Andrási Zoltán| osztályvezető

XVI. AIDA Budapest Biztosítási Kollokvium - 2022.11.25

FELHŐSZOLGÁLTATÁSOK ÉS A BIZTOSÍTÁSOK EGYÉB INFORMATIKAI KIHÍVÁSAI

IT FELÜGYELÉS

A jegybanktörvény alapján az MNB folyamatos felügyeletet gyakorol a pénzügyi ágazati törvények hatálya alá tartozó szervezetek és személyek felett.

Az MNB SZMSZ alapján az Informatikai felügyeleti főosztály látja el a felügyelt intézmények informatikai működésével kapcsolatos felügyeleti feladatokat

17 fő + 2 gyakornok – 40+ nemzetközi minősítés (CISA, CISM, CISSP, CEH, CRISK, CCSP, CDPSE), 300+ év auditori tapasztalat

jogszabály, szabályozó eszközök, tervezés
vizsgálati módszertan

2 év alatt:

- 90+ vizsgálat
- 4500+ db feladat

MÓDSZERTAN

Jogszabály

Vonatkozó pénzügyi ágazati törvények (Hpt., Bszt., Tpt., **Bit**., Kbftv., Öpt., Mpt., **Pmt** stb.)

Az informatikai rendszerek védelméről szóló 42/2015. (III.12.) Korm. rendelet

Pmt. végrehajtására kiadott 26/2020. (VIII.25.) MNB rendelet

Szabályozó eszközök

A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről

A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről

A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről

Vizsgálatot támogató anyagok

Belső szabályzatok, vizsgálati kézikönyv

COBIT alapokra felépített vizsgálati program – 4 fő – 45 altémakör

Sztenderd dokumentációk, technikai vizsgálati segédanyagok

Biztonságirányítás és technikai ismeret megosztása

A 8/2020.(VI.22.) IT AJÁNLÁS BEMUTATÁSA

?

Az ajánlás átfogóan tartalmazza az MNB informatikai rendszerekkel kapcsolatos elvárásait egységesen a felügyelt intézményekre vonatkozóan.

+

A felülvizsgálat során a korábbi ajánlás szerkezete nem változott, de tartalmilag kibővült a szakmailag indokolt kiegészítésekkel és az EBA ICT ajánlás új követelményeivel.

#

A 8/2020. (VI.22.) számú MNB ajánlás 2021. január 1-től alkalmazandó, a korábbi 7/2017 és 15/2015 ajánlások hatályai megszűntek.

Forrás | MNB

A 12/2020.(XI.6.) TÁVMUNKA AJÁNLÁS BEMUTATÁSA

?

A pandémiás helyzet indokolttá tette, hogy távmunkával összefüggő informatikai biztonságra vonatkozó felügyeleti elvárások egy önálló ajánlásban kerüljenek meghatározásra.

+

A távoli hozzáférés a megfelelő tárgyi és technikai feltételek mellett, a vonatkozó jogszabályok betartásával és a biztonsági követelmények figyelembevételével történjen.

#

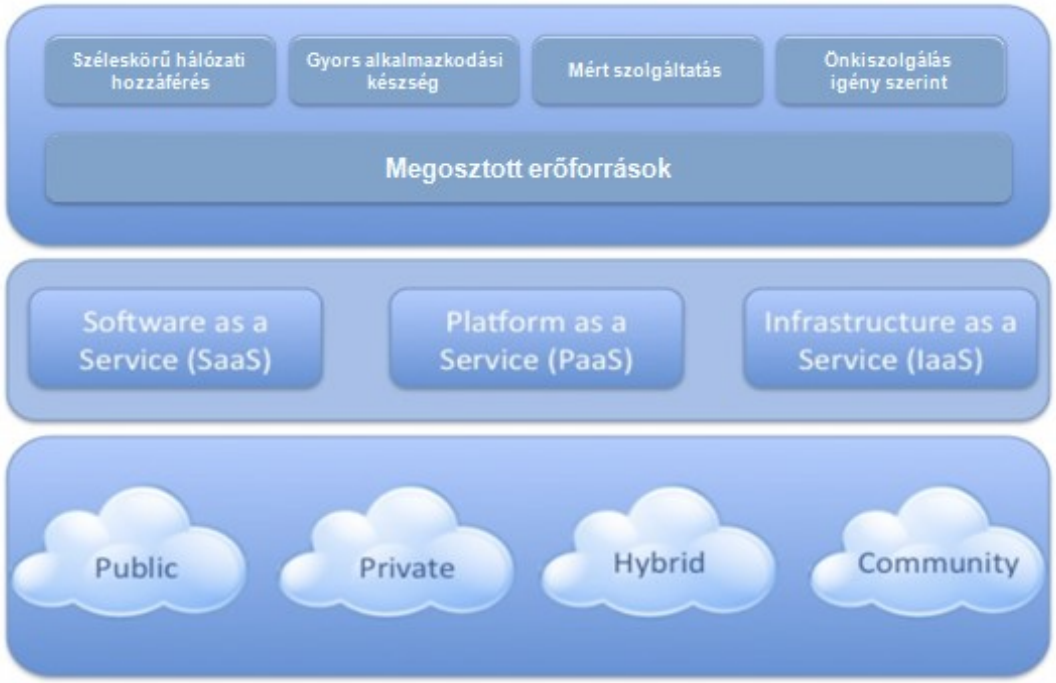
Az ajánlás szerkezetét és elvárásait tekintve illeszkedik a 8/2020.(VI.22.) ajánláshoz, amelynek specifikus kiegészítéseként alkalmazandó.

Forrás | MNB

FELHŐSZOLGÁLATÁS

A FELHŐ MEGHATÁROZÁSA

Felhő = költséghatékony, igény szerinti adattárolási és feldolgozási kapacitás a hálózaton keresztül



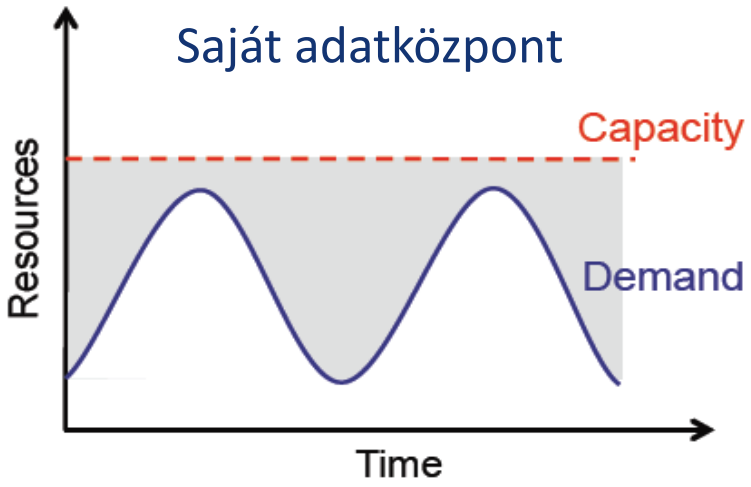
Alapvető ismérvek

Szolgáltatási modellek

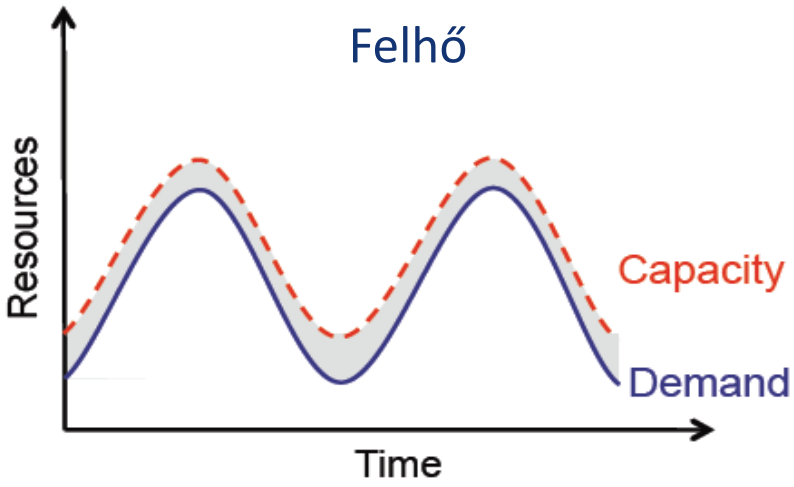
Működtetési modellek

Forrás | [2]

A FELHŐ ELŐNYEI



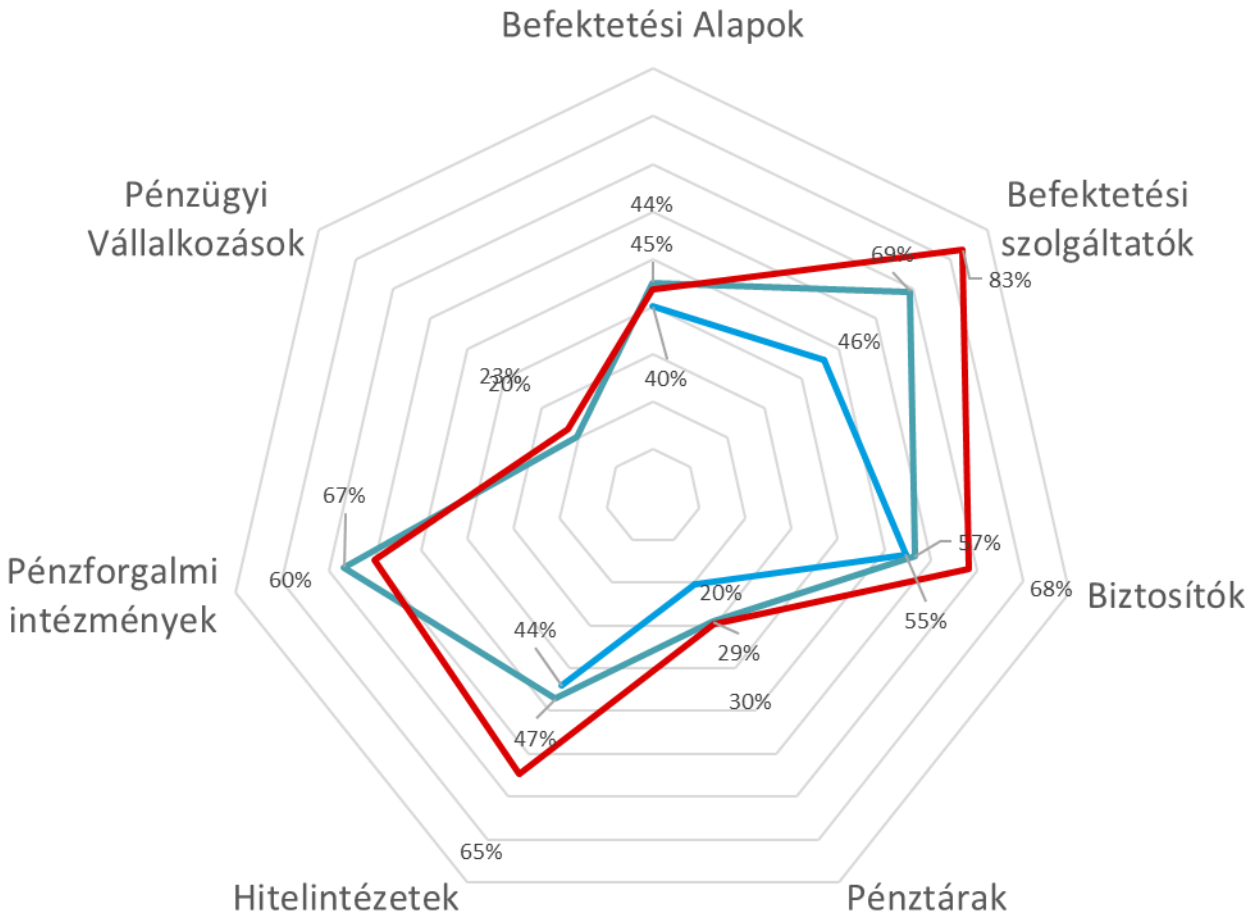
Maximális igénybevételhez méretezett kapacitások -> drága



A változó igénybevételhez alkalmazkodó kapacitások -> gazdaságos

Forrás | MNB

JELENLEGI HELYZET MAGYARORSZÁGON – 1

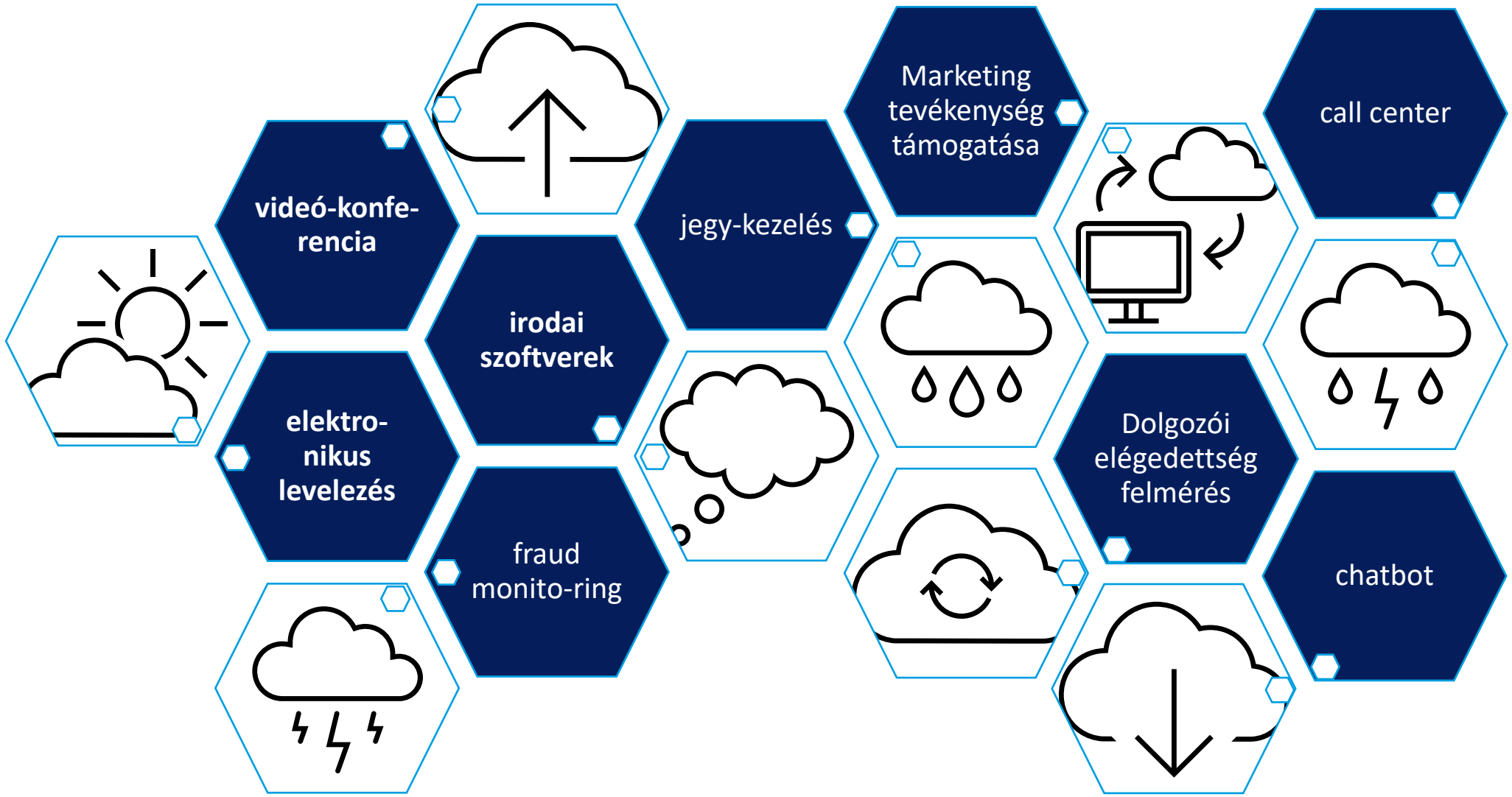


FELHŐSZOLGÁLTATÁST IGÉNYBE VEVŐ INTÉZMÉNYEK ARÁNYA

2020 Q4 – 2021 Q1 – 2022 Q

Forrás | MNB

JELENLEGI HELYZET MAGYARORSZÁGON – 2



Forrás | MNB

FELHŐ ELŐNYEI ÉS KOCKÁZATAI

- Méretgazdaságosság
- Rugalmasság
- Standardizált szolgáltatások
- Gyors, hatékony hibajavítás
- Egyszerű biztonságmenedzsment
- Redundancia, magas rendelkezésre állás
- Egységes kontrollok

- Közvetlen kontroll elvesztése
- Standard szerződéses feltételek
- Adat- és titokvédelmi kihívások
- Adatok elkülönítésének problémái
- Ellenőrizhetőségi gondok
- Jogi megfelelőség problémái
- Kiszolgáltatottság a felhőszolgáltatónak

Forrás | MNB

KONTROLLVESZTÉS VAGY MEGOSZTÁS?

Házon belül	Hosting	IaaS	PaaS	SaaS
App	App	App	App	App
VM	VM	VM	VM	VM
Szerver	Szerver	Szerver	Szerver	Szerver
Tároló	Tároló	Tároló	Tároló	Tároló
Hálózat	Hálózat	Hálózat	Hálózat	Hálózat

Saját kontroll

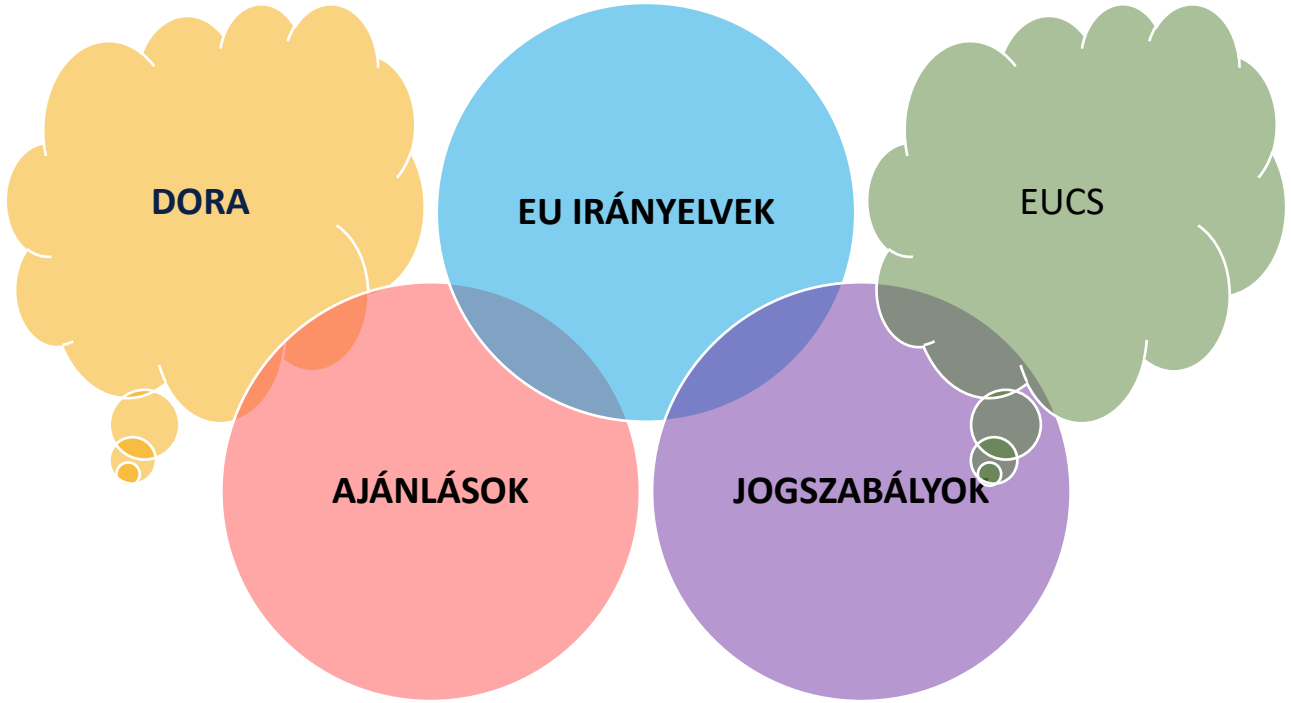
Osztott kontroll

Szállítói kontroll

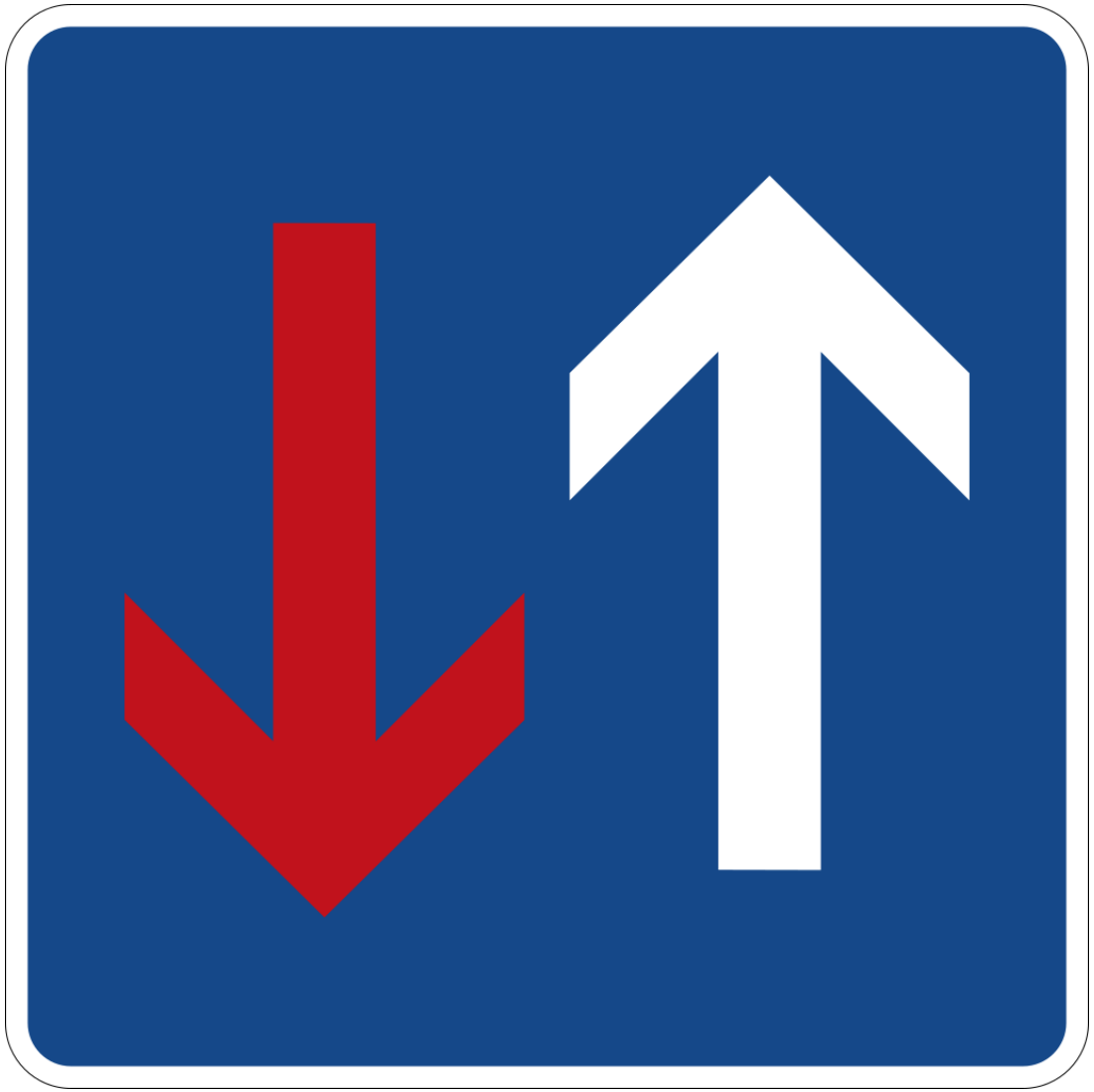
„SHARED RESPONSIBILITY MODEL” vö. RACI

Forrás | MNB

A FELHŐSZOLGÁLTATÁSOK JOGSZABÁLYI KÖRNYEZETE



Forrás | MNB



MAGYAR JOGSZABÁLYOK

- 42/2015. (III. 12.) Korm. Rendelet [4]
- Ágazati jogszabály - Bit.,
- Általános Adatvédelmi Rendelet (GDPR) [5]
- 2013. évi L. törvény (Ibtv.) [6]

Forrás | MNB

A 4/2019.(IV.1.) FELHŐ AJÁNLÁS BEMUTATÁSA

?

A hatályos „a közösségi és publikus felhőszolgáltatások igénybevételéről szóló” 4/2019. (IV.1.) számú MNB ajánlás alkalmazása 2019. május 1-től elvárt.

+

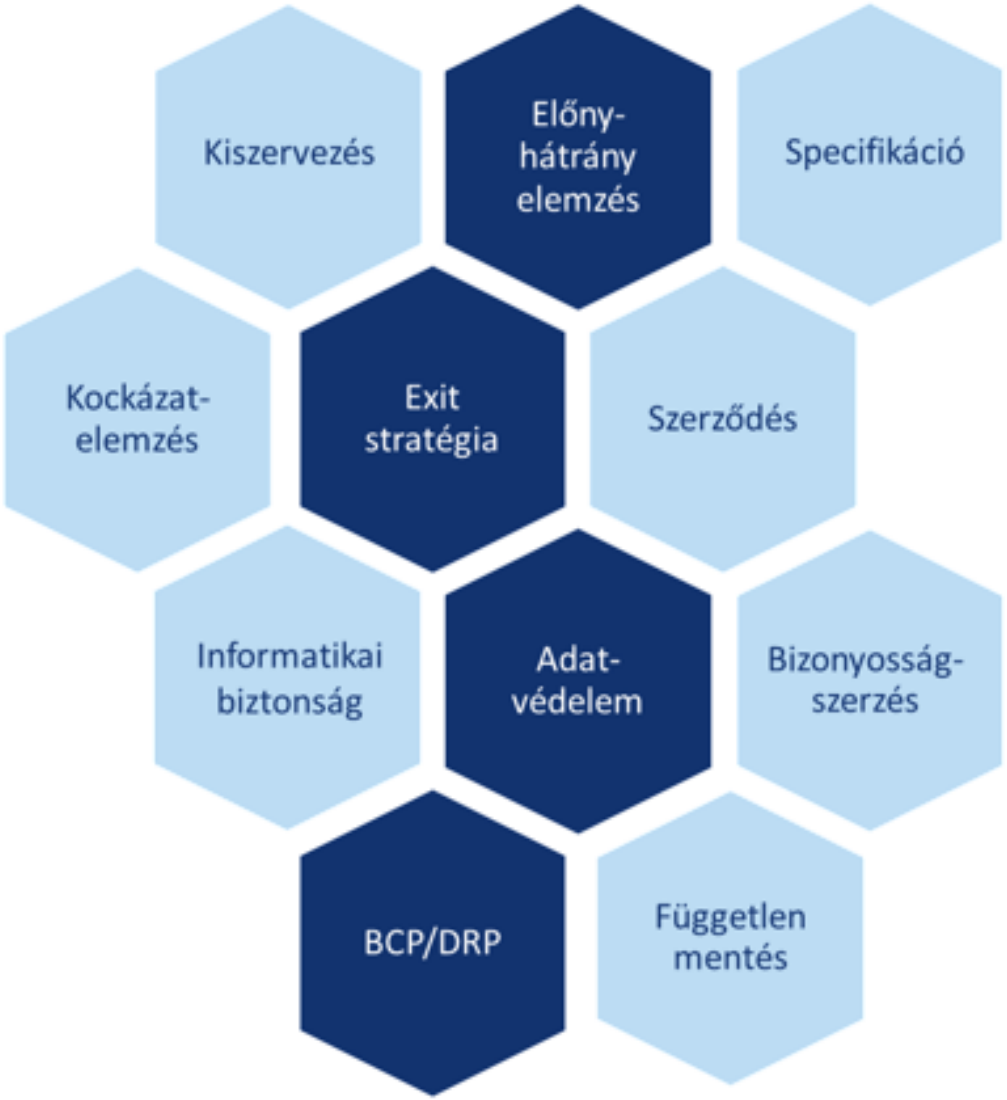
A felülvizsgálat során a korábbi ajánlás szerkezete nem változott, de kibővült az EBA felhő ajánlás új követelményeivel.

#

Fókuszterületek: Költség-haszon elemzés, Exit stratégia, Adat-védelem, BCP/DRP

Forrás | MNB

AZ AJÁNLÁS FÓKUSZTERÜLETEI



Forrás | MNB

FELHŐBIZTONSÁGI ALAPELVEK

Az adatok biztonsága továbbítás közben

A tárolt adatok biztonsága

Adatvédelem

Erőforrások védelme

Informatikai folyamatok biztonsága

Biztonságmenedzsment

Üzemeltetés biztonsága

Fejlesztés biztonsága

Felhasználó- és jogosultságkezelés

Forrás | MNB

KOCKÁZATELEMZÉS

A döntés-előkészítés része.

Teljes kockázatkezelési folyamat.

Jogszabálysértés nem elfogadható kockázat.

Kivezetés kockázatainak kezelése.

Rendszeres felülvizsgálat.

SZERZŐDÉSES KÖVETELMÉNYEK

Felmondás, felmondási idő szabályozása.

Feltétlen ellenőrzési jog.

Adatfeldolgozási helyszínek.

Adatbiztonsági és adatvédelmi elvárások – szolgáltatási lánc.

Folyamatok és rendszerek biztonsági elvárásai.

Incidenskezelési és forensic eljárások.

Forrás | MNB

EXIT STRATÉGIA ÉS AKCIÓTERV

Az üzleti folyamatoknak a kilépés alatt és után is zavartalanul működniük kell.

Szaktudás rendelkezésre kell álljon.

Részletes végrehajtási terveket kell készíteni.

Pesszimista forgatókönyv.

Biztonságos adattörlés és erről való bizonyosság.

BIZONYOSSÁGSZERZÉS

Az Intézmény és a Felügyelet közvetlen ellenőrzési jogát fent kell tartani.

Célszerű független auditokra és tanúsításokra is támaszkodni.

Bizonyossági szintek:

- közepes szintű bizonyosság
- magas szintű bizonyosság

A bizonyosságszerzés álljon összhangban a kockázattal.

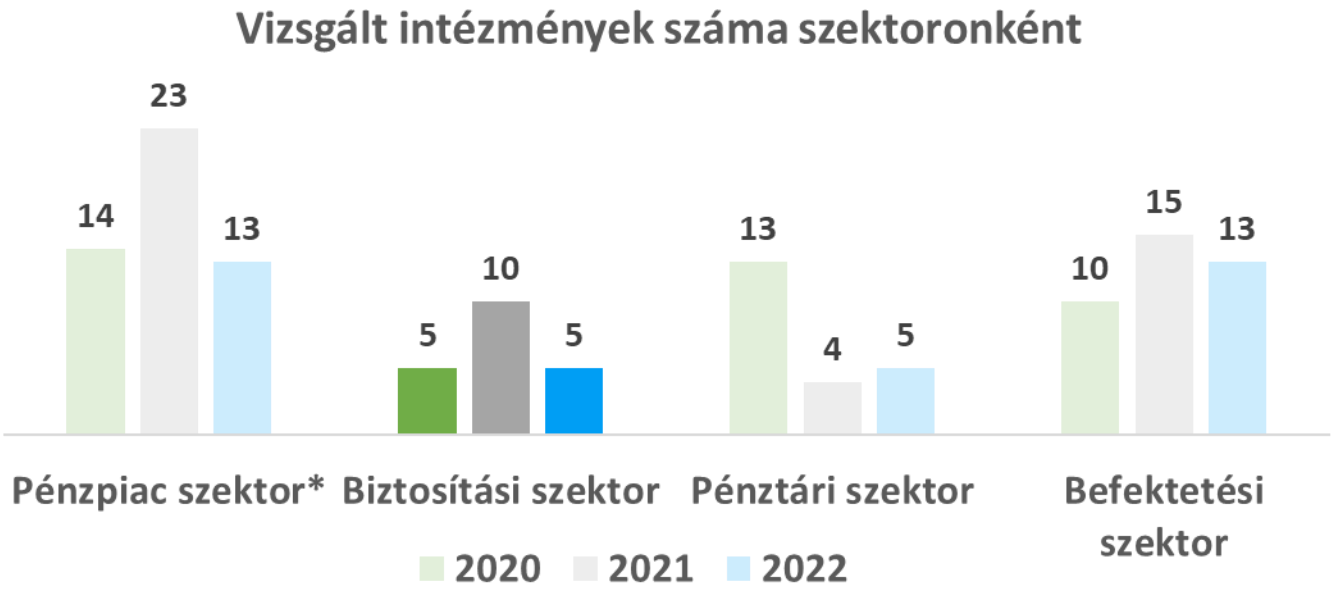
Forrás | MNB

FELÜGYELÉS – HELYSZÍNI VIZSGÁLAT ELLENŐRZÉSI TAPASZTALATOK

INTENZÍV VIZSGÁLAT

9 év alapján évente átlag 50 db vizsgálatban való részvétel.

2020-ban a COVID-19 miatt 11 db vizsgálat (zömében utóvizsgálat) törlésre került.



*Pénzpiac szektor 2020-ban magában foglal 4 db számlainformációs szolgáltatót

KIEMELT ELLENŐRZÉSI TERÜLETEK

2022-es prioritások:

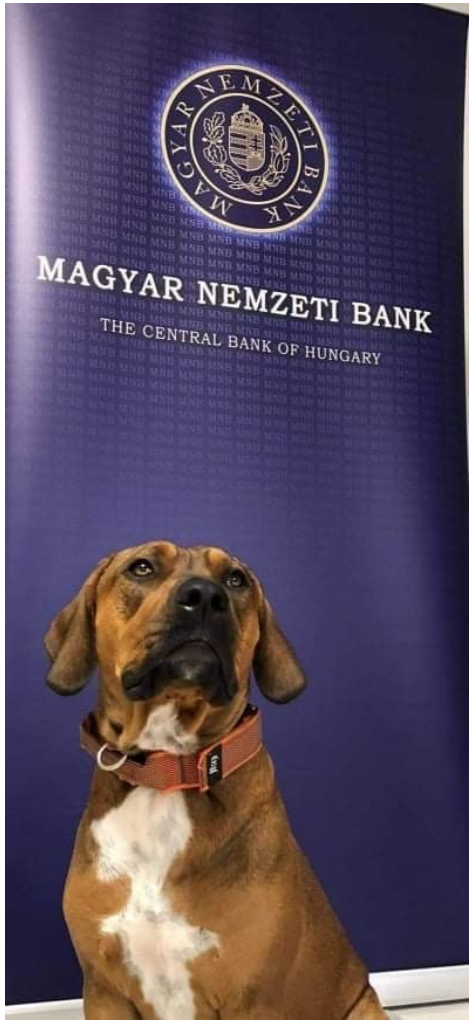
Incidenskezelés vizsgálata
Jogosultságkezelés
Naplózás
Kiberbiztonsági ellenállóképesség vizsgálata

2021-es prioritások:

Online ügyfélazonosítás, online szerződéskötés
Kiberbiztonsági ellenállóképesség vizsgálata
Elavult IT rendszerek

2020-as prioritások:

Az Azonnali Fizetési Rendszer (AFR) követelmények ellenőrzése;
IT biztonság megfelelőségének vizsgálata a pénztáraknál;
Az elavult IT rendszerek kiemelt vizsgálata;
PSD2 követelmények ellenőrzése - témavizsgálat



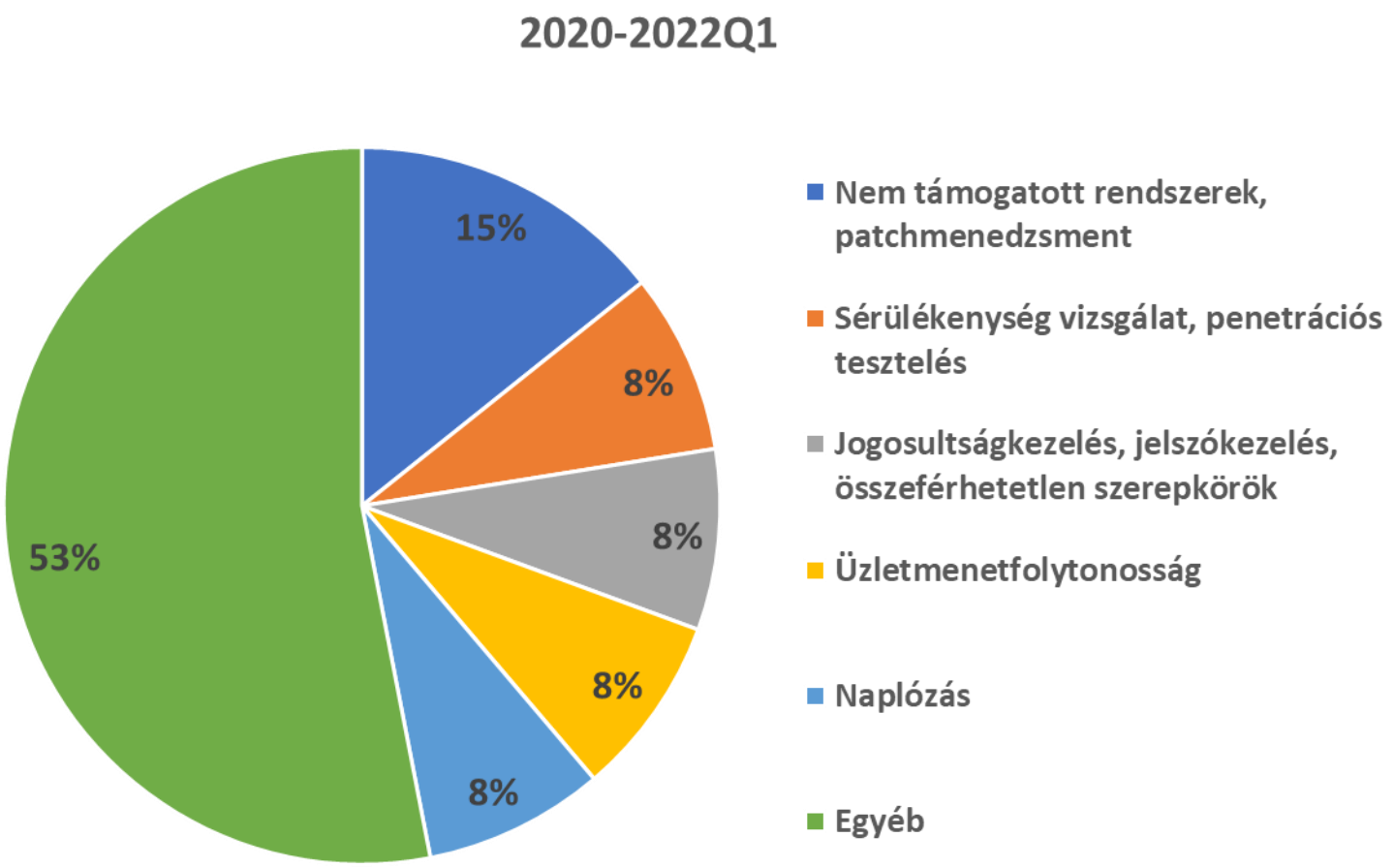
Forrás | MNB

ELLENŐRZÉSI TAPASZTALATOK

LEGPROBLÉMÁSABB TÉMAKÖRÖK

Határozati kötelezés összesen 22 db témakörben született.

A leggyakoribb 5 témakör az összes határozati kötelezés 47%-át teszi ki.



NEM TÁMOGATOTT RENDSZEREK

8/2020.(VI.22.) IT ajánlás – 7. és 8. fejezetei - Hálózati védelem, Logikai védelem

42/2015. (III. 12.) Korm. rendelet

- 3. § (2) bekezdés d) és e) pontjai
- 5/B. § j) és r) pontjai
- 5/A. § (3) bekezdés c) pont cc) alpontja

- szabályozás
- patchmenedzsment
- elavult, támogatás nélküli szoftverek:
  - adatbáziskezelő,
  - operációsrendszer,
  - alkalmazás,
  - hardver

SÉRÜLÉKENYSÉGVIZSGÁLAT ÉS PENETRÁCIÓS TESZTELÉS

8/2020.(VI.22.) IT ajánlás – 13.fejezet – Kiszervezés

42/2015. (III. 12.) Korm. rendelet

- 3. § (2) bekezdés b) és g) pontjai
- 5/B. § b), e), g), h), j) és n) pontjai

- Külső és belső sérülékenységvizsgálatok végrehajtása nem történik
- Penetrációs tesztelés során feltárt hibák nem kerülnek javításra
- Szabályozás
- Internet irányból elérhető szolgáltatások behatolási tesztelése nem történik meg

JOGOSULTSÁGKEZELÉS

8/2020.(VI.22.) IT ajánlás – 9.fejezet - Hozzáférési rend

42/2015. (III. 12.) Korm. rendelet

- 3. § (3) bekezdés c)
- 4. § (1) bekezdés d)
- 3. § (4) bekezdése
- 5/A. § (3) bekezdés c) pont ca) alpontja

- nyilvántartás
- felülvizsgálat
- naplózás
- személyhez rendelés
- összeférhetetlenség
- jelszóbeállítás
- szerepkör szétválasztás
- jelszóboríték

ÜZLETMENET-FOLYTONOSSÁG

8/2020.(VI.22.) IT ajánlás – 11.fejezet – Szolgáltatásfolytonosság

42/2015. (III. 12.) Korm. rendelet

- 3. § (3) bekezdés c) és g) pontjai
- 5/B. § k) pontja

- BCM keretrendszer felülvizsgálata/oktatás/tesztelés nem rendszeres, nem teljeskörű
- dokumentációk kitöltése hiányos (pl. BIA esetében jogszabályi függőség, DRP – tesztelés dátuma)
- DR teszt nem valós – minden nagyon „előkészített”
- DR teszt nem terjed ki minden kritikus rendszerre
- DR felkészültség hiányos (HW, SW) nem jól azonosítottak
- BIA alapján felmért folyamat kritikussága nincs összhangban a jogszabályi elvárással. Alkalmazás szintű helyreállítási teszt nem történik.

NAPLÓZÁS

8/2020.(VI.22.) IT ajánlás – 14.fejezet – Naplózás

42/2015. (III. 12.) Korm. rendelet

- 3. § (2) bekezdés c) és d) pontjai
- 5/A. § (3) bekezdés c) pont cb) alpontja
- 5/B. § f) pontja és g) pontja

- kritikus IT biztonsági események nem naplózottak
- loggyűjtés nem teljeskörű
- naplózási szint nem megfelelő
- naplóelemzés nem történik
- naplózással kapcsolatos elvárások, feladatok csak magas szinten szabályozottak

ÜGYFÉLAZONOSÍTÁS, SZERZŐDÉSKÖTÉS VIZSGÁLAT ELLENŐRZÉSI TAPASZTALATOK

ÜGYFÉLAZONOSÍTÁS, SZERZŐDÉSKÖTÉS FÓKUSZ TERÜLETEI

- Jogi, technikai megfelelőség
- Magatartás-kódex, ügyfélpéldány
- Hosszútávú megőrzés, mentések biztonsága
- Átvilágítás, azonosítás technikai követelményei
- Adatok hitelessége, visszakereshetősége
- Kockázatcsökkentő intézkedések
- Zártsági audit
- Kiszervezés
- Szerződéskötés hitelessége, megfelelősége

ÜGYFÉLAZONOSÍTÁS, SZERZŐDÉSKÖTÉS

A témavizsgálat kiterjedt 5 db intézményre – 3 db bank és 2 db biztosító.

26/2020. (VIII. 25.) MNB rendelet

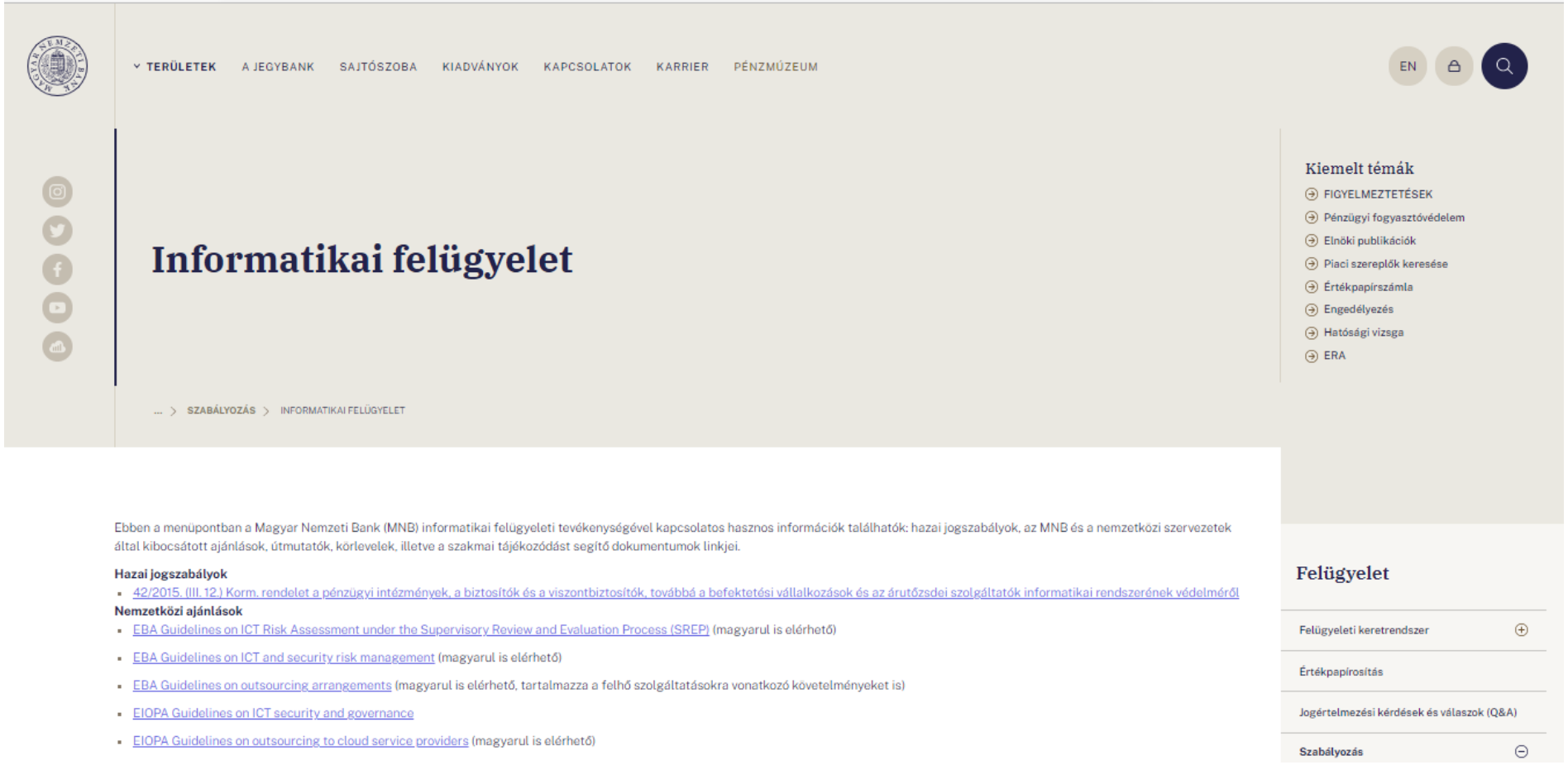
Vezetői körlevél az elektronikus úton megkötött írásbeli szerződésekről, megtett írásbeli jognyilatkozatokról

- a zártsági tanúsítási vizsgálati jelentés hiánya
- az okmányokról és arcképről készített képek minősége nem megfelelő
- az ügyfélazonosításnál a többfaktoros azonosítás nem megfelelő (azonosító kód hiánya)
- az ügyfél-átvilágítás ellátásához szükséges vizsga hiánya
- az ügyféllel felépített elektronikus átviteli csatornán keresztül folyó távadatátvitel nem titkosított
- a szerződés a jogszabályban előírt formai és tartalmi követelményeknek nem felel meg

TÖBBRÉTEGŰ VÉDELEM

- Emberek (biztonsági tudatosság)
- Folyamatok (kontrollok)
- Technológia (rendszerek)

IFF ALOLDAL AZ MNB HONLAPON



TERÜLETEK A JEGYBANK SAJTÓSZOBA KIADVÁNYOK KAPCSOLATOK KARRIER PÉNZMÚZEUM EN

Informatikai felügyelet

... > SZABÁLYOZÁS > INFORMATIKAI FELÜGYELET

Ebben a menüpontban a Magyar Nemzeti Bank (MNB) informatikai felügyeleti tevékenységével kapcsolatos hasznos információk találhatók: hazai jogszabályok, az MNB és a nemzetközi szervezetek által kibocsátott ajánlások, útmutatók, körlevelek, illetve a szakmai tájékozódást segítő dokumentumok linkjei.

Hazai jogszabályok

- 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

Nemzetközi ajánlások

- EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (magyarul is elérhető)
- EBA Guidelines on ICT and security risk management (magyarul is elérhető)
- EBA Guidelines on outsourcing arrangements (magyarul is elérhető, tartalmazza a felhő szolgáltatásokra vonatkozó követelményeket is)
- EIOPA Guidelines on ICT security and governance
- EIOPA Guidelines on outsourcing to cloud service providers (magyarul is elérhető)

Kiemelt témák

- FIGYELMEZTETÉSEK
- Pénzügyi fogyasztóvédelem
- Elnöki publikációk
- Piaci szereplők keresése
- Értékpapírszámla
- Engedélyezés
- Hatósági vizsga
- ERA

Felügyelet

- Felügyeleti keretrendszer
- Értékpapírosítás
- Jogértelmezési kérdések és válaszok (Q&A)
- Szabályozás

https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet

Forrás | MNB

KÖSZÖNÖM A FIGYELMET!