Tikos Anita | főosztályvezető

Mamira Zoltán | osztályvezető

Informatikai felügyeleti főosztály

MNB | Felügyeleti Akadémia | 2026

MINI-DORA SZAKMAI NAP

1. BLOKK

KRITIKUS VAGY FONTOS FUNKCIÓ

ÉRTELMEZÉSE ÉS ALKALMAZÁSA

Mamira Zoltán

AZONOSÍTÁS

Feltérképezés célja

1 Üzleti funkciók

Kritikus vagy fontos / minden egyéb

2 Feladatok- és felelősségek köre

Irányítás és végrehajtás rendszere

3 Erőforrások

Eszköz, szolgáltatás, folyamat, adat stb.

4 Kockázati függőségek

Kitettség és kapcsolatok feltérképezése

DORA

8. CIKK AZONOSÍTÁS

Feltérképezés és osztályozás

Üzleti funkciókkal való egyértelmű összerendelés

Adatok és rendszerek osztályozása

IKT-kockázati források és kezelésük

Harmadik fél szolgáltatók

Eszköz- és vagyonelem-nyilvántartások

Elavult rendszerek

KRITIKUS VAGY FONTOS FUNKCIÓ

DORA

Fokozott kontroll területek

- Megerősített **azonosítás, osztályozás** és külön jelölt, naprakész nyilvántartás
- Szigorúbb **BIA** és rögzített **RTO/RPO** célértékek
- Magasabb szintű **redundancia**, kapacitás és erőforrás-biztosítás
- Szigorított **logikai és fizikai elkülönítés**
- Kiemelt **mentési** és visszaállítási rend (gyakoribb, elkülönített, tesztelt)
- Szigorúbb **hozzáférés**-kezelés (legkisebb jogosultság, erős hitelesítés, rendszeres review)
- Fokozott **naplózás**, monitorozás és valós idejű riasztás
- Prioritásos **sérülékenység**- és javításkezelés rövidebb határidőkkel
- Gyorsított és részletesebb **incidenskezelési** folyamatok
- Gyakoribb és mélyebb reziliencia **tesztelés** kritikus forgatókönyvekkel
- **Külső IKT-szolgáltatók**nál szigorított szerződéses, felügyeleti és kilépési követelmények

KRITIKUS VAGY FONTOS FUNKCIÓ FOGALOM

DORA

3. cikk

22. pont

„kritikus vagy fontos funkció”

(critical or important function – „**CIF**”):

- olyan funkció, amelynek zavara lényegesen rontaná a pénzügyi szervezet pénzügyi teljesítményét, vagy szolgáltatásai és tevékenységei megbízhatóságát vagy folytonosságát, vagy
- az említett funkció kiesése, hibás vagy meghiúsult működése lényegesen rontaná a pénzügyi szervezet képességét az engedélyében foglalt feltételek és kötelezettségek, valamint
- a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt egyéb kötelezettségei folyamatos teljesítésére.

FUNKCIÓ FOGALMA

FUNKCIÓ FOGALMA

DORA019 – 2959
Q&A EIOPA
válasz

A DORA szándékosan **nem ad taxatív definíciót** a „funkció” fogalmára, ennek célja a rugalmasság biztosítása, hogy a pénzügyi szervezetek:

- **üzleti modelljükhöz**,
- **szervezeti struktúrájukhoz**,
- **belső taxonómiájukhoz** igazodva határozhassák meg funkcióikat.

Mit kell funkción érteni?

- **tevékenységek**,
- **szolgáltatások**,
- **folyamatok vagy műveletek**,
- illetve ezek **csoportjai (clusterei)**

Funkciók típusai:

- **alaptevékenységekhez** kapcsolódó funkciók
- **támogató funkciók**, amelyek az alaptevékenységek működését teszik lehetővé

Ezek közül kell kijelölni:

- a kritikus vagy fontos funkciókat

Üzleti és pénzügyi hatás

- közvetlen hatás a pénzügyi teljesítményre
- szolgáltatások megbízhatóságának romlása
- üzletmenet-folytonosság sérülése

Működési és szolgáltatási kockázat

- szolgáltatás kiesése vagy hibás működése
- ügyfélkiszolgálás és működési stabilitás romlása
- engedélyes tevékenység megszakadása

Szabályozói és engedélyezési megfelelés

- engedélyben foglalt feltételek nem teljesítése
- jogszabályi kötelezettségek megsértésének kockázata
- felügyeleti és reputációs következmények

- **A szabályzat tartalmazza** (vagy egyértelműen hivatkozza) a CIF támogatottság megállapításának módszertanát, valamint az értékelés elvégzésének és felülvizsgálatának rendjét. ((EU) 2024/1773 rendelet 3. cikk (2))
- A besorolás a szerződéses megállapodások életciklus dokumentációjában egységesen rögzítésre kerül. ((EU) 2024/1773 rendelet 4. cikk e) pont)
- A CIF besorolás kötelező a szerződéskötést megelőzően és lényeges módosítás esetén ismételten elvégzendő. ((EU) 2024/1773 rendelet 5. cikk (1)–(2); 4. cikk b) pont)
- **A módszertannak ki kell terjednie:**
  - dokumentált összerendelés „IKT szolgáltatás → támogatott üzleti funkció, szolgáltatás → CIF státusz”;
  - teszt annak értékelésére, hogy a szolgáltatás igénybevétele esetén a támogatott a funkció zavara rontaná a pénzügyi teljesítményt vagy a szolgáltatások, tevékenységek megbízhatóságát vagy folytonosságát, illetve a megfelelési képességet. ((EU) 2022/2554 rendelet 3. cikk 22. pont)

A **„lényegesség” megítélése** a digitális működési reziliencia stratégiában **rögzített IKT-kockázati toleranciaszinthez** és az IKT-zavarok hatástűréséhez igazodik, és ezt a módszertan igazolható módon felhasználja a CIF-döntés meghozatalában. ((EU) 2022/2554 rendelet 6. cikk (8) b))

CIF-ET TÁMOGATÓ TPP

„A szabályzatba bele kell foglalni azt a módszertant, amellyel meghatározható, hogy mely IKT-szolgáltatások támogatnak kritikus vagy fontos funkciókat.”

TIPIKUS HIBÁK A CIF MINŐSÍTÉSI GYAKORLATBAN

- Panaszkezelés
- Pénzmosás ellenőrzés
- Biztonsági IKT-funkciók

Kritikus vagy fontos funkció

PANASZKEZELÉSI FUNKCIÓ IKT TÁMOGATÁSA

- Telefonos ügyfélszolgálat- és call center rendszerek (VoIP, IVR, hívásirányítás)
- Automatikus hangrögzítő rendszerek (hálózati vagy felhő alapú)
- Hangfelvételek tárolása és archiválása (biztonságos tárhely, visszakereshetőség)
- Ügyfélkapcsolati- és panaszkezelő rendszerek (CRM, ticketing, ügyiratkezelés)
- Digitális ügyfélcsatornák (e-mail, webes űrlap, chat, chatbot)
- Workflow és határidőkezelő rendszerek (panaszok nyomon követése, eszkaláció)
- Beszéd- és adatelemző eszközök (kulcsszókeresés, minőségellenőrzés)
- Hozzáférés- és jogosultságkezelés (felhasználói szintek, naplózás)
- Adatvédelmi és biztonsági megoldások (titkosítás, adatkezelési szabályok)
- Integrációs megoldások (kapcsolódás core rendszerekhez, API-k)

2013. évi CCXXXVII. törvény (Hpt.) 288. §

66/2021. (XII.20.) MNB rendelet – panaszkezelés részletes szabályai

PÉNZMOSÁS ELLENI FUNKCIÓ IKT TÁMOGATÁSA

- Ügyfél-azonosító és KYC rendszerek (digitális onboarding, okmányellenőrzés, ügyféladat-nyilvántartás)
- Tranzakció-monitoring rendszerek (valós idejű gyanús mintázat felismerés, riasztáskezelés)
- Szankció- és PEP-szűrő rendszerek (watchlist, blacklist ellenőrzés)
- Kockázatértékelő- és scoring rendszerek (ügyfél- és tranzakciós kockázati pontszámítás)
- Esetkezelő rendszerek (riasztások kivizsgálása, dokumentálás, workflow)
- Adat- és dokumentumkezelő rendszerek (KYC dokumentumok, audit trail, visszakereshetőség)
- Riportáló- és interfész rendszerek (hatósági jelentések, automatikus adatátadás)
- Integrációs- és API megoldások (kapcsolat core rendszerekkel, külső adatbázisokkal)

2017. évi LIII. törvény (Pmt.)

BIZTONSÁGI FUNKCIÓ IKT-TÁMOGATÁSA

- Hozzáférés- és jogosultságkezelő rendszerek (IAM, auditálható hozzáférés)
- Titkosítási megoldások (adatok védelme tárolás és továbbítás során)
- Adatnaplózó és audit rendszerek (log management, hozzáférés és adattovábbítás nyomon követése)
- Integrációs middleware és API réteg (biztonságos adatcsere belső és külső rendszerek között)
- Tűzfal- és proxy rendszerek (adattovábbítási, kapcsolati szabályok)
- Adatszivárgás elleni rendszerek (MDM, webproxy, DLP)

2013. évi CCXXXVII. törvény (Hpt.) 165-166. §

2. BLOKK

IKT-KOCKÁZATKEZELÉSI KERETRENDSZER FELÜLVIZSGÁLATA

Mamira Zoltán

DORA rendelet 16. cikk (1) bekezdés második albekezdésének a) pont

Megbízható és dokumentált IKT-kockázatkezelési keretrendszert kell létrehozni és fenntartani, amely részletezi az IKT-kockázat gyors, hatékony és átfogó kezelését célzó mechanizmusokat és intézkedéseket, többek között a releváns fizikai összetevők és infrastruktúrák védelme érdekében.

DORA rendelet 16. cikk (2) bekezdés

Az IKT-kockázatkezelési keretrendszert dokumentálni kell, és a felügyeleti utasításoknak megfelelően időszakonként és minden jelentős IKT-vonatkozású esemény bekövetkezésekor felül kell vizsgálni. A keretet folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján.

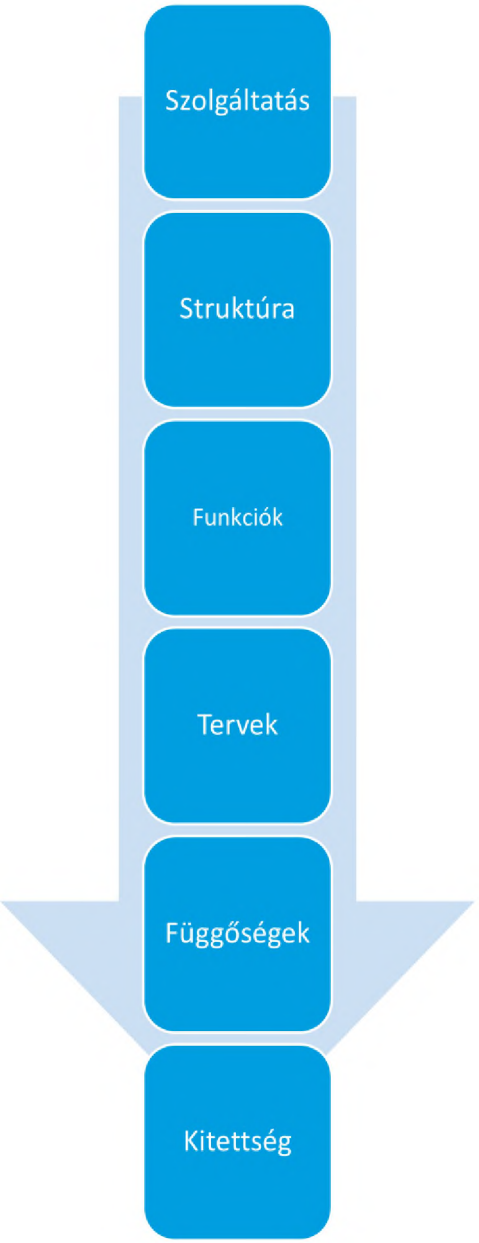
Az IKT-kockázatkezelési keretrendszer felülvizsgálata

Formátum követelmény	Leírás	Felügyeleti / audit elvárás	Audit támogatás
Kereshető elektronikus formátum	Kereshető PDF	Szabványos forma	Gyors visszakeresés
Strukturált dokumentum	Logikai fejezetek	Áttekinthetőség	Audit trail
Verziókövetés	Verziók követése	Nyomon követhetőség	Változások auditja
Dokumentált evidenciák	Források csatolása	Bizonyíték alap	Hitelesség
Teljesség és visszakereshetőség	Teljes, kereshető tartalom	Transzparencia	Kontroll hatékonyság

Formai követelmények

Követelmény	Tartalom
Vezető testületi jóváhagyás	Igazgatósági jegyzőkönyv / határozat
Felülvizsgálat oka – felügyeleti	Hatósági levél / utasítás
Felülvizsgálat oka – eseményvezérelt	Incidens lista + gyökérok-elemzés
Felülvizsgálati időszak	Kezdő és záró dátum
Felelős személy	Szervezeti kijelölés (pl. CISO)

Formai követelmények



A pénzügyi vállalkozás kötelező bemutatása az arányosság (méret, komplexitás) és kritikusság alapelveinek megfelelően.

Cél a pénzügyi szervezet működési és IKT-kontextusának teljes feltárása!

Kötelező elemek:

- szolgáltatások, tevékenységek, műveletek jellemzői
- szervezeti struktúra
- kritikus funkciók
- stratégia és főbb projektek
- IKT-függőségek (belső és kiszervezett, harmadik fél IKT-szolgáltatók)
- kiesési hatások értékelése

Vezetői szintű, konszolidált kockázati helyzetkép:

- az aktuális **kockázati kitettség** bemutatása,
- várható kockázati **trendek** azonosítása,
- a fenyegetettségi **környezet** (pl. kibertámadási minták, beszállítói lánc kockázatok) értékelése.

Kötelezően rögzítendő továbbá:

- a **kontrollok hatékonyság**ának értékelése (preventív, detektív és korrektív)
- „kiberbiztonsági helyzet”, **a szervezet érettségi szintje**, valamint rezilienciájának aktuális helyzete.

Hatókör definiálása

A jelentésnek egyértelműen rögzítenie kell:

- mely kritikus vagy fontos és egyéb funkciók,
- szolgáltatások,
- harmadik-fél szolgáltatók,
- IKT-rendszerek,
- szervezeti egységek, stb. tartoznak a felülvizsgálat tárgyi körébe.

Ez biztosítja az auditálhatóságot, az értelmezési határok egyértelműségét, a megismételhetőséget, a felügyeleti validáció lehetőségét.

- Teljes IKT-kockázatkezelési **keretrendszer értékelése**, felülvizsgálati megállapítások összefoglalása
- Kontrollkörnyezet és kiberbiztonsági **érettség vizsgálata** (gyengeségek, hiányosságok, lefedetlenségek azonosítása)
- Üzleti hatások elemzése minimálisan a kritikus funkciókon
- Súlyossági besorolás (alacsony / közepes / magas / kritikus)
- Részletes ok- és hatáselemzés
- Kritikus vagy fontos funkciók érintettsége
- IKT-függőségek és kiszervezések hatása, külső szolgáltatói kitettség figyelembevétele

- Korrekciós intézkedések meghatározása, minden hiányossághoz **konkrét intézkedés** rendelése (különösen kritikus funkciók esetén)
- Általános **következtetések**, megállapítások
- Kockázatalapú **priorizálás, határidők** (Végrehajtási határidők és felelősök)
- Folyamatos **nyomon követés** és dokumentált státusz
- Kontroll**hatékonyság** és kiberreziliencia értékelése
- **Fejlesztési fókuszok** (pl. monitoring, automatizálás)
- **Harmadik fél** IKT-kockázatkezelés és incidenskezelés fejlesztése

TAPASZTALT HIÁNYOSSÁGOK

- Az **IKT-kockázatfelmérés ≠ keretrendszer felülvizsgálat**
- A felülvizsgálat nem kockázatalapú, hanem **dokumentáció központú**
- Nem történik érdemi kontrollhatékonyság-vizsgálat, a megállapítások általánosak, nem konkrétak
- Nincs egyértelmű funkció-azonosítás
- Harmadik fél kockázatai nem jelennek meg, beszállítói kitettség nincs feltérképezve
- Intézkedések nem konkrétak vagy nem mérhetők, nincs meghatározott felelős vagy határidő, nem kapcsolódnak az egyes megállapításokhoz

„kiinduló állapot”

3. BLOKK

IKT SZOLGÁLTATÁSOK DEFINÍCIÓJA ÉS KAPCSOLÓDÓ SZABÁLYOKKAL KAPCSOLATOS TAPASZTALATOK

Tikos Anita

IKT SZOLGÁLTATÁS DEFINÍCIÓJA

DORA rendelet 3. cikk

- (19) **harmadik fél IKT-szolgáltató:** IKT-szolgáltatásokat nyújtó vállalkozás
- (21) **IKT-szolgáltatások**: IKT-rendszerek útján egy vagy több **belső vagy külső felhasználó részére** folyamatos jelleggel nyújtott digitális és adatszolgáltatások, ideértve a hardvert mint szolgáltatást és a hardverszolgáltatásokat, ami magában foglalja a hardverszolgáltató általi szoftver- vagy belsőrendszervezérlőprogram-(firmware-) **frissítéseket is**, ide **nem értve a hagyományos analóg telefonszolgáltatásokat**
- **63. preambulum:** Figyelembe véve az IKT-kockázat különböző forrásainak összetettségét, ugyanakkor a pénzügyi szolgáltatások zökkenőmentes nyújtását lehetővé tevő technológiai megoldások szolgáltatóinak nagy számát és sokféleségét is, e rendeletnek a harmadik fél IKT-szolgáltatók széles körére - köztük a felhőalapú számítástechnikai szolgáltatásokat, szoftvereket, adatelemzési szolgáltatásokat kínáló szolgáltatókra és az adatközpont-szolgáltatásokat nyújtó szolgáltatókra - kell vonatkoznia.

A preambulum kiemeli, hogy harmadik fél IKT-nak minősül:

- a pénzügyi csoporton belül beszerzett IKT-szolgáltatásokkal összefüggésben, azon vállalkozások, amelyek egy pénzügyi csoport részét képezik, és elsősorban az anyavállalatuk vagy az anyavállalatuk leányvállalatai vagy fióktelepei számára nyújtanak IKT-szolgáltatásokat,
- a pénzforgalmi szolgáltatások ökoszisztémájának azon résztvevői, amelyek fizetésfeldolgozási tevékenységet végeznek vagy fizetési infrastruktúrákat üzemeltetnek.

Kivétel: a fizetési vagy értékpapír-kiegyenlítési rendszereket működtető központi bankok, valamint az állami feladatok ellátása keretében IKT-vonatkozású szolgáltatásokat nyújtó hatóságok.

IKT SZOLGÁLTATÁS DEFINÍCIÓ

Q&A030 (DORA030-2999) ESA-k válasza

A preambulum bekezdés ellenére is számos kérdés merül fel az IKT szolgáltatók tekintetében, így például az IKT szolgáltatások fogalmának értelmezése és alkalmazása a pénzügyi szolgáltatások tekintetében:

- a kérdés és megközelítés lényege, hogy a pénzügyi szolgáltatások ha önmagukban már DORA által szabályozottak, akkor is IKT szolgáltatásnak minősülnek –e
- a pénzügyi intézmény feladata megítélni, hogy a szolgáltatás IKT szolgáltatásnak minősül-e
- azt is meg kell vizsgálni, hogy a szolgáltatás szabályozott pénzügyi szolgáltatásnak minsül-e (valamely ágazati jogszabály által)
- pénzügyi szolgáltatás + IKT-komponens esetén kettős teszt elvégzése szükséges:

  Ha egy pénzügyi entitás másik pénzügyi entitásnak pénzügyi szolgáltatásához kapcsolódóan nyújt IKT-elemet, a fogadó intézmény vizsgálja:

  (i) a kapott elem IKT-szolgáltatás-e a DORA 3. cikk (21) szerint, és

  (ii) a nyújtó intézmény és a nyújtott pénzügyi szolgáltatás szabályozott-e (uniós, tagállami, harmadik országbeli jog alapján)

Ha mindkettő igen: az IKT-elem túlnyomórészt pénzügyi szolgáltatásnak minősül, és **nem kezelendő IKT-szolgáltatásként a DORA 3. cikk (21) szerint.**

VISZONT-ELADÓK ÉRTÉKELÉSE

DORA215/3300

ESA-k válasza

Amennyiben a viszonteladó kizárólag licenceket szállít, és nem nyújt IKT szolgáltatást folyamatos jelleggel, akkor **nem minősül harmadik fél IKT-szolgáltatónak** az IKT-szolgáltatás fogalma alapján.

Amennyiben a nyújtott szolgáltatás IKT szolgáltatásnak minősül, két esetet kell elkülöníteni:

1) van közvetlen szerződés a pénzügyi szolgáltató és a tényleges IKT-szolgáltató között, akkor a tényleges IKT szolgáltatót kell IKT-szolgáltatónak tekinteni,
2) ha nincs közvetlen szerződés a tényleges IKT-szolgáltatóval, akkor a pénzügyi szolgáltató a viszonteladóval kötött megállapodást alapján a tényleges szolgáltató, mint alvállalkozó értelmezhető a szolgáltatási láncban.

IKT SZOLGÁLTATÁS VS. KISZERVEZÉS

Eredeti cél

A DORA által bevezetett IKT szolgáltatási definíció és elvárások a kiszervezési és felhőszolgáltatásokkal kapcsolatos követelményeken alapultak és azokat szerették volna kiterjeszteni és tökéletesíteni.

Jelenlegi jogi helyzet

- a kiszervezési előírásokat nem írta felül és nem is törölte el a DORA rendelet, így a két követelményrendszer egyszerre alkalmazandó
- az IKT szolgáltatás definíciója jelentősen különbözik a kiszervezéstől, így fontos az új megközelítés megértése (pl. ha nincs ügyfél vagy személyesadat hozzáférés vagy nem a pénzügyi szolgáltatáshoz kapcsolódik akkor is IKT szolgáltatásnak minősülhet egy szolgáltatás).

KRITIKUS FONTOS FUNKCIÓ VS. KRITIKUS IKT SZOLGÁLTATÓ

- Az intézmény megvizsgálja, hogy **IKT szolgáltatásnak** minősül-e a szolgáltatás, a szolgáltató pedig **IKT szolgáltatónak** aztán pedig azt, hogy **kritikus vagy fontos funkciót támogat-e a szolgáltatás.**
- **„kritikus harmadik fél IKT-szolgáltató”:** 3. cikk 23. pontja szerint a 31. cikkel összhangban kritikusként kijelölt, harmadik fél IKT-szolgáltató.

A DORA rendelet EU-s szinten, a pénzügyi szektor (vagy azon belüli ágazatok) számára kritikus IKT szolgáltatók kijelölését írja elő kritikus harmadik fél IKT szolgáltatónak. A kijelölést az Európai Felügyeleti Hatóságok (ESA-k) végzik, a kijelölés célja pedig, hogy ezen szolgáltatókat az ESA-k felvigyázzák.

Gyakori félreértések:

- Intézményi és nemzeti szinten nem kell kritikus IKT szolgáltatót kijelölni
- A felvigyázást az ESA-k végzik, így a felvigyázással kapcsolatos információk az EBA, ESMA és EIOPA honlapján lesz elérhető
- A tagállami hatóságok közreműködnek a felvigyázásban és közvetítik az esetleges feltárt hiányosságokat és kockázatokat az intézmények felé
- Kritikus IKT szolgáltató alkalmazása esetén is minden DORA követelménynek eleget kell tenni, az ESA-k nem elvégzik el az auditálást, ellenőrzéseket átvilágításokat az intézmények helyett, hanem segítik az intézmények érdekérvényesítését a DORA megfelelés érdekében a globális nagy cégek esetében.

2025-BEN KIJELÖLT KRITIKUS IKT SZOLGÁLTATÓK

- **Accenture plc**
- **Amazon web Services EMEA Sarl**
- **Bloomberg L.P.**
- **Capgemini SE**
- **Colt Technology Services**
- **Deutsche Telekom AG**
- **Equinix (EMEA) B.V.**
- **Fidelity National Information Services, Inc.**
- **Google Cloud EMEA Limited**
- **International Business Machine Corporation**
- **InterXion HeadQuarters B.V.**
- **Kyndryl Inc.**
- **LSEG Data and Risk Limited**
- **Microsoft Ireland Operations Limited**
- **NTT DATA Inc.**
- **Oracle Nederland B.V.**
- **Orange SA**
- **SAP SE**
- **Tata Consultancy Services Limited**

Felvigyázójuk: EBA

EBA felvigyázással kapcsolatos információk:

https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/dora-oversight

4. BLOKK

ADATSZOLGÁLTATÁSI ÉS ROI TAPASZTALATOK

Tikos Anita

KÉT ADATSZOLGÁLTATÁSI KÖTELEZETTSÉG

43/2025. (XII. 4.) MNB rendelet

- **Kritikus vagy fontos funkciót támogató IKT szolgáltatói szerződésekkel kapcsolatos bejelentés (IKT KR):**
  - Új szerződés kötése (5 munkanappal a szerződés aláírás előtt)
  - Kritikus vagy fontos funkciót támogató szerződéssé válás (5 munkanapon belül)
  - Kritikus vagy fontos funkciót már nem támogat (5 munkanapon belül)
  - Módosítás (5 munkanappal a módosítás aláírása előtt)
  - Megszűnés (5 munkanappal megszűnés aláírása előtt)

- **Szolgáltatói nyilvántartás (RoI) : éves adatszolgáltatás (minden év január 31-ig kell beküldeni)**

A kitöltendő űrlap elérhetősége: https://www.mnb.hu/letoltes/adatbekero-dokumentum.xlsx

A nyilvántartás űrlap tartalmát és felépítését az (EU) 2024/2956 VÉGREHAJTÁSI RENDELETE (2024. november 29.) tartalmazza (ez tekinthető kitöltési útmutatónak)

Nem MNB engedélyhez/ jóváhagyáshoz kötött a szerződés kötés, megszűnés vagy módosítás, viszont hiányosság esetén az MNB módosítást kérhet.

KR ŰRLAP

Kiszervezés:

- Átfedés okán dupla bejelentés kellhet
- Kiszervezés bejelentésnél MNB DORA megfelelést is néz

DORA_1002_v1 azonosító kódú űrlap

Felügyeleti ellenőrzés szempontjai: (űrlapon is kitöltendő és dokumentummal alátámasztandó)

- Szerződés megfelel –e a DORA követelményeknek (30. cikk és kapcsolódó RTS).
- BCP, átállási és kilépési tervek megléte és megfelelősége
- Alvállalkozók kérdésköre
- **Új szerződés esetén:** átvilágítással kapcsolatos felmérések, kockázatelemzés stb.
- **Módosítás esetén:** módosítás oka és tartalma, érinti –e a kockázatelemzést, alvállalkozói kérdést, BCP, átállási vagy kilépési tervet
- **Már nem kritikus vagy fontos funkciót támogatás esetén**: a felülvizsgálat dokumentációja, ami alátámasztja az átminősítést
- **Megszűnés esetén:** megszűnés oka valamint, hogy a szolgáltatás hogyan kerül megvalósításra ezután

Jelentős elmaradásban vannak a PV-k ezen adatszolgáltatással: 10%-tól kaptunk ilyen bejelentést!

KR ŰRLAP TAPASZTALATOK

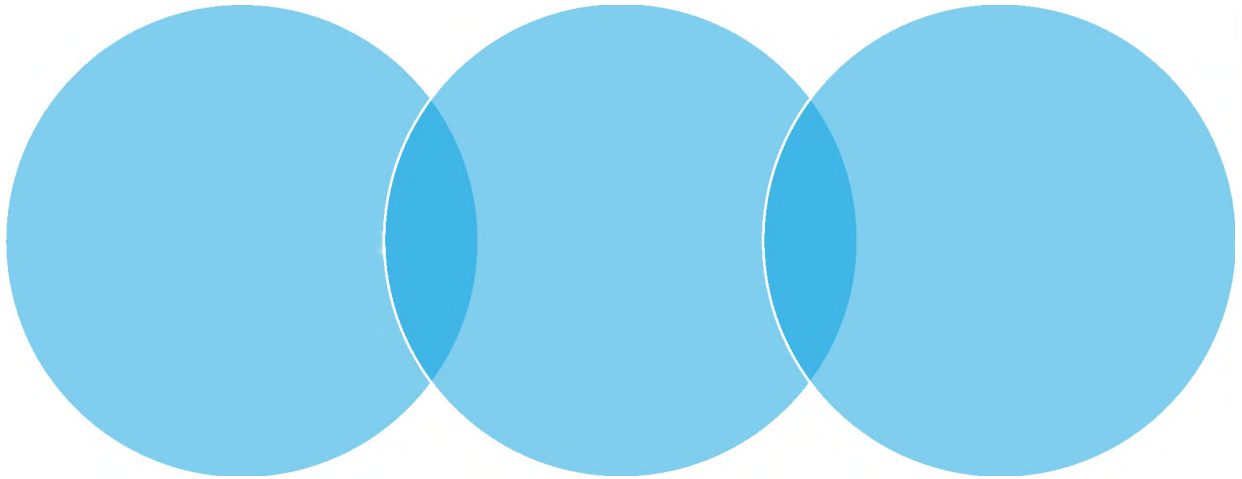
- Az űrlap sok kérdést tartalmaz: kitöltéssel már önellenőrzés is történik, hogy a követelményeknek való megfelelést be tudja –e mutatni az intézmény,
- A KR űrlapon szerződésenként kell jelentést tenni, (nem szolgáltatónkként)
- A korábban beküldött űrlapok módosítása a bejelentések összekötését okozza, nehezíti az átláthatóságot,
- A szerződés módosítás esetén lehetőség van Szerződés első bejelentésének azonosítóját megadni (K-szám): ez a korábban ezen az űrlapon beküldött adatszolgáltatások számára vonatozik, (nem a RoI-ra és nem a kiszervezési bejelentésre)
- Az űrlaphoz csatolni kell a szükséges dokumentumokat is (szerződés, exit stratégia, BCP és DR tervek stb.).

SZOLGÁLTATÓI NYILVÁNTARTÁS (ROI)

DORA rendelet 28. cikk (3):

„…információ-nyilvántartást kell vezetniük és naprakészen tartaniuk a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló valamennyi szerződéses megállapodásról.„

Célja:



- A nyilvántartást folyamatosan vezetni kell
- MNB-nek évente kell beküldeni
  (előző év dec 31-es referencia dátummal)
- A nyilvántartás kitöltése egyszer szükséges nulláról, utána folyamatosan frissítendő évközben.

SZOLGÁLTATÓI NYILVÁNTARTÁS (ROI) TAPASZTALATOK

- **Az adatszolgáltatás sikertelen amíg hibakódok állnak fenn:**
  - Az ERA szolgáltatás a nyilvántartást a beküldés után ellenőrzi. Ha hibát talál akkor az ERA postaládába megküldi a hibakódokat.
- **Kitöltési javaslat:**
  - Az első 2-3 fül/tábla kitöltését követően, javasolt a B_06.01 – A funkciók azonosítása tábla kitöltése,
  - A funkció azonosításnál javasoljuk az összes funkció feltüntetését.
- **Gyakori hibák:**
  - 1 funkció van, az kritikus vagy fontos így minden szerződés annak számítana,
  - Kritikusság értékelése: nem vizsgált opció olyan funkció esetén nem választható, amelyhez IKT szerződés kapcsolódik hiszen akkor nem alátámasztott, hogy hogyan kell kezelni a szerződést,
  - Van amikor tévesen a kiszervezésnek minősülő szerződések is bekerülnek a nyilvántartásba.

5. BLOKK

JELENTŐS INCIDENS BEJELENTÉSEKKEL KAPCSOLATOS TAPASZTALATOK

Tikos Anita

JELENTŐS INCIDENS KEZELÉS ÉS BEJELENTÉS

Kezelés

- Esemény: észlelésére, kezelésére, bejelentésére szolgálófolyamat kialakítása, végrehajtása
- Egy az IKT-val kapcsolatos események nyomon követésére és naplózására alkalmas folyamat kidolgozása, alkalmazása
- Nyilván kell tartani valamennyi IKT eseményt és jelentős kiberfenyegetést
- Kommunikációra vonatkozó tervek, eljárások (média, ügyfelek, szolgáltatók, belső eszkaláció)

Osztályozás

- Az IKT vonatkozású incidensek osztályozása megadott kritériumrendszer szerint (RTS-ben meghatározott küszöbértékek alapján)
- Fenyegetések osztályozása

Bejelentés

- Az incidensek bejelentése az NCA-knak az ESA-k által kidolgozandó egységes űrlapok alkalmazásával;
  - jelentős IKT események
  - jelentős pénzforgalmi vonatkozású működési vagy biztonsági események
  - jelentős kiberfenyegetések (önkéntes alapú)

INCIDENS OSZTÁLYOZÁSI SZABÁLYOK

Szolgáltatás kritikussága	**kritikus vagy fontos funkcióit támogató IKT-szolgáltatásokat, vagy hálózati és információs rendszereket érint**
	engedélyhez vagy nyilvántartásba vételhez kötött szolgáltatásokat érint vagy az illetékes hatóságok felügyelete alá tartoznak
	sikeres, rosszindulatú és illetéktelen hozzáférést eredményez vagy eredményezett-e a pénzügyi szervezet hálózati és információs rendszereihez
Ügyfelek, pénzügyi partnerek és ügyletek	érintett ügyfelek száma meghaladja **az érintett szolgáltatást igénybe vevő összes ügyfél 10 %-át**
	érintett **ügyfelek száma meghaladja a 100 000-et**
	érintett pénzügyi partnerek száma meghaladja a tevékenységeket végző összes pénzügyi partner 30 %-át
	ügyletek száma meghaladja a **végrehajtott ügyletek napi átlagos számának vagy értékének 10 %-át**
	relevánsnak minősített ügyfelek vagy pénzügyi partnerek érintettek
A hírnevet érintő hatás	az esemény megjelent a sajtóban
	különböző ügyfelektől vagy pénzügyi partnerektől ismétlődő panaszokat eredményezett
	nem lesz képes teljesíteni a szabályozási követelményeket
	elveszíti vagy az üzleti tevékenységére jelentős hatást gyakorló ügyfeleit vagy pénzügyi partnereit
Időtartam és leállási idő	az esemény időtartama meghaladja a 24 órát
	a leállási idő meghaladja a 2 órát
Földrajzi kiterjedés	két vagy több tagállamban fejt ki hatást
Adatvesztések	**adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére gyakorolt hatás** hátrányosan érinti pénzügyi szervezet üzleti célkitűzéseinek megvalósítását vagy a szabályozási követelményeknek való megfelelésre való képességét
Gazdasági hatás	felmerült költségek és veszteségek meghaladták vagy valószínűleg meghaladják a 100 000 EUR-t.

JELENTŐSSÉ MINŐSÍTÉS

Kritikus szolgáltatás+

- legalább 2 további küszöbértéket elér, vagy
- sikeres, rosszindulatú és illetéktelen hozzáférés történik olyan hálózati és információs rendszerekhez, ahol ez a hozzáférés adatvesztéshez vezethet.

A BIZOTTSÁG (EU) 2024/1772 FELHATALMAZÁSON ALAPULÓ RENDELETE

INCIDENS BEJELENTÉSI HATÁRIDŐK

Kezdeti jelzés

- Osztályozást követő 4 órán belül,
- De legalább az incidens azonosításához képest **24 órán belül**

Időközi jelentés

- Minden esetben amikor az incidens státusza változik, az incidens kezelése módosul új információk okán (DORA 19. cikk (4))
- Hatóság kérésére (DORA 19. cikk (4))
- 72 órával a kezdeti jelzést követően
- Vagy ha a szolgáltatás helyre állt (back to normal)

Záró jelentés

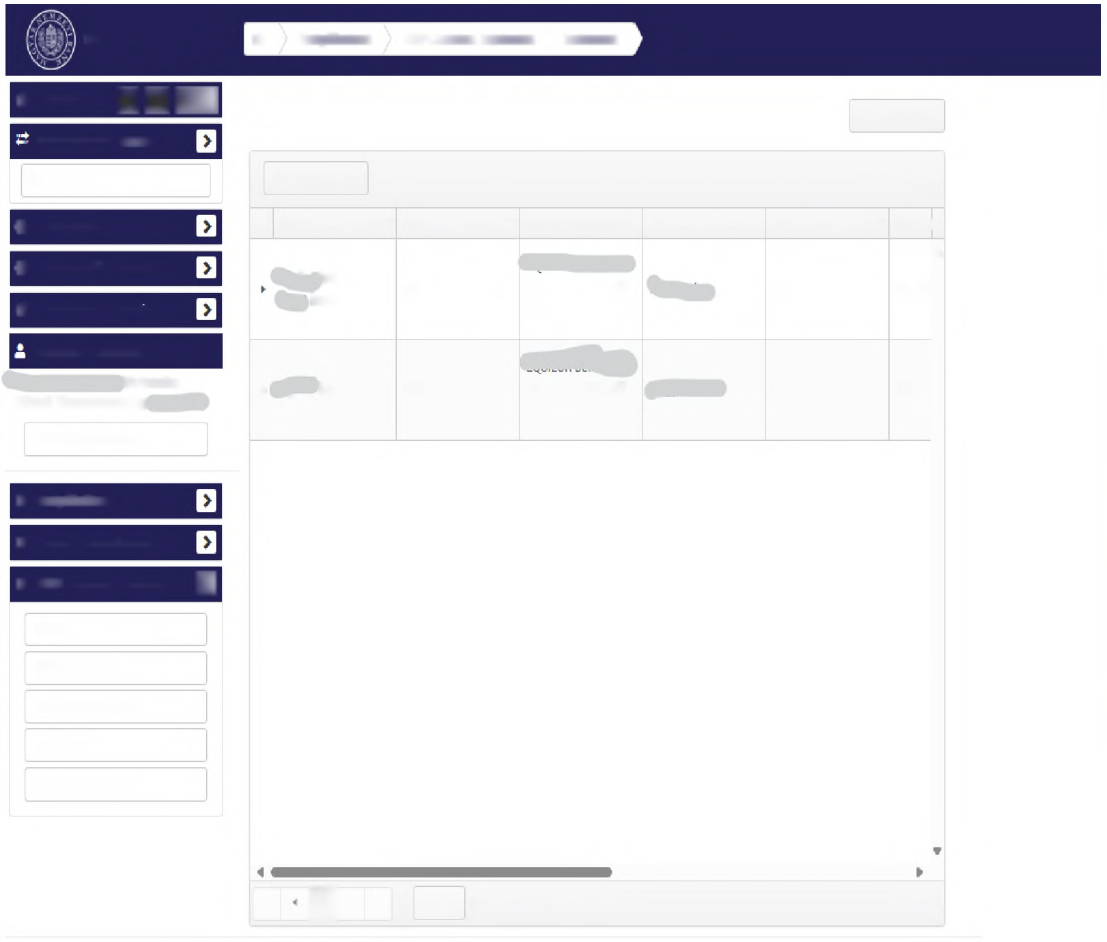
- utolsó időközi jelentést követő 30 napon belül
- (kivéve ha még nem záródott le az esemény, ezesetben a lezárást követő napon)

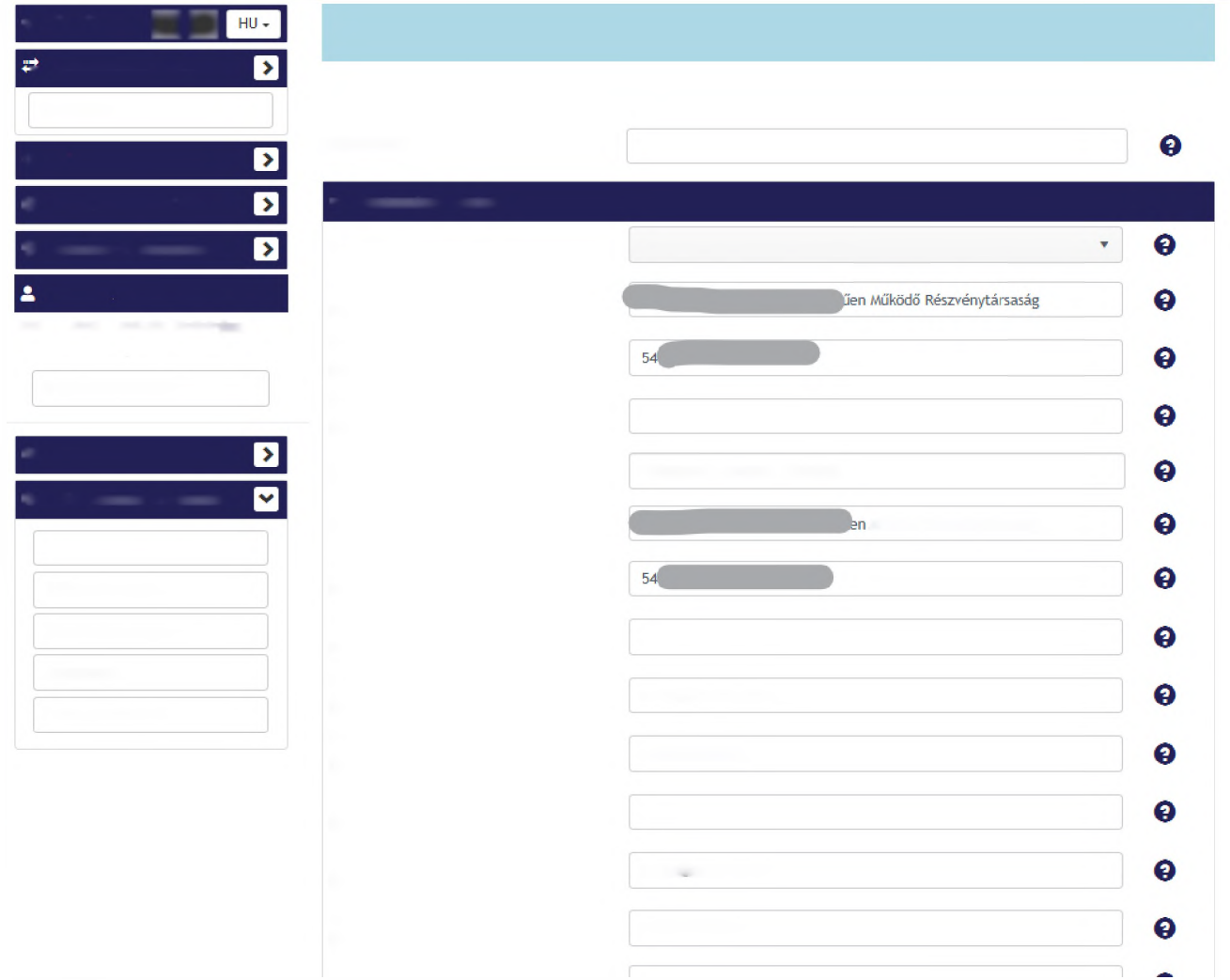
INCIDENS BEJELENTÉSI PLATFORM ÉS TAPASZTALATOK

Elérhetősége: ERA-ban a Szolgáltatások menüpont alatt a DORA incidens bejelentés szolgáltatás keretében (regisztrálni kell a szolgáltatásra az eléréshez, amely intézmény nincs regisztrálva fontos lenne a pótlása)

- A pénzügyi szervezetek kiszervezhetik az incidens bejelentési kötelezettségeket harmadik fél szolgáltatónak [DORA rendelet 19. cikk (5) bekezdés]
- Ebben az esetben ezt is be kell jelenteni: ERA DORA incidens bejelentési szolgáltatás **/ Küldő intézmény /Új felvétel menüpont alatt**
- A kiszervezés bejelentése teszi lehetővé, hogy az ERA-n az intézmény nevében a megbízott harmadik fél incidenst tudjon bejelenteni az intézmény nevében
- Pénzügyi vállalkozások incidens bejelentési tapasztalatai: nem tudunk beszámolni ilyenről mert eddig 1 db incidens jelentésre került sor ezen intézményektől.

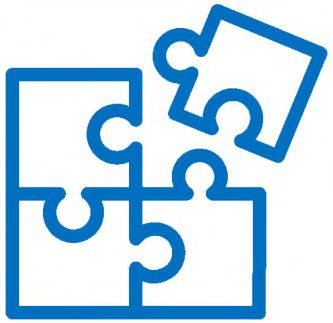
INCIDENS BEJELENTÉSI PLATFORM





ÖSSZEGZŐ GONDOLATOK

- A DORA és részletszabályai egy **átfogó keretrendszert** hoztak létre
- A **funkció helyes besorolása kritikus** lehet a teljes DORA megfelelés tekintetében
- A **vezetői felelősséget** és interakciót megnövelte a korábbiakhoz képest
- Jelentős dokumentációs kötelezettséggel jár!



A DORA rendelet és a kapcsolódó RTS-ek, ITS-ek elérhetőek az **MNB honlapon, az Informatika Felügyeleti főosztály aloldalán**: Informatikai felügyelet | MNB.hu

A jogértelmezésben az MNB követi az ESA-k által kiadott Q&A-ket melyek elérhetőek mindegyik **ESA honlapján**: Search for Q&As | European Banking Authority

KÉRDÉSEK?

Tikos Anita | főosztályvezető
Mamira Zoltán | osztályvezető

KÖSZÖNJÜK A FIGYELMET!