Tikos Anita I Vezető felügyelő

ISACA
MÁSODIK SZERDA
2023.02.08.

DORA RENDELET: AZ EU PÉNZÜGYI SZEKTOR DIGITÁLIS ELLENÁLLÓKÉPESSÉGRE VONATKOZÓ ÁTFOGÓ SZABÁLYOZÁS

DORA RENDELET ELŐZMÉNY, MEGJELENÉS

Előzmények 2019:

2019 ESAs joint technical advice

2019 december: társadalmi konzultáció

Digitális Pénzügyi Csomag (DFP):

2020. szeptember

- Markets in Crypto-Assets (MiCA)
- DLT Pilot Regime
- **Digital Operational Resilience Act (DORA)**

DORA végleges szövegének elfogadása

2022. június 29-30.

Megjelent az EU hivatalos lapban:

2022. december 27.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2554 RENDELETE

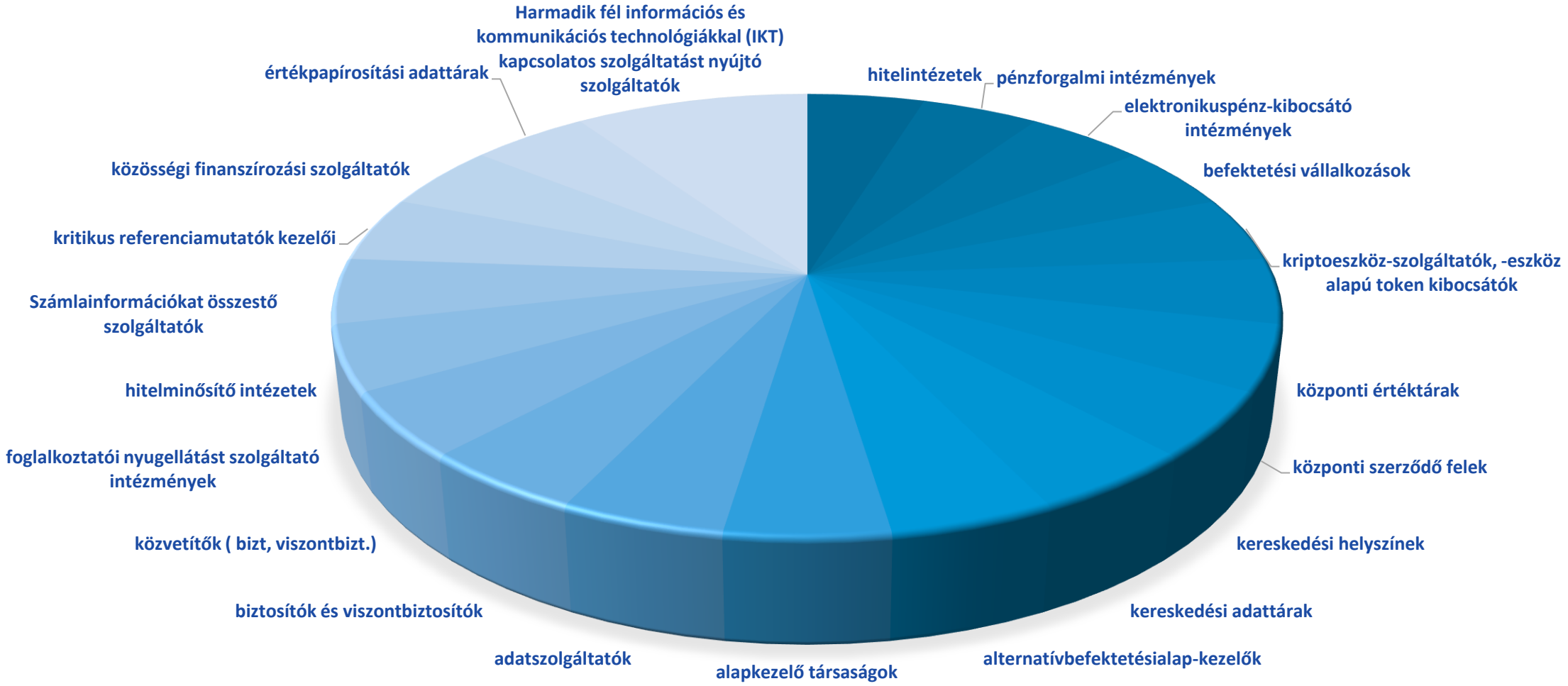
a pénzügyi ágazat digitális működési rezilienciájáról

RENDELET CÉLJA

- Egységes terminológia használata a teljes pénzügyi szektorban EU szerte
- Széttöredezett szabályozási keretrendszer egyesítése
- Incidensjelentési kötelezettségek egységesítése/bevezetése
- A harmadik fél szolgáltatókkal kapcsolatos kockázatok kezelése
- A legnagyobb és legkritikusabb szolgálatók EU-s szintű felvigyázása
- NIS2 irányelvhez (2022/2555 számú irányelv) szektorspecifikus lex specialis
- Arányosság elve szerinti alkalmazás

Forrás | MNB

DORA HATÁLYA

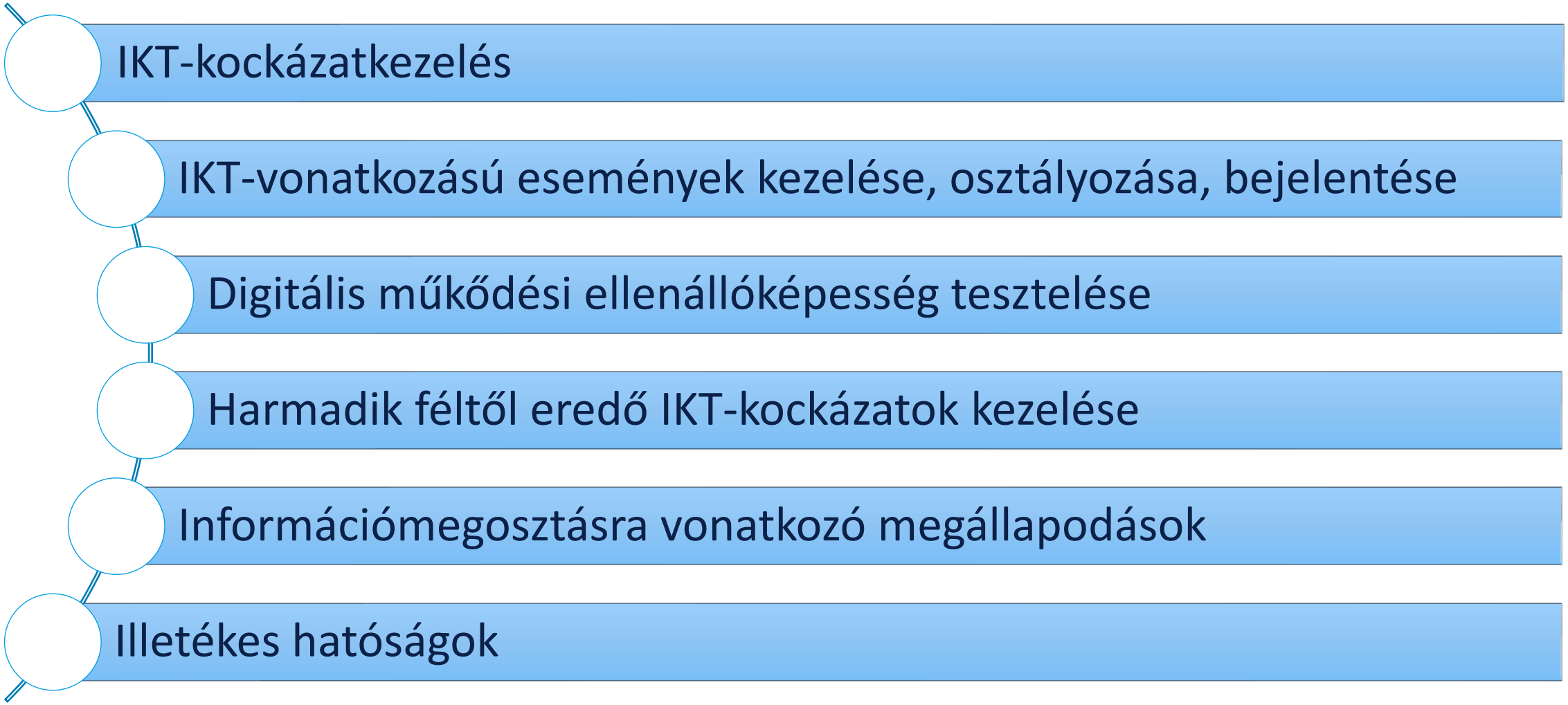


Forrás | MNB

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 viszontbiztosítók;
- 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

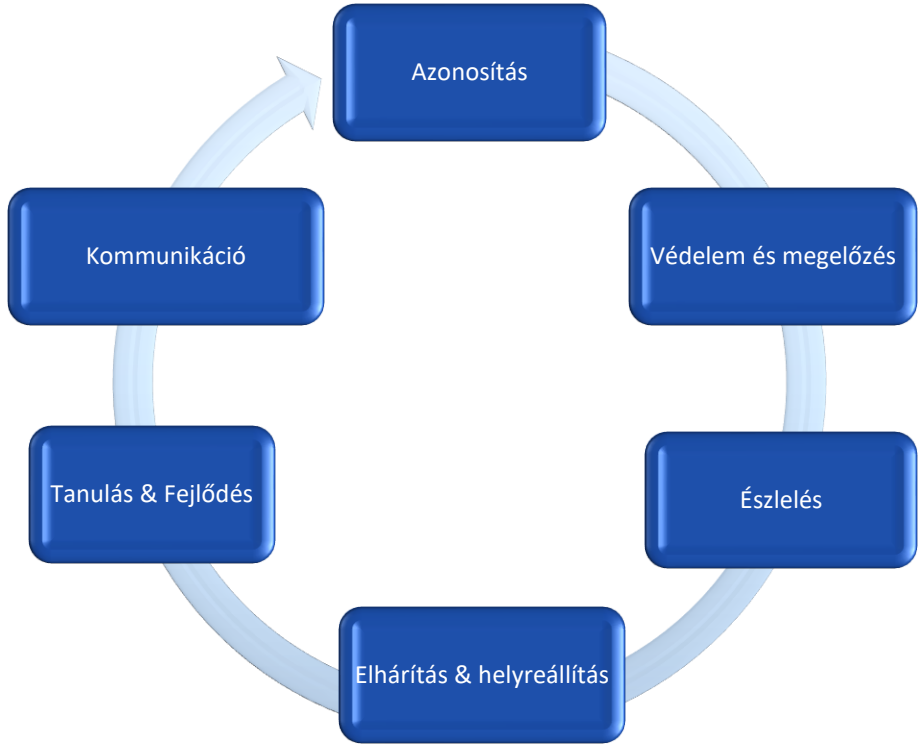


Forrás | MNB

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

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



Egyszerűsített IKT-kockázatkezelési keretrendszer (16. cikk)
„Mini DORA”

Forrás | MNB

IKT-VONATKOZÁSÚ BIZTONSÁGI ESEMÉNYEK

Kezelés

- 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 (a későbbi 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)
- NCA továbbítja az ESA-nak, esetleg tájékoztat más hatóságokat

NIS2 irányelvvel harmonizáció!

RTS: az incidensek osztályozásának részletszabályaira, bejelentési űrlapra, incidens által okozott kár kiszámítása

Riport: egy későbbi EU-s 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)**
  TPLT: nagyon komplex, idő és humánerőforrás igényes teszt
- 3 évente (kivéve mikrovállalkozások és 16. cikk szerinti intézmények)
- 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)
TPP-vel kötendő szerződéses megállapodások	• **Főbb alapelvek** (arányosság; Pü. intézmény felelőssége, dokumentáció) • **Register of information:** intézményi lista a szerződéses TPP-kről (Részletek és űrlap RTS-ben) • Koncentrációs kockázat előzetes felmérése • Főbb szerződéses követelmények (SLA, adatvédelmi intézkedések, ellenőrzés stb.).
Uniós felvigyázói keretrendszer a kritikus IKT harmadik fél szolgáltatókra vonatkozóan	• **Felvigyázó: valamely ESA (EBA, EIOPA, vagy ESMA)** • Kritikus kijelölés: ESA-k által (tagállami adatszolg. alapján) • Felvigyázói Fórum – szektorokon átívelő koordináció az IKT kockázatok vonatkozásában, tagjai az NCA-k is, itt történik a döntések és javaslatok előkészítése • JET: közös vizsgálócsoport – vizsgálatok, ellenőrzések végrehajtása

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	• ESA 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 a végrehajtást (felügyelt intézmények oldaláról)

Forrás | MNB

A RENDELETBŐL ADÓDÓ FELADATOK ÜTEMEZÉSE

Alkalmazandó: 2025. január 17.

EU-s feladatok:

Nemzeti feladatok:

Nem átültetendő, de kell jogharmonizáció

MNB informatikai ajánlásainak és az ágazati jogszabályok felülvizsgálata

DORA szerinti adatszolgáltatások, űrlapok bevezetése

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
Email: tikosa@mnb.hu

Forrás I MNB