Tikos Anita | főosztályvezető

Őszi könyvvizsgálói kamarai előadások | 2026.11.12.

A DORA RENDELET HATÁSA A FELÜGYELET ELVÁRÁSAIBAN, A KÖNYVVIZSGÁLAT SZEREPE

MNB INFORMATIKAI FELÜGYELETI FŐOSZTÁLY

- Feladat: a pénzügyi szektor informatikai és információbiztonsági felügyelése (bank, biztosító, pénztár, bef. váll., pv. stb.)
- Cél: a felügyelt intézmények *biztonságos és megfelelő* funkcionális működésének ellenőrzése
- Jogi Háttér: ágazati jogszabályok, DORA rendelet és MNB ajánlások



FELÜGYELÉSI TEVÉKENYSÉG



Vizsgálatok

- Átfogó
- Téma
- Célvizsgálat



Adatszolgáltatások

- Incidens bejelentések
- Keretrendszer felülvizsgálati jelentések
- Negyedéves adatszolg.
- Szolgáltatói szerződések



Auditok, tesztek

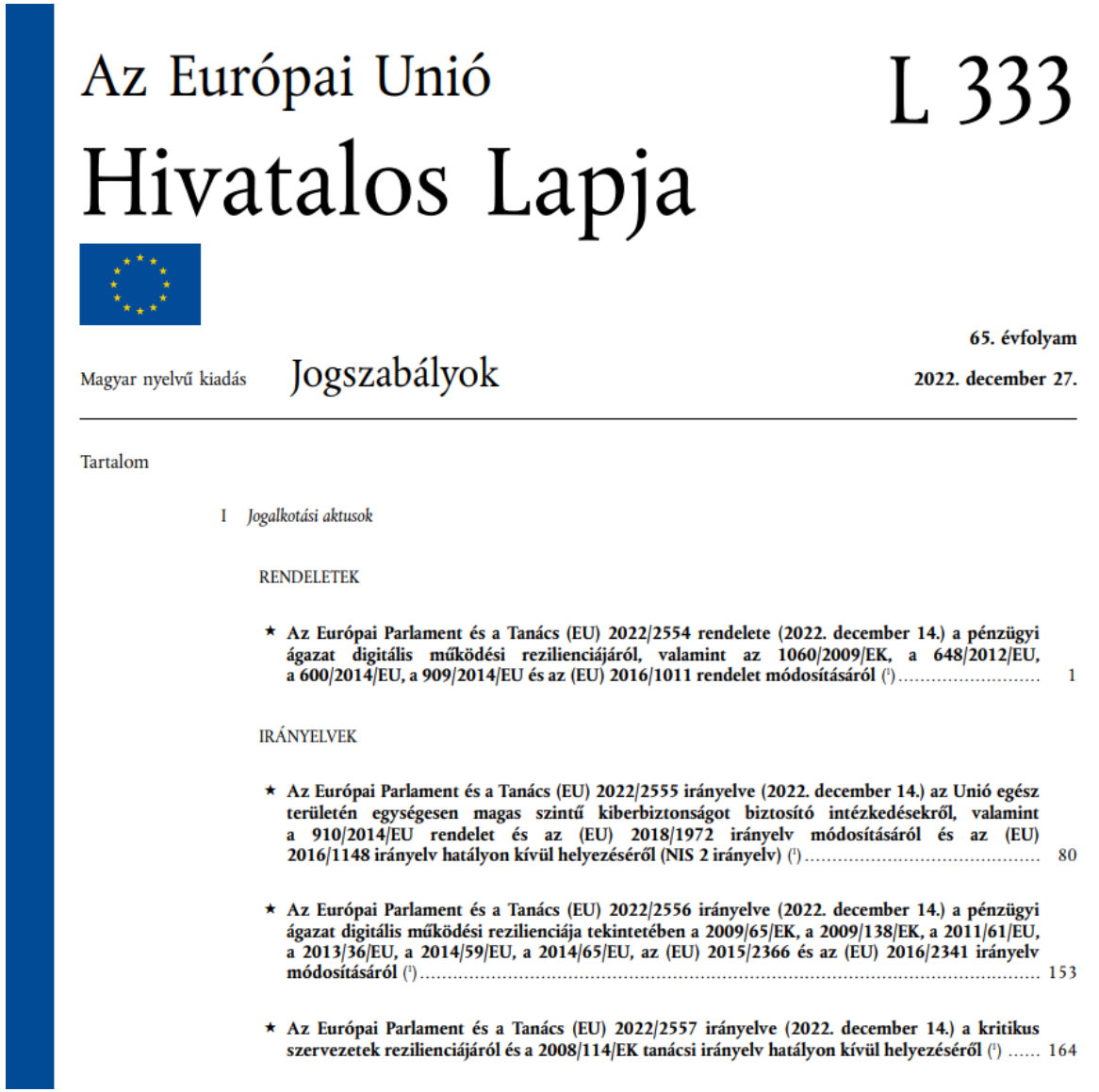
- Külsős auditok
- Belső ellenőri auditok
- **Könyvvizsgálati jelentés IT része**
- Technológiai tesztek (pl. sérülékenységvizsgálatok)
- Tanusítványok

Összesen közel **4 000** darab off-site feladat megvalósítása két év alatt

DORA RENDELET

DORA végleges szövegének elfogadása 2022. június 29-30.

Alkalmazandó: 2025. január 17.



Az Európai Unió

Hivatalos Lapja

L 333

Magyar nyelvű kiadás Jogszabályok

65. évfolyam

2022. december 27.

Tartalom

I *Jogalkotási aktusok*

RENDELETEK

★ **Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról** (1) 1

IRÁNYELVEK

★ **Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)** (1) 80

★ **Az Európai Parlament és a Tanács (EU) 2022/2556 irányelve (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciája tekintetében a 2009/65/EK, a 2009/138/EK, a 2011/61/EU, a 2013/36/EU, a 2014/59/EU, a 2014/65/EU, az (EU) 2015/2366 és az (EU) 2016/2341 irányelv módosításáról** (1) 153

★ **Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről** (1) 164

RÉSZLETSZABÁLYOK

12 hónap

- Kockázatkezelési keretrendszer (RTS): 2024/1774. sz. rendelet
- Egyszerűsített IKT kockázatkezelési keretrendszer (RTS): 2024/1774 sz. r.
- IKT szolgáltatásokra vonatkozó szabályzati elvárások (RTS):
- Események osztályozásának kritériumai (RTS): 2024/1772 sz. rendelet
- Harmadik fél szolgáltatókról szóló nyilvántartás (ITS): 2024/2956 sz. végrehajtási rendelet

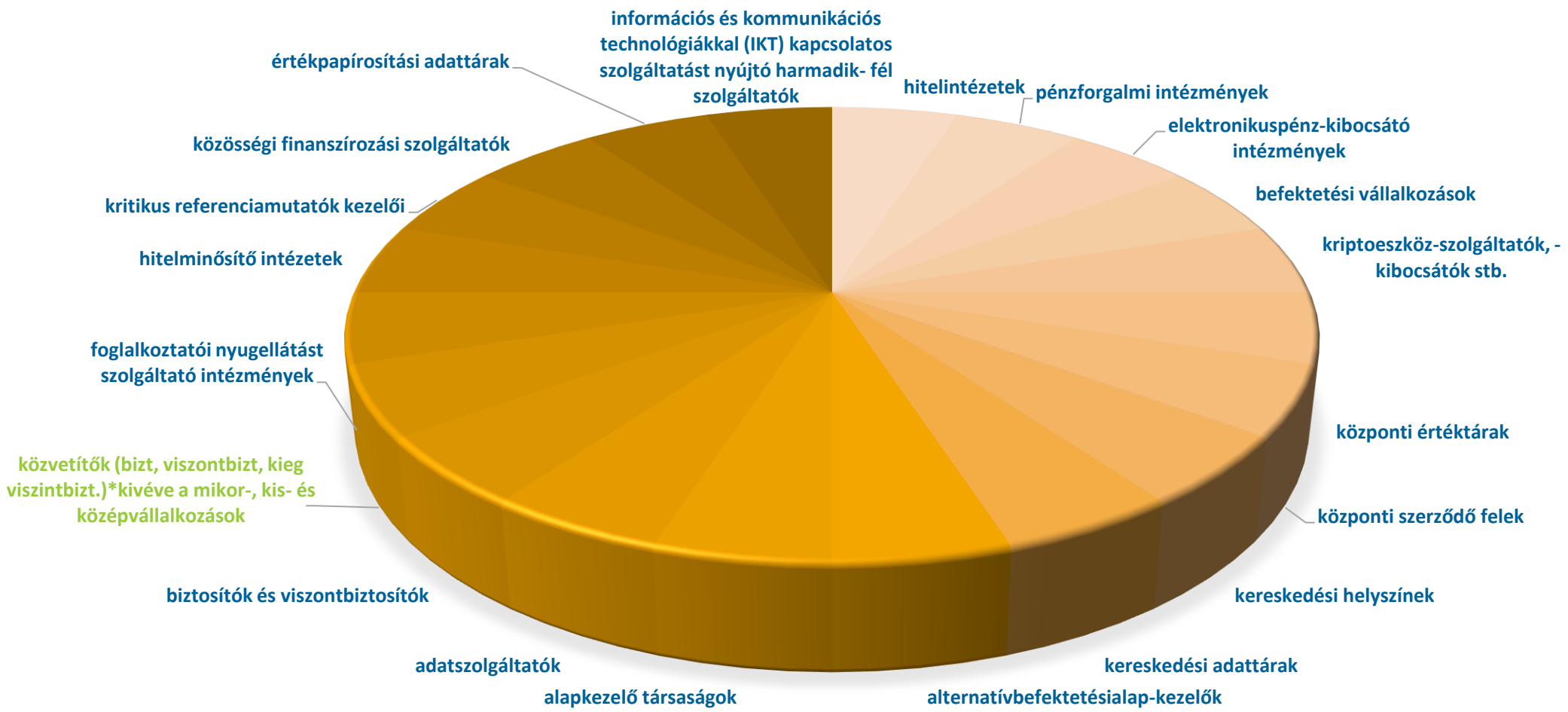
18 hónap

- TLPT teszt (RTS) 2025/1190 sz. rendelet
- Alvállalkozók alkalmazásának feltételei (RTS) 2025/532 sz. rendelet
- Események bejelentési szabályai (RTS): 2025/301 sz. rendelet
- Események bejelentéseinek tartalma (ITS): 2025/302 sz. végrehajtási rendelet
- Események okozta kár/költség becslésének módja (GL)
- ESA-k és a tagállami hatóságok közötti együttműködés (GL) (végleges)
- A felvigyázói tevékenységgel kapcsolatos feltételek/ információk harmonizálása (RTS): 2025/295 sz. rend

24 hónap

- Megvalósíthatósági tanulmány az IKT vonatkozású események központosított EU-s bejelentési felületére (végleges)

DORA HATÁLYA (21 ENTITÁS)



A RENDELET NEM ALKALMAZANDÓ:

- 2013/36/EU irányelv 2. cikke (5) bekezdésének 3. pontjában említett postai elszámolóközpontok;
- a 2011/61/EU irányelv 3. cikkének (2) bekezdésében említett alternatívbefektetésialap-kezelők;
- a 2009/138/EK irányelv 4. cikkében említett biztosítók és viszontbiztositók;
- olyan nyugdíjkonstrukciókat működtető foglalkoztatói nyugellátást szolgáltató intézmények, amely nyugdíjkonstrukciók összesen nem rendelkeznek tizenötnél több taggal;
- a 2014/65/EU irányelv 2. és 3. cikke alapján mentességet élvező természetes vagy jogi személyek;
- A tagállamok kizárhatják e rendelet hatálya alól a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett, saját területükön található jogalanyokat, Magyarországon az **„MFB Magyar Fejlesztési Bank Zártkörűen Működő Részvénytársaság” és a „Magyar Export-Import Bank Zártkörűen Működő Részvénytársaság**”.

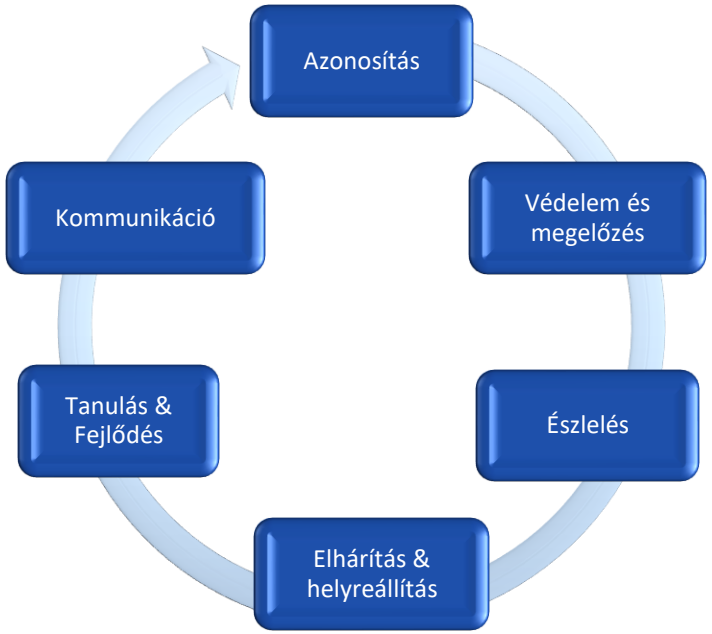
DORA RENDELET FELÉPÍTÉSE

- IKT-kockázatkezelés
- IKT-vonatkozású biztonsági események
- Digitális működési ellenállóképesség tesztelése
- Harmadik féltől eredő IKT-kockázatok kezelése
- Információ megosztásra vonatkozó megállapodások
- Kompetens hatóságok

IKT-KOCKÁZATKEZELÉS

- Irányítás és szervezeti felépítés (irányító testület felelőssége)
- IKT kockázatkezelési keretrendszer
- IKT-rendszerek, -protokollok, -eszközök
- Azonosítás (adatvagyon és eszköz osztályozás)
- Védelem és megelőzés
- Észlelés
- Elhárítás és helyreállítás (BCP, DRP)
- Biztonsági mentési szabályzatok és helyreállítási módszerek
- Tanulás és alkalmazkodás
- Kommunikáció

Az IKT-kockázatkezelési eszközök, módszerek, folyamatok és szabályzatok további harmonizációja (RTS)



IKT-KOCKÁZATKEZELÉS
Főbb újdonságok (példák)

Szabályok kidolgozása a harmadik fél IKT-szolgáltatók által nyújtott **IKT szolgáltatások igénybevételéről szóló megállapodásokra**

Az IKT-kockázatkezelési keretrendszert dokumentálni kell, és **legalább évente** egyszer felül kell vizsgálni, vagy változáskor (kivéve mikrovállalkozások: időszakonként)

BCP és DRP tervek tesztelése évente (vagy kritikus, fontos funkciót támogató rdsz. változása esetén)

legalább évente, vagy: a technológiák, alkalmazások vagy rendszerek összekapcsolása előtt és után, célzottan értékelniük kell valamennyi elavult IKT-rendszer IKT-kockázatait (kivéve mikrovállalkozások)

EGYSZERŰSÍTETT IKT-KOCKÁZATKEZELÉSI KERETRENDSZER „MINI DORA”

Megbízható és dokumentált IKT-kockázatkezelési keretrendszert kell létrehozniuk és fenntartaniuk

Folyamatosan nyomon kell követniük valamennyi IKT rendszer biztonságát és működését

Minimalizálniuk kell az IKT-kockázat hatását […]

Azonosítaniuk kell a harmadik fél IKT szolgáltatótól való függőségeket

Biztosítaniuk kell a kritikus és lényeges funkciók folytonosságát BCP tervekkel […]

Rendszeresen tesztelni kell a fenti tervek és kontrollok hatékonyságát

IKT-kockázatkezelési keretrdsz.-t **dokumentálni kell, időszakonként** és jelentős IKT-vonatkozású események bekövetkezésekor **felül kell vizsgálni.**

IKT-VONATKOZÁSÚ BIZTONSÁGI ESEMÉNYEK

Kezelés

- Egy az IKT-val kapcsolatos események nyomon követésére és naplózására, alkalmas folyamat kidolgozása, alkalmazása,
- **Jelentős incidensek esetén:** felsővezetés tájékoztatása, után követés, Kommunikáció: belső, külső (ügyfél és média tájékoztatása, ügyfélpanasz) és partner pü. szervezetek

Osztályozás

- Az IKT vonatkozású incidensek osztályozása a rendelet kritériumai alapján (RTS-ben meghatározott részletek, küszöbértékek alapján):
  - érintett ügyfelek száma vagy relevanciája
  - esemény időtartalma (leállási idő is)
  - földrajzi kiterjedés
  -adatvesztések
  - érintett szolgáltatás kritikussága
  - gazdasági hatás

NIS irányelvvel harmonizáció!

Bejelentés

- Az incidensek bejelentése a tagállami hatóságoknak (ESAk által kidolgozás alatt álló egységes űrlapok alkalmazásával): Kezdeti, időközi és záró jelentések!
- NCA továbbítja az ESA-nak szükség esetén

Alkalmazandó: pénzforgalmi vonatkozású működési vagy biztonsági eseményekre, valamint a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekre is

DIGITÁLIS MŰKÖDÉSI ELLENÁLLÓKÉPESSÉG

- **Általános tesztelésre vonatkozó követelmények:** (kock. kezelési keretrendszer része); **kulcsfontosságú IKT-rendszerek, alkalmazások tesztelése legalább évente**
- Az IKT-eszközök és rendszerek tesztelése (tesztek felsorolása)
- Az IKT-eszközök, rendszerek és folyamatok „fejlett módszerekkel” történő, **fenyegetettségi alapú behatolási tesztelése (TLPT):** (nagyon komplex, idő és humánerőforrás igényes teszt)

  - kritikus vagy fontos funkciókat támogató éles rendszereken * **kivéve: 16. cikk szerinti intézmények és mikrovállalkozások**
  - Harmadik fél IKT szolgáltatóra is kiterjedhet
  - 3 évente –hatósági döntés alapján lehet eltérő-
- Fontos kérdés: kölcsönös elismerés, kompetens hatóság
- A tesztelőkre vonatkozó követelmények **(TLPT)**

RTS: A TLPT részletszabályai

HARMADIK FÉLTŐL EREDŐ IKT-KOCK. KEZELÉS

IKT harmadik fél szolgáltatók (TPP) kockázatainak kezelésének harmonizálása	• Minimum követelmények meghatározása • Az IKT TPP-k kockázatok teljes körű monitorozása a szerződéses jogviszony teljes életciklusán (szerződéskötés, teljesítés, megszüntetés)
Uniós felvigyázói keretrendszer a kritikus IKT harmadik fél szolgáltatókra vonatkozóan	• **Felvigyázó: ESA-k (főbb vitapont, EBA, EIOPA, vagy ESA-k)** • Kritikus kijelölés: ESA-k által (tagállami adatszolg. alapján) • Felvigyázói Fórum – szektorokon átívelő koordináció az IKT kockázatok vonatkozásában, tagjai az NCA-k i, itt történik a döntések és javaslatok előkészítése
TPP-vel kötendő szerződéses megállapodások	• **Főbb alapelvek** (arányosság; Pü intézmény felelőssége, dokumentáció) • **Register of information:** intézményi lista a szerződéses TPP-kről (Részletek RTS-ben) • Koncentrációs kockázat előzetes felmérése • Főbb szerződéses követelmények (SLA, adatvédelmi intézkedések, ellenőrzés stb).

KÖSZÖNÖM A FIGYELMET

Tikos Anita
főosztályvezető

INFORMATIKAI
FELÜGYELETI
FŐOSZTÁLY

1122 Bp., Krisztina krt. 6.
Telefon: +36 1 489 9753
Email: tikosa@mnb.hu