

Tikos Anita | főosztályvezető

Mamira Zoltán | osztályvezető

Informatikai felügyeleti főosztály



MNB | Felügyeleti Akadémia | 2026

DORA SZAKMAI NAP

A stylized, light blue graphic element consisting of several overlapping, curved lines that form a complex, abstract shape, possibly representing a network or a stylized letter 'D'.



1. BLOKK





KRITIKUS VAGY FONTOS FUNKCIÓ ÉRTELMEZÉSE ÉS ALKALMAZÁSA

Mamira Zoltán



Üzleti funkciókkal való egyértelmű összerendelés

Adatok és rendszerek osztályozása

IKT-kockázati források és kezelésük

Harmadik fél szolgáltatók

Eszköz- és vagyonelem-nyilvántartások

Elavult rendszerek

Feltérképezés és
osztályozás



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-szolgáltatóknál** szigorított szerződéses, felügyeleti és kilépési követelmények



„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 megghiúsult 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

Folyamat

Szolgáltatás

Tevékenység

IKT-
vagyonelem

IKT-eszköz



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
- Jogsabályi 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:
 - (i) dokumentált összerendelés „IKT szolgáltatás → támogatott üzleti funkció, szolgáltatás → CIF státusz”;
 - (ii) 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))

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





Panaszkezelés



Pénzmosás ellenőrzés



Biztonsági IKT-funkciók

Kritikus vagy fontos funkció





- 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, eskaláció)
- 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



- 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.)



- 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

A faint, light blue decorative graphic consisting of several overlapping, stylized, curved lines that resemble a calligraphic or abstract pattern, positioned below the horizontal line.



IKT-KOCKÁZATKEZELÉSI KERETRENDSZER FELÜLVIZSGÁLATA

Mamira Zoltán



DORA rendelet 6. cikk (1) bekezdés második albekezdésének a) pont

A pénzügyi szervezeteknek általános kockázatkezelési rendszerük részeként megbízható, átfogó és jól dokumentált IKT-kockázatkezelési keretrendszerrel kell rendelkezniük, amely lehetővé teszi számukra az IKT-kockázat gyors, hatékony és átfogó kezelését, továbbá a digitális működési reziliencia magas szintjének biztosítását.

DORA rendelet 6. cikk (5) bekezdés

Az IKT-kockázatkezelési keretrendszert dokumentálni kell, és legalább évente egyszer felül kell vizsgálni, továbbá jelentős IKT-vonatkozású események bekövetkezésekor, valamint a digitális működési reziliencia tesztelésére vagy ellenőrzésére irányuló releváns folyamatokból származó felügyeleti utasításokat és következtetéseket követően. A keretet folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján.





Formai követelmények

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)

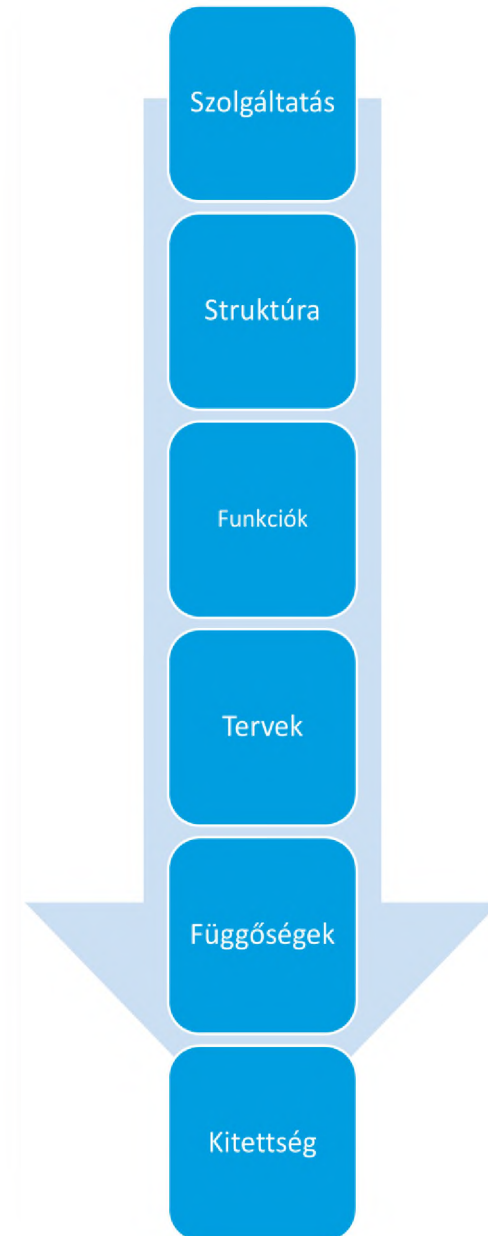


A pénzügyi szervezet kötelező bemutatása az arányosság (méret, komplexitás) és kritikusság alapelveinek megfelelően, a csoportfelépítés ismertetése.

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



BEVEZETŐ RÉSZ 1.

A szervezet
tevékenysége
és háttere



Változások összefoglalása

- az előző jelentés benyújtása óta történt jelentős változások

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

Hatókör definiálása

(összhangban a reziliencia stratégiával, ellenőrzési programmal és az irányítási rendszerrel)

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.

Keretrendszert érintő változások és fejlesztések

A hatókörben leírt IKT-kockázatkezelési keretrendszerben *(az előző felülvizsgálat óta)* bekövetkezett **jelentős** változások és fejlesztések leírása; **a reziliencia stratégiára, ellenőrzési programra és az irányítási rendszere hatás elemzése.**

- Teljes IKT-kockázatkezelési **keretrendszer értékelése**, felülvizsgálati megállapítások összefoglalása
- Kontrollkörnyezet és kiberbiztonsági **érettség vizsgálata** (gyengeségek, hiányosságok, lefedetlenségek azonosítása)
- Súlyossági besorolás (pl. saját kockázatértékelésnek megfelelően, transzparensen)
- Üzleti hatások elemzése minimálisan a kritikus funkciókon
- Kritikus vagy fontos funkciók érintettsége
- Részletes ok- és hatáselemzés
- IKT-függőségek és kiszervezések hatása, külső szolgáltatói kitétség figyelembevétele
- **Szükség esetén az illetékes hatóság tájékoztatásának folyamatára vonatkozó információk**



- Korrekciós intézkedések összefoglalása, általános **következtetések**, megállapítások
- Feltárt gyengeségek tételes és részletes ismertetése
- Korrekciós intézkedések részletes meghatározása, minden hiányossághoz konkrét intézkedés rendelése (különösen kritikus funkciók esetén)
- az intézkedések végrehajtásáért **felelős** funkció azonosítása
- Kockázatalapú **priorizálás, határidők** (Végrehajtási határidők és felelősök)
- Folyamatos **nyomon követés** és dokumentált státusz, illetve a végrehajtás kockázatai
- Hiányosság költségvetési, humán és anyagi erőforrás hatása (intézkedésé is!)
- **Fejlesztési fókuszok** (pl. monitoring, automatizálás)
- **Harmadik fél** IKT-kockázatkezelés és incidenskezelés fejlesztése

Intézkedések
értékelése,
nyomon
követése



Kockázatelfogadás esetén:

- Üzleti hatáselemzés
- IKT-kockázat értékelés
- fennmaradó kockázat elfogadás dokumentumai

Döntéselőkészítő módszertan

Értékelés és magyarázat, hogy miként biztosítható a digitális reziliencia elvárt mértéke.



- Információk a tervezett további fejlesztésekről;
- a keretrendszer felülvizsgálatának eredményeként leszűrt következtetések;
- a múltbeli felülvizsgálatokra vonatkozó információk,
- az eddigi felülvizsgálatok jegyzéke;
- a legutóbbi értékelésben szereplő korrekciós intézkedések végrehajtásának állapota;
- az eredménytelen korrekciós intézkedések javítására vonatkozó tervek és az esetleges váratlan kihívások bemutatása

Keretrendszer
fejlesztése



Felhasznált információforrások:

- az informatikai működést érintő **belső ellenőrzések** eredményei;
- **a megfelelőség értékeléseinek** eredményei:
 - belső kontroll területi auditok,
 - KPI, KRI értékelések,
 - minőségbiztosítási felmérések,
 - GAP-elemzések,
 - MNB vizsgálatok,
 - könyvvizsgálói jelentések,
 - tanúsítások eredményei...
- a digitális működési reziliencia **tesztelésének** eredményei (+TLPT fejlett tesztelésének eredményei)
 - sérülékenységi értékelések és ellenőrzések,
 - nyílt forrású elemzések,
 - hálózatbiztonsági értékelések,
 - eltéréselemzések,
 - fizikai biztonsági felülvizsgálatok,
 - kérdőívek és szoftveres átvilágítási megoldások,
 - forráskódvizsgálatok,
 - forgatókönyv-alapú tesztek,
 - kompatibilitás-tesztelés,
 - teljesítmény-tesztelés,
 - end-to-end tesztelés,
 - behatolási tesztelés...
- **külső források**



Felhasznált külső információforrások:

ICT harmadik fél szolgáltatók

- pl. felhőszolgáltató (AWS, Azure, stb.)
- kiszervezett partner, TPP
- üzemeltetési szolgáltató

Külső biztonsági források

- CERT-ek (pl. CSIRT-ek)
- hatósági riasztások
- fenyegetettségi információs szolgáltatók

Más piaci szereplők jelzései

- más pénzügyi intézmények értesítései
- iparági megosztások

Nyilvános információforrások

- publikált sebezhetőségek (pl. CVE adatbázis)
- médiában megjelent incidensek

Információk
forrása és
kapcsolódó
dokumentáció





- Az IKT-kockázatelemzés \neq 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

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 minősül –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.**



Ha 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.

Eredeti cél:

A DORA által bevezetett IKT szolgáltatási definíció és elvárások a kiszervezési és felhőszolgáltatásokkal kapcsolatos követelményeken alapultak és azokat szeretnék 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 személyes adat hozzáférés vagy nem a pénzügyi szolgáltatáshoz kapcsolódik akkor is IKT szolgáltatásnak minősülhet egy szolgáltatás)



- 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

A decorative graphic element consisting of a complex, interlocking knot-like pattern in a light blue color, positioned below the horizontal line.



ADATSZOLGÁLTATÁSI ÉS ROI TAPASZTALATOK

Tikos Anita

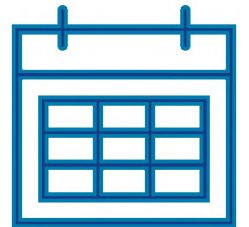
Adatszolgáltatási MNB rendelet

- **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)

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

- **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)

Kiszervezés:

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



Felügyeleti ellenőrzés szempontjai

- 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



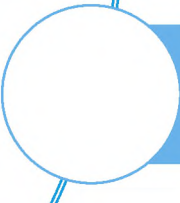
Az ūrlap sok kérdést tartalmaz: kitöltéssel már önellenőrzés is történik, hogy a követelményeknek való megfelelést be tudja –e mutatni az intézmény



A KR ūrlapon szerződésenként kell jelentést tenni (nem szolgáltatónként)



A korábban beküldött ūrlapok 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 ūrlapon beküldött adatszolgáltatások Kszámára vonatzik (nem a RoI-ra és nem a kiszervezési bejelentésre)

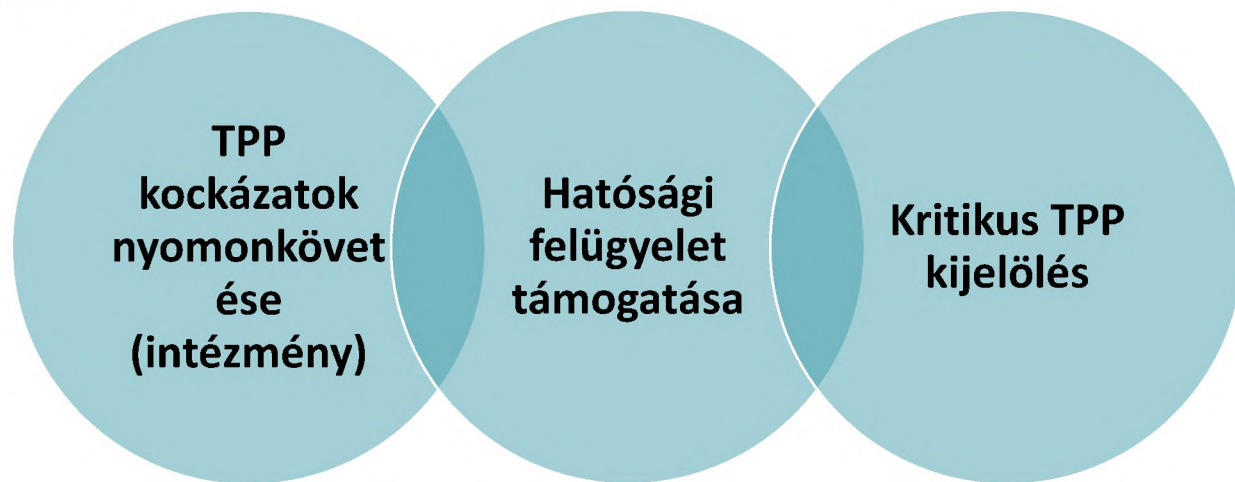


Az ūrlaphoz csatolni kell a szükséges dokumentumokat is (szerződés, exit stratégia, BCP és DR tervek)

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

Minden DORA intézménynek
be kell küldenie

Nem minden Rol kerül az MNB
által átadásra

Rol folyamatos vezetése

- Szerződéssel kapcsolatos változás esetén frissíteni kell,
- Új szerződés esetén frissíteni kell,
- Megszűnés után is (de 5 évig benne marad a szerződés)

Rol benyújtása ERA-n (jan. 31- ig)

- Dec. 31-es referencia adat
- Beküldés előtt az ERA űrlapot ellenőrzi
- Rol-t beküldés után ellenőrzi az ERA
- Sikeresnek akkor tekinthető ha nem küld több hibakódot az ERA

MNB átadja a Rol-t az EBA-nak (márc. 31)

- ERA is végez automatikus validációt
- Jelentős átfedésben van az MNB-ével
- Hiba esetén az ERA-n küldjük vissza, javítani szükséges

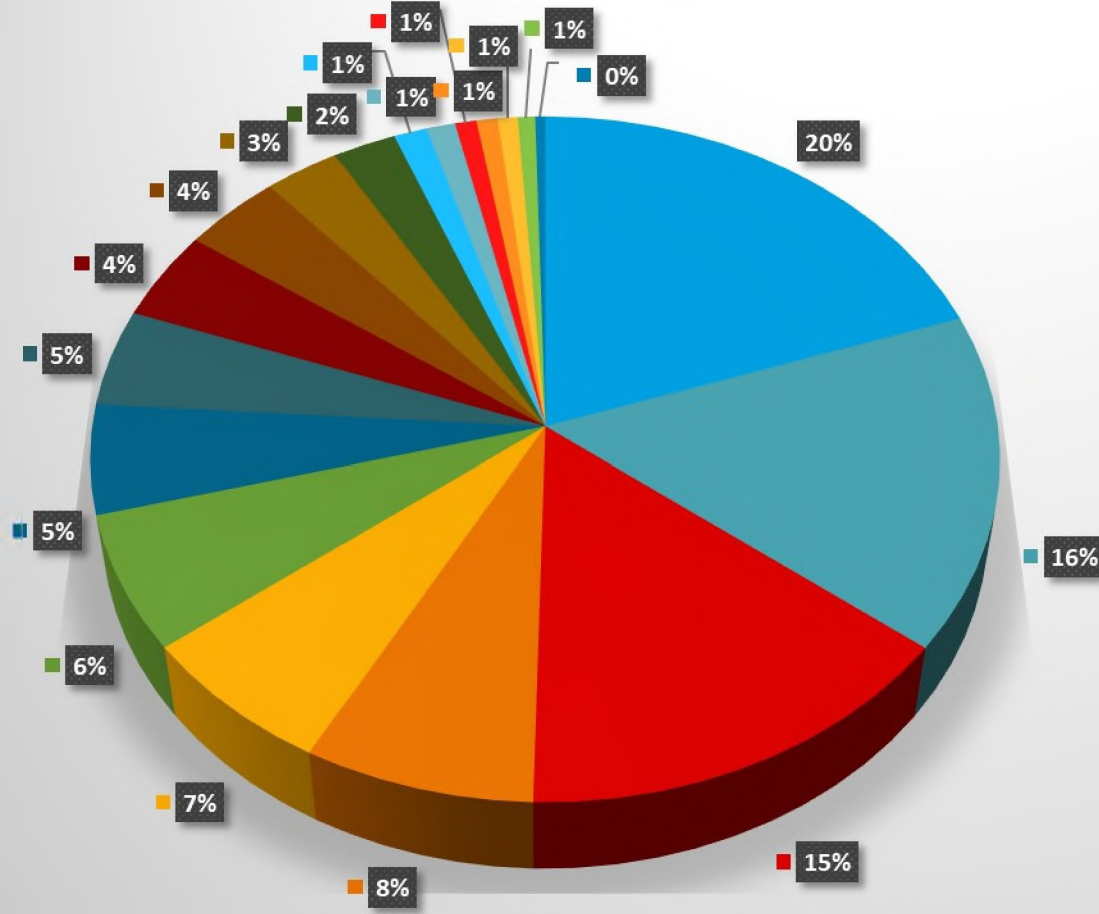
EBA adattisztítás utáni visszajelzései

- Idén került bevezetésre
- Márc 31 után adattisztítás céljából másik ellenőrzés
- Itt is kapunk hibakódokat (ERA-n küldjük)



- 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

Szerződések szolgáltatás szerinti eloszlása



- S14. IKT-üzemeltetés kezelése (beleértve a karbantartást is)
- S13. Szoftverek licencbe adása (kivéve a SaaS-t)
- S02. IKT-fejlesztés
- S05. Adatszolgáltatás
- S15. IKT-vel kapcsolatos tanácsadás
- S10. Távközlési szolgáltató
- S03. IKT-ügyfélszolgálat és első szintű támogatás
- S19. Felhőalapú szolgáltatások: SaaS
- S11. Hálózati infrastruktúra
- S12. Hardver és fizikai eszközök
- S04. IKT-vel kapcsolatos biztonságirányítási szolgáltatások
- S07. IKT, létesítmények és tárhelyszolgáltatások (kivéve a felhőalapú szolgáltatásokat)
- S06. Adatelemzés
- S01. IKT-projektmenedzsment
- S18. Felhőalapú szolgáltatások: PaaS
- S09. Nem felhőalapú adattárolás
- S08. Számítások
- S17. Felhőalapú szolgáltatások: IaaS
- S16. IKT-kockázatkezelés



5. BLOKK





JELENTŐS INCIDENS BEJELENTÉSEKKEL KAPCSOLATOS TAPASZTALATOK

Tikos Anita

Kezelés

- Esemény: észlelésére, kezelésére, bejelentésére szolgáló folyamat 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 eskaláció)

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)

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 osztályozási RTS 15. cikk Ismétlődő események jelentési kötelezettségét vezeti be

Amennyiben egy esemény önmagában nem minősül jelentősnek de:

- 6 hónapon belül legalább kétszer előfordult/ ismétlődött,
- az incidens jelentési űrlapban szereplő gyökérok lista szerint azonos a gyökérok az ismétlődő eseményeknek
- együttesen már elérik a jelentős esemény küszöbértékeit

Az elemzéseket havi rendszerességgel kell elvégezni az ismétlődő eseményekre

A jelentős eseményekre vonatkozó űrlapon kell bejelenteni

Mikrovállalkozások felmentést kapnak a cikk alól!!!!

- Minden incidenst nyilván kell tartani, nem csak a jelentőset
- A nyilvántartásból ki kell derüljenek az osztályozási kritériumok és a gyökérok minden incidens esetében
- Ez segít majd az ismétlődő incidenst mérni
- A nyilvántartásba érdemes az incidensbejelentés kérdéseinek egy részét bevonni (szintén a riportálást segíti)
- Egy incidens jelentés nem lezárható attól, hogy helyreállt a szolgáltatás (gyökérok, ismétlődést megelőző intézkedések és okozott kár és költség információk is kellene hozzá): érdemes ezt a nyilvántartásba is jelezni vagy követni (incidensjegy vs. Problemjegy)

DORA SZERINTI JELENTŐS INCIDENSEK



Beküldött incidensek száma

107

Kezdeti és időközi állapotú incidensek: 7

Beküldött bejelentések száma

406

Kezdeti: 99, Időközi: 142, Záró: 154, i

Beküldött fenyegetések száma

1

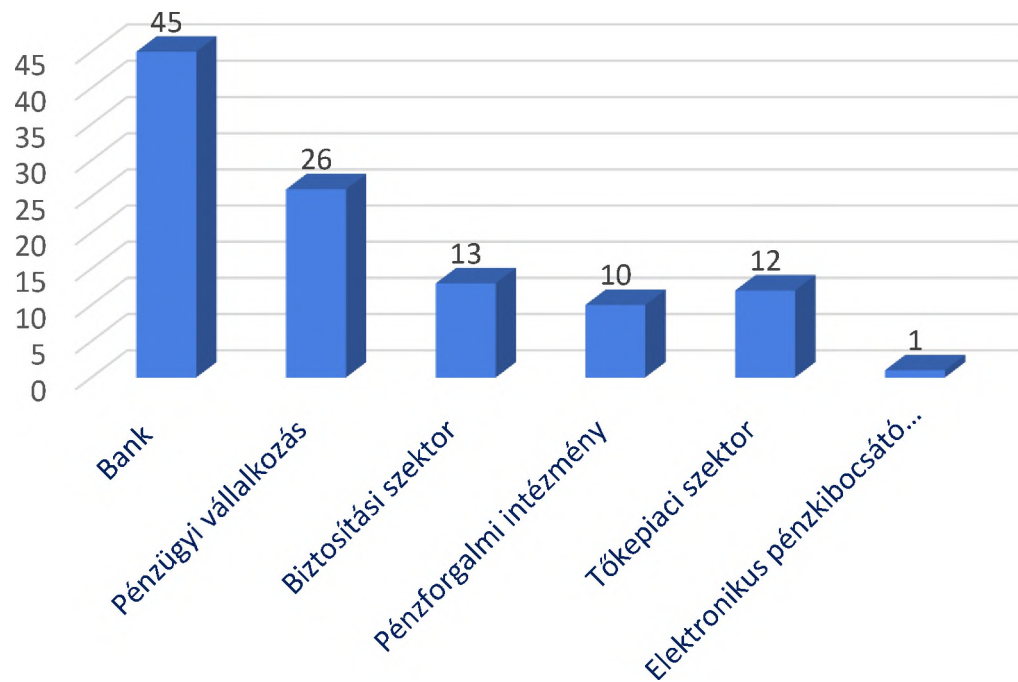
Nyitott fenyegetettségek: 1

Érintett intézmények száma

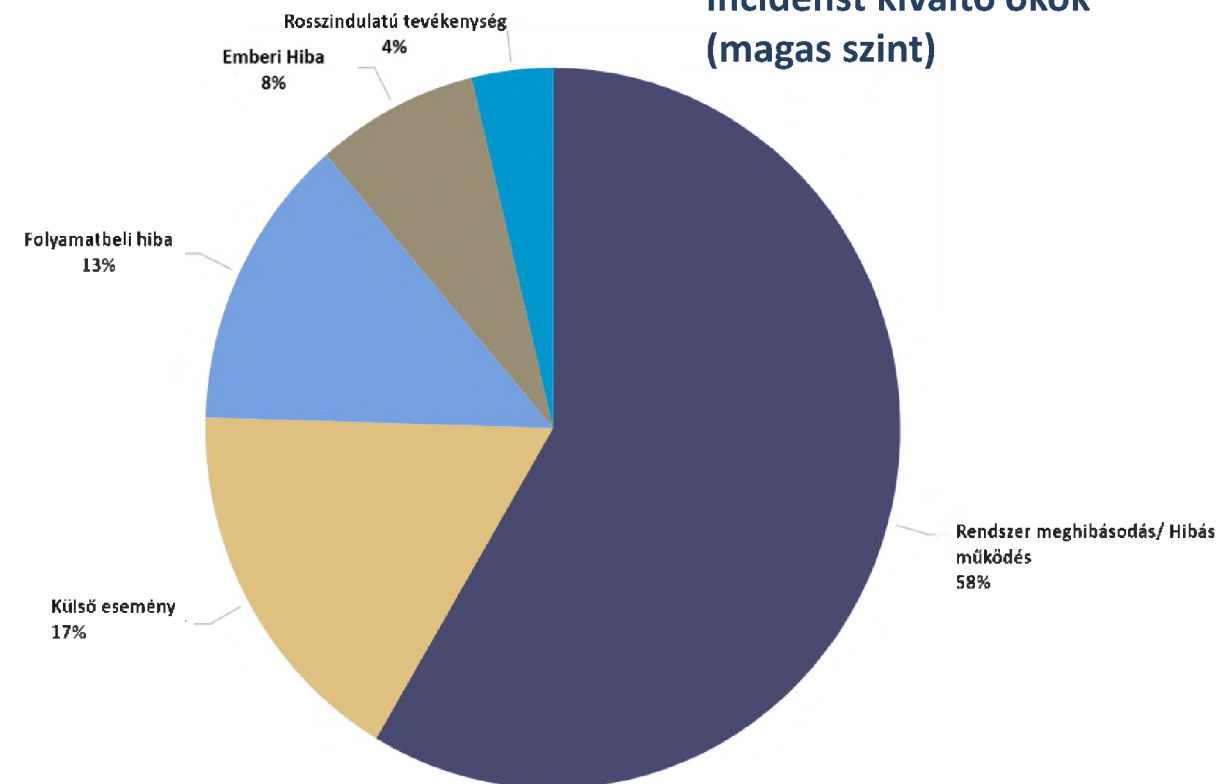
31

Intézmények (kezdeti és időközi incidenssel): 5

Incidensek eloszlása

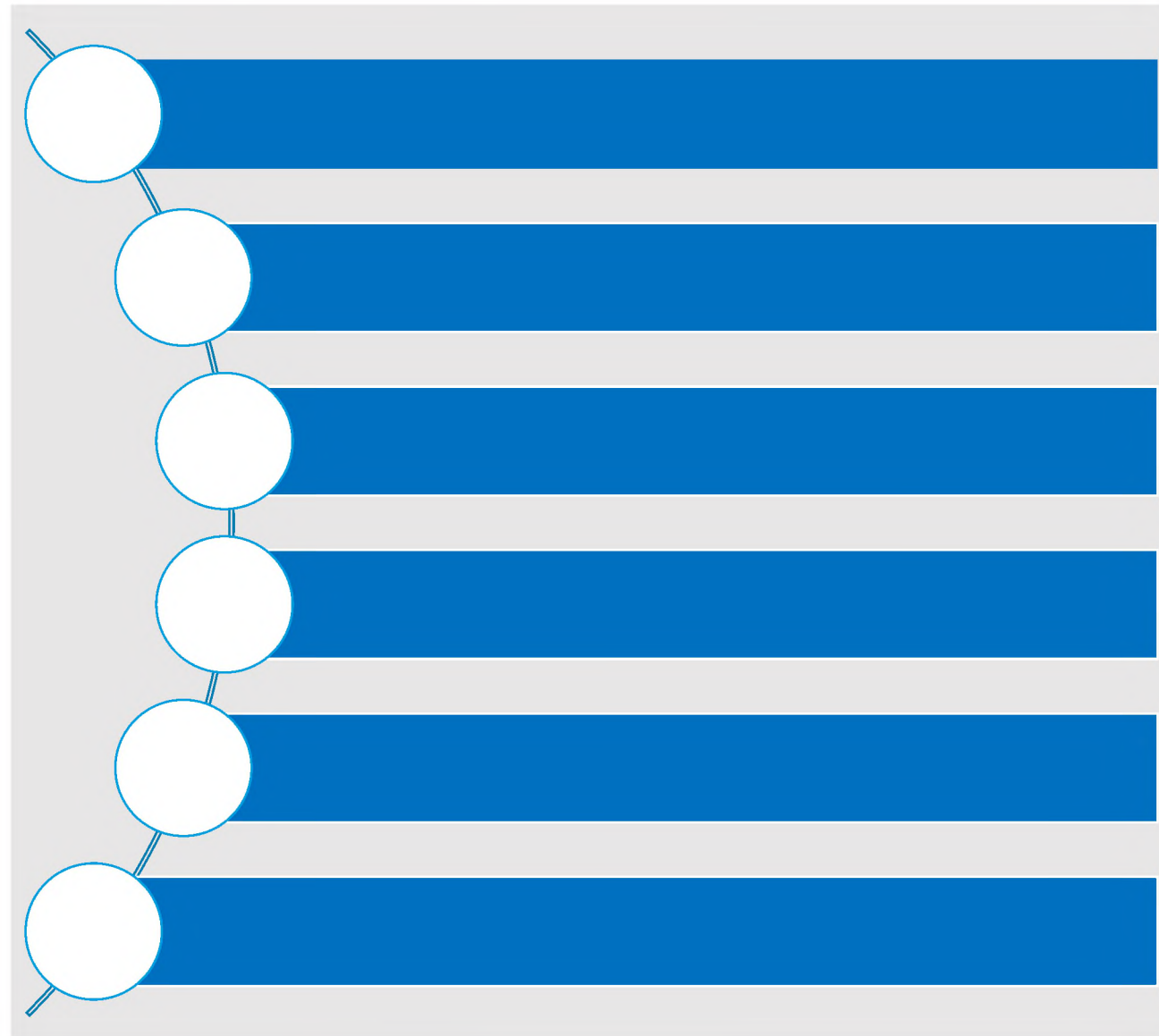


Incidenst kiváltó okok (magas szint)



BEJELENTÉSI PLATFORM

- 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.



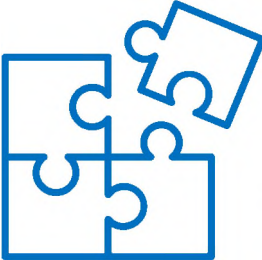
INCIDENS BEJELENTÉSI PLATFORM



This screenshot shows the main interface of the incident reporting platform. On the left, there is a dark sidebar with several menu items, each with a right-pointing arrow. The main area features a table with several rows and columns, some of which contain blurred text. Below the table is a large, empty text input area. At the top of the main area, there are some navigation controls and a search bar.

This screenshot shows a sidebar menu with a language selector at the top set to 'HU'. Below it, there are several menu items, each with a right-pointing arrow. At the bottom of the sidebar, there are several input fields and a dropdown menu.

This screenshot shows a form or list view with multiple input fields. Some fields contain blurred text, while others have visible text like '54' and 'en'. A vertical column of question mark icons is on the right side of the form. The top of the form has a light blue header bar.

- 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!

A stylized, light blue graphic element consisting of several overlapping, curved lines that form a complex, abstract shape, possibly resembling a knot or a decorative flourish, positioned below the main text and a horizontal line.