Tikos Anita I Vezető felügyelő

Hétpecsét: Információvédelem menedzselése Szakmai fórum
2022.11.16.

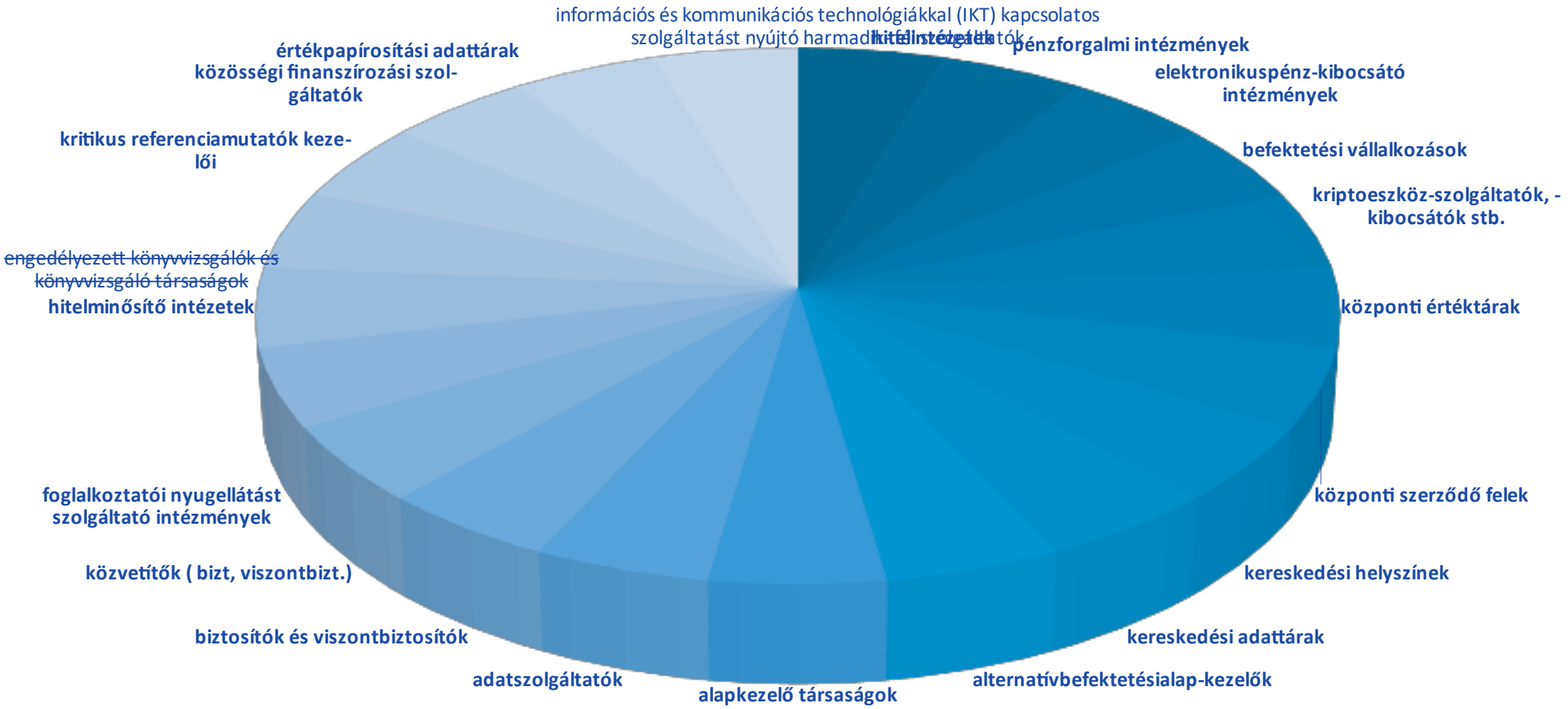
DORA RENDELET: A PÉNZÜGYI SZEKTOR DIGITÁLIS ELLENÁLLÓKÉPESSÉGÉRE VONATKOZÓ ÁTFOGÓ EU-S SZINTŰ SZABÁLYOZÁSA

RENDELET CÉLJA

- Meglévő szabályozási környezet harmonizálása (a teljes pénzügyi szektorra)
- Incidensjelentési kötelezettségek egységesítése/bevezetése
- A harmadik fél szolgáltatókkal kapcsolatos kockázatok kezelése
- NIS irányelvhez szektorspecifikus lex specialis
- Arányosság elve szerinti alkalmazás

Forrás | MNB

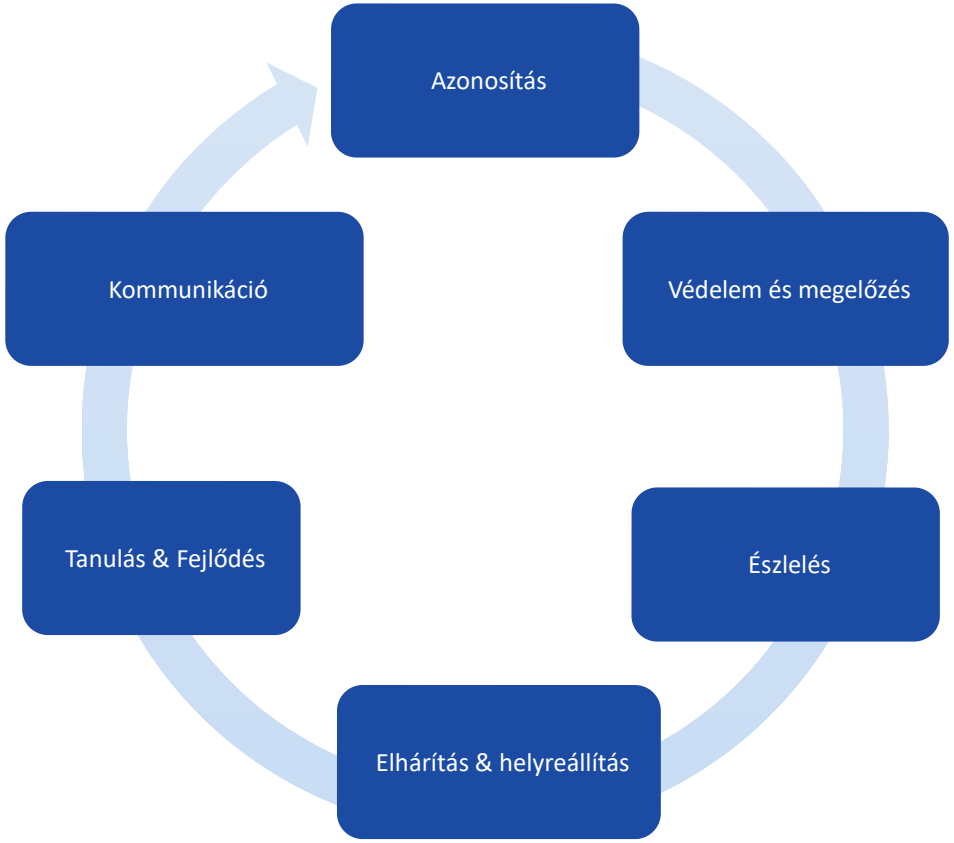
DORA HATÁLYA



Forrás | MNB

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)*



Forrás | MNB

IKT-VONATKOZÁSÚ BIZTONSÁGI ESEMÉNYEK

Kezelés

- Egy az IKT-val kapcsolatos események nyomon követésére és naplózására alkalmas folyamat kidolgozása, alkalmazása

Osztályozás

- Az IKT vonatkozású incidensek osztályozása (a későbbi RTS-ben meghatározott szempontok alapján)

Bejelentés

- Az incidensek bejelentése az NCA-knak az ESAk által kidolgozandó egységes űrlapok alkalmazásával;
  NCA továbbítja az ESA-nak szükség esetén

NIS irányelvvel harmonizáció!

RTS: az incidensek osztályozásának részletszabályaira, bejelentési űrlapra, incidens által okozott kár kiszámítása
Riport: egy későbbi EUs központosított reporting felület lehetőségéről

Forrás I MNB

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)**

  (3 évente, nagyon komplex, idő és humánerőforrás igényes teszt)
  Fontos kérdés: kölcsönös elismerés, kompetens hatóság)
- A tesztelőkre vonatkozó követelmények **(TLPT)**

RTS: A TLPT részletszabályai

Forrás | MNB

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).

Forrás | MNB

HARMADIK FÉL SZOLG. FELVIGYÁZÁSA

Feladatok	• IKT kockázatkezelés, fizikai biztonság, irányítás, incidenskezelés ellenőrzése • Adathordozhatóság megvalósíthatóságának ellenőrzése • IKT tesztelés ellenőrzése • Nemzeti és nemzetközi szabványok, követelményrendszer alapján
Ellenőrzési jogok	• Dokumentumok, információk bekérése • Ellenőrzések végrehajtása – akár on-site vizsgálat • Riportok kérése • Követelmények megfogalmazása
Nem megfelelés esetén	• EBA közzéteszi honlapján a meg nem felelést • Tájékoztatja a nemzeti felügyeleti hatóságot • Harmadik fél szolg.-nak értesítenie kell ügyfeleit a meg nem felelésről • Az intézménynek kezelnie kell a kockázatot
Felvigyázói bírság	• Adatszolgáltatás elmaradása, a hozzáférés és az ellenőrzés megtagadása esetén
Nemzeti szintű végrehajtás	• NCA részvétele a vizsgálati csapatban • NCA kikényszeríti és nyomon követi nyomon a végrehajtást (felügyelt intézmények oldaláról)

Forrás | MNB

HATÁLYBA LÉPÉS ÉS AZT FELADATOK

Várható megjelenés: 2023. Q1 → **Alkalmazandó: 2025. Q1**

Nemzeti feladatok:

- nem átültetendő, de kell jogharmonizáció
- MNB informatikai ajánlásainak felülvizsgálata
- incidens bejelentő űrlapok bevezetése

EU-s feladatok:

12 hónap

- IKT kockázatkezelési keretrendszer (RTS)
- Egyszerűsített IKT kockázatkezelési keretrendszer (RTS)
- IKT szolgáltatásokra vonatkozó szabályzati elvárások meghatározása (RTS)
- IKT vonatkozású események osztályozásának kritériumai (RTS)
- IKT harmadik fél szolgáltatókról szóló nyilvántartás űrlapja (ITS)

18 hónap

- TLPT teszt aspektusainak specifikációja (RTS)
- Kritikus vagy fontos funkciók esetén alvállalkozók alkalmazásának feltételei (RTS)
- IKT vonatkozású események bejelentési szabályai (RTS)
- IKT vonatk. események bejelentésének tartalma (ITS)
- A jelentős IKT vonatk. események okozta kár/költség megbecslésének módja (GI.)
- ESAk és a tagállami hatóságok közötti együttműködés a felvigyázási struktúrában (GI.)
- A felvigyázói tevékenységgel kapcsolatos feltételek/információk harmonizálása (RTS)

24 hónap

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

\+ ESA ajánlások felülvizsgálata 18 hónap után

Forrás | MNB

KÖSZÖNÖM SZÉPEN A FIGYELMET!

Anita TIKOS
vezető felügyelő

1122 Bp., Krisztina krt.6.
Telefon: +36-1- 489-9753
Mobil: +36 (30) 902 1251
Email: tikosa@mnb.hu

Forrás I MNB