrend, jogosultsági mátrix	- Fiókkezelés (pl. új MFA be- és kivezetése) - Távoli hozzáférés

Érintett követelménycsalád	Érintett dokumentum(ok)	Tipikusan érintett kontrollok (rendszerfüggő)
		- Vezetéknélküli hozzáférés - Külső rendszerek használata
Tudatosság és képzés	Képzések anyagai	- Üzemeltetők és érintett rendszerfelhasználók képzése
Naplózás és elszámoltathatóság	Naplózási eljárásrend	- Naplózható események - Naplózandó események felülvizsgálata
Biztonságértékelés	Biztonságértékelési terv, Engedélyezési dokumentáció	- KPI-k - Monitorozási paraméterek - Belső rendszerkapcsolatok - Engedélyezés
Konfigurációkezelés	Alapkonfiguráció, szabályzat és eljárásrend	- EIR paraméterei - Egységes biztonsági beállítások - Legszűkebb jogosultság - Rendszerelem leltár
Üzletmenet-folytonosság	BCP, DRP, Mentési rend	- Helyettesítő intézkedések - Alternatív helyszín - Folyamatos működésre felkészítő képzés - Tesztelés - EIR mentései - Helyreállítás és újraindítás
Azonosítás és hitelesítés	Szabályzat és eljárásrend, Azonosítók és hitelesítő eszközök nyilvántartása	- Felhasználók azonosítása - Hitelesítő eszközök kezelése
Karbantartás	Szabályzat és eljárásrend	- Szabályozott és távoli karbantartás
Tervezés	Rendszerbiztonsági terv	- Biztonsági osztályba sorolás - EIR paraméterek
Kockázatkezelés	Kockázatelemzés	- Kockázatok módosítása - Sérülékenységek kezelése

Érintett követelménycsalád	Érintett dokumentum(ok)	Tipikusan érintett kontrollok (rendszerfüggő)
Rendszer és kommunikáció védelem	Szabályzat és eljárásrend	- Határok védelme - Kriptográfiai kulcsok kezelése - Folyamatok elkülönítése
Rendszer- és információsértetlenség	Szabályzat és eljárásrend	- Hibajavítás - Kártékony kódok elleni védelem - EIR monitorozása
Rendszer- és szolgáltatásbeszerzés	Szerződés, üzemeltetési dokumentációk,	- Biztonsági paraméterek - SLA-k meghatározása - Felhasználói, adminisztrátori leírások

Mint a táblázatból kiderül, egy EIR megváltozása, be és kivezetése, szinte az összes felsőbb szintű és jelentős számú alacsonyabb szintű dokumentum megváltoztatásával járhat, ezért érdemes ezeket minden egyes esetben önálló folyamatként kezelni. Ez alól akkor lehet eltérni, ha a módosítás a normál konfigurációkezelési folyamat részeként értelmezhető. Például egy meglévő szakrendszer üzletileg indokolt funkció bővítésénél, elképzelhető, hogy a jogosultság mátrixot frissíteni kell, de az alapkonfiguráció, az eszközlétár, a monitorozás stb. nem fog változni, hiszen alapesetben az már beállításra került az adott szakrendszerhez.

3.2 Új rendszer bevezetés

3.2.1 Mikor beszélünk új rendszer bevezetéséről

A gyakorlatban akkor célszerű új rendszerként kezelni egy megoldást, ha:

- önálló szervezeti vagy üzleti feladatot támogat;
- saját felhasználói és jogosultsági körrel rendelkezik;
- önálló adatállománya vagy adatbázisa van;
- más rendszerekkel interfészekon keresztül kommunikál;
- saját üzemeltetési, mentési, naplózási vagy helyreállítási rendje van;
- önálló szolgáltató vagy beszállító biztosítja;
- a kiesése vagy kompromittálódása külön értékelhető szervezeti hatást okozna.

Így például egy felhőalapú ügyviteli rendszer, HR-rendszer, SaaS-szolgáltatás, beléptetőrendszer vagy termelésirányítási megoldás akkor is lehet új EIR, ha a szervezet egyetlen szervert sem vásárol hozzá.

Ezzel szemben, mint ahogy előzőekben említésre került, egy meglévő rendszer kisebb verziófrissítése, új riportja vagy korlátozott funkcióbővítése jellemzően nem új EIR, hanem a meglévő EIR változása. Az elhatárolási döntést azonban dokumentálni kell.

3.2.2 Javasolt bevezetési folyamat

1. Igény bejelentése

Cél, funkció, felhasználók, kezelt adatok és indokoltság meghatározása:

- mire szolgál az új rendszer;
- mely folyamatokat támogatja;
- ki lesz a rendszer szakmai tulajdonosa;
- kik és hányan használják;
- milyen adatokat kezel;
- kezel-e személyes, különleges, üzleti titkot vagy más érzékeny adatot;
- mely más rendszerekkel fog kapcsolatot létesíteni;
- milyen következménye lenne a rendszer kiesésének;
- ki végzi a fejlesztést, üzemeltetést és támogatást;
- hogyan lehet később az adatokat kinyerni és a szolgáltatást megszüntetni.

2. Előzetes vizsgálat

Annak eldöntése, hogy új rendszerről vagy meglévő rendszer változásáról van-e szó. Utóbbi esetben a folyamat konfiguráció kezelés részeként kezelendő.

3. Hatás-és kockázatértékelés

Bizalomassági, sértetlenségi, rendelkezésre állási, adatvédelmi és működési kockázatok felmérése:

- a rendszer kiesésének hatása a szervezet működésére;
- az adatvesztés vagy jogosulatlan adatmódosítás következménye;
- a kezelt adatok jogosulatlan megismerésének hatása;
- a rendszer kapcsolódása más, kritikus jellegű EIR-ekhez;
- a szolgáltatótól, felhőszolgáltatástól vagy külső interfésztől való függőség.

4. Követelmények meghatározása

Biztonsági, üzemeltetési, adatvédelmi és szerződéses követelmények rögzítése:

- egyedi felhasználói azonosítás;
- szerepköralapú, legkisebb jogosultság elvén működő hozzáférés;
- adminisztrátori hozzáférések elkülönítése;
- MFA alkalmazása;
- jelszó- és hitelesítőeszköz-kezelés;
- titkosított adatátvitel és szükség szerint titkosított adattárolás;
- naplózás és a naplókhoz való szervezeti hozzáférés;
- monitorozás és riasztások;
- biztonsági mentés, visszaállítás és helyreállítás;
- sérülékenység- és javításkezelés;

- külső adattárolás szerződés megszűnésekor az adatok visszaadása és törlése.

5. Lehetséges megoldások és szolgáltatók értékelése, a megoldás kiválasztása

A kiválasztás során a szervezetek szempontjai eltérőek lehetnek, más preferenciákat helyezhetnek előtérbe, de az alábbi szempontokat érdemes figyelembe venni:

- funkcionális megfelelés;
- integrálhatóság a meglévő rendszerekkel;
- információbiztonsági követelmények teljesíthetősége;
- hozzáférés-kezelés és MFA támogatása;
- naplózási és monitorozási lehetőségek;
- mentési, helyreállítási és adatexportálási lehetőségek;
- felhőszolgáltatás és alvállalkozók igénybevétele;
- sérülékenység- és javításkezelés;
- rendelkezésre állás, támogatás és SLA;
- licenelési és teljes életciklusköltség;
- a szolgáltató pénzügyi, szakmai és kiberbiztonsági megbízhatósága;
- a rendszer támogatásának várható időtartama.

6. Kialakítás és tesztelés

A rendszer kiválasztása és beszerzése után a kialakítás és a tesztelés következik, az alábbi szempontok figyelembevételével:

- biztonságos alapkonfiguráció meghatározása (portok, protokollok, szolgáltatások, hálózati címek, kapcsolatok)
- környezet elkülönítése (fejlesztő, teszt, illetve éles)
- hozzáférések kialakítása
- hálózati rendszerkapcsolatok dokumentálása
- naplózás és monitorozás kialakítása, tesztelése
- mentés és helyreállítás kialakítása és tesztelése
- frissítések és sérülékenységek kezelése
- funkcionális tesztelés
- jogosultsági tesztelés
- naplózási, riasztási tesztelés
- üzemeltetési, adminisztrátori dokumentáció ellenőrzése

7. Használatbavételi döntés

A megfelelés, hiányosságok és fennmaradó kockázatok vezetői értékelése:

- A Rendszergazda igazolja az üzemeltethetőséget, integrációt, mentést és helyreállíthatóságot.

- Az Információbiztonsági felelős véleményezi a biztonsági követelmények teljesülését és a fennmaradó kockázatokat.
- Az Adatvédelmi tisztviselő személyes adatok kezelése esetén adatvédelmi véleményt ad.
- A Szervezeti egység/HR vezető- vagy adatgazda, jóváhagyja a hozzáférési és adatkezelési rendet.
- A Szervezet vezetője vagy kijelölt vezető dönt a használatbavételről és szükség esetén a fennmaradó kockázat elfogadásáról.

8. Szervezeti dokumentáció aktualizálása

Mint a 3.1 pont alatti táblázatban látható, egy új rendszer bevetése során jelentős mennyiségű dokumentumot kell frissíteni, amely az szabályzatokban meghatározott személyek (információbiztonsági felelős, rendszergazda, informatikai vezető, stb...) feladata

3.3 Meglévő rendszer kivezetése

A meglévő EIR kivezetése akkor megfelelő, ha a rendszer működése ugyan megszűnik, de a megőrzendő adatok továbbra is hozzáférhetők és védettek maradnak, miközben nem maradnak vissza aktív fiókok, interfészek, szolgáltatói hozzáférések vagy ellenőrizetlen adatmásolatok.

A rendszer egyszerű kikapcsolása tehát még nem rendszerkivezetés.

Javasolt kivezetési folyamat

1. Kivezetési igény

A kivezetés oka, tervezett időpontja és a helyettesítő megoldás meghatározása:

- a kivezetendő EIR megnevezése és azonosítója;
- a kivezetés oka;
- a tervezett kivezetési időpont;
- a helyettesítő rendszer megnevezése (ha van ilyen);
- a rendszer szakmai tulajdonosa;
- az üzemeltetésért felelős személy vagy szolgáltató;
- az érintett szervezeti egységek és felhasználók;
- a rendszerben kezelt adatok fő csoportjai;
- a kapcsolódó rendszerek és szolgáltatók;
- az alkalmazandó megőrzési kötelezettségek;

2. Hatásvizsgálat

Folyamatok, adatok, felhasználók, kapcsolatok és függőségek felmérése:

- mely folyamatok használják a rendszert;
- mely szervezeti egységeket érinti a leállítás;
- lesz-e olyan feladat, amely támogatás nélkül marad;

- szükséges-e átmeneti manuális eljárás;
- mely felhasználókat és külső partnereket kell értesíteni;
- szükséges-e az új rendszer használatára vonatkozó oktatás (ha lesz ilyen).

3. Kivezetési terv

Archiválás, leállítás, adatmigráció (ha másik rendszer kerül bevezetésre) és felelősségek, illetve az alábbi feladatok megtervezése:

- archiv adatok tárolása és védelme
- leállítás ütemezése
- feladatok és felelősök megnevezése

4. Adatok kezelése

Az adatcsoportokat szelektálni kell és dönteni kell a további sorsukról. Ez lehet archiválás, törlés, vagy másik rendszer esetében migrálás. Amennyiben az adatok megőrzésre kerülnek, gondoskodni kell arról, hogy:

- a fájlformátum később is olvasható legyen;
- az adatok értelmezéséhez szükséges metaadatok rendelkezésre álljanak;
- az adatokhoz csak jogosult személyek férjenek hozzá;
- a hozzáférés naplózható legyen;
- az archivált adatok sértetlensége ellenőrizhető legyen;
- a szükséges titkosítási kulcsok rendelkezésre álljanak;
- ne kelljen a teljes, már nem biztonságos rendszert újraindítani egyetlen adat visszakereséséhez.

5. Adatmigráció elvégzése (másik rendszer esetén)

Ha az adatok másik rendszerbe kerülnek át, ellenőrizni és dokumentálni kell:

- a migrálandó adatok körét;
- a rekordok számát és teljességét;
- az adatmezők megfeleltetését;
- az adatok sértetlenségét;
- a jogosultságok megfelelő átvitelét;
- az időbélyegek, státuszok és kapcsolatok megmaradását;
- az adatátadás titkosítását;
- a hibás, hiányzó vagy duplikált rekordokat;
- a migráció közben létrejött ideiglenes állományokat.

6. Átmeneti és párhuzamos működés (másik rendszer esetén)

Új rendszerre történő áttéréskor indokolt lehet a régi és az új rendszer átmeneti párhuzamos működtetése. Ennek azonban:

- előre meghatározott kezdő és záró időponttal kell rendelkeznie;

- szabályozni kell, melyik rendszer az elsődleges;
- meg kell akadályozni az eltérő adatok párhuzamos keletkezését;
- meg kell határozni az adatszinkronizáció módját;

A határidő nélküli párhuzamos működés jellemzően oda vezet, hogy a régi rendszer informálisan tovább él, miközben már nem kap megfelelő frissítést és felügyeletet, ami komoly információbiztonsági veszélyeket rejt magában. Lásd Magyar Államkincstár kibertámadása, amikor is (legalábbis rendelkezésre álló adatok szerint) egy régi, nem használt, ezáltal nem felügyelt, de éles rendszer került kompromitálásra.

7. Technikai leállás

A technikai kivezetés során legalább a következőket kell elvégezni:

- hozzáférési fiókok(felhasználói/adminisztrátori/technikai) törlése, külső vagy szolgáltatói hozzáférések, tanúsítványok, SSH kulcsok, VPN hozzáférések megszüntetése
- rendszerkapcsolatok megszüntetése (interfészek, tűzfalszabályok eltávolítása, fájmegosztások megszüntetése, monitorozási és naplózási feladatok kivezetése, mentési feladatok leállítása)
- infrastruktúra kezelése (licenszek felszabadítása, eszközök selejtezése vagy újrafelhasználása, adathordozók biztonságos törlése vagy megsemmisítése, eszköznyilvántartások frissítése)

8. Szervezeti dokumentáció aktualizálása

Mint a 3.1 pont alatti táblázatban látható, egy új rendszer bevetése során jelentős mennyiségű dokumentumot kell frissíteni, amely az szabályzatokban meghatározott személyek (információbiztonsági felelős, rendszergazda, informatikai vezető, stb...) feladata

3.4 EIR összetételének megváltoztatása

Ez az eset az **EIR konfigurációjának és rendszerelem-leltárának változása**. Nem új EIR jön létre, és a teljes EIR sem kerül kivezetésre, hanem megváltozik annak műszaki összetétele, határa, kapcsolatrendszere vagy működési képessége. Itt az a döntő kérdés, hogy a rendszerelem hozzáadása vagy kivétele milyen biztonsági, működési és besorolási hatást okoz az egész EIR-re.

A folyamatok hasonlóak a korábbiakhoz, de az adott EIR szempontjából kell elvégezni a következő lépéseket:

1. Hatásvizsgálat

Biztonsági, működési, adatvédelmi és üzletmenet-folytonossági hatások értékelése

2. Besorolás felülvizsgálata

Annak eldöntése, hogy változik-e az EIR biztonsági osztálya.

3. Jóváhagyás

Az IT, az IBF, a rendszer- vagy folyamatgazda és szükség esetén a vezető jóváhagyása.

4. Kockázatelemzés

Kockázatelemzés frissítése.

5. Dokumentálás

Rendszerbiztonsági terv, BCP, DRP egyéb kapcsolódó folyamatok frissítése.

3.5 Auditorok és hatóság értesítése

Új rendszer bevezetése, EIR összetételének változása, a rendszerek átcsoportosítása során sem kell értesíteni sem volt auditort vagy hatóságot. Az audit és a hatóságok szempontjából az a fontos, hogy a következő auditra az új rendszerkörnyezetet definiáló EIR csoportosítással, besorolással és a megfelelő szabályozással menjen a szervezet.

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 1/2025 (I.31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról