A FIZETÉSI RENDSZERT MŰKÖDTETŐ PÉNZÜGYI VÁLLALKOZÁSRA, A HITELINTÉZETTEL EGYENÉRTÉKŰ PRUDENCIÁLIS SZABÁLYOZÁSNAK MEGFELELŐ PÉNZÜGYI VÁLLALKOZÁSRA, VALAMINT AZ OLYAN PÉNZÜGYI VÁLLALKOZÁSRA, AMELYRE AZ ÖSSZEVONT ALAPÚ FELÜGYELET KITERJED VONATKOZÓ KÖVETELMÉNYEK AZ INFORMATIKAI TÁRGYÚ SZABÁLYZATOK ÉS DOKUMENTUMOK TEKINTETÉBEN

Dokumentum megnevezése	Tartalmi elemek	Tartalmi elemet előíró norma
Digitális működési rezilienciára vonatkozó stratégia **Éves informatikai beruházási és költség tervek**	A digitális működési rezilienciára vonatkozó stratégia összhangban van a szervezet üzleti stratégiájával és célkitűzéseivel. A digitális működési rezilienciára vonatkozó stratégia tartalmazza a • az üzleti stratégia és célkitűzések eléréséhez szükséges eszközök és tevékenységek leírását; • az IKT-kockázati toleranciaszintet és az IKT-zavarok hatásaival kapcsolatos tolerancia elemzését; • az információbiztonsági célokat és a kapcsolódó teljesítménymutatókat és kockázati mérőszámokat; • az IKT-referenciaarchitektúrát és az egyes konkrét üzleti célok eléréséhez szükséges változásokat; • az IKT-vonatkozású események észlelése, hatásaik megelőzése és az azzal szembeni védelem céljából bevezetett eljárásokat; • a digitális működési reziliencia aktuális helyzetének leírását és a helyzetfelmérést megalapozó tényeket; • a digitális működési reziliencia tesztelésére vonatkozó eljárások és az IKT-vonatkozású események esetén alkalmazandó kommunikációs stratégia leírását. A stratégiában foglaltakat éves költségvetési tervekkel kell alátámasztani.	DORA* 6. cikk (8) DORA 6. cikk (2) g)
Szervezeti és működési szabályzat	A szervezet méretével és feladatellátásával arányos informatikai, informatikai biztonsági és informatikai ellenőrzési területek megnevezése, feladat- és hatáskörük feltüntetése.	DORA 4. cikk (1)-(2) DORA 5. cikk (2) c)

Kiszervezési szerződések	A kiszervezett tevékenységet végző szervezetekkel kötött szerződések.	Hpt. 68. §.
Adatgazda, rendszergazda kijelölő dokumentumok	Az adatgazda és rendszergazda kijelölő iratokban az érintett személyeket egyértelműen össze kell rendelni a gondjaikra bízott vagyonelemekkel. A kijelölést az érintett személyek a kijelölő dokumentumban aláírásukkal tudomásul veszik. Az adatgazdák és a rendszergazdák feladatait és felelősségeit a kijelölő dokumentumban vagy szabályzatban egyértelműen meg kell határozni. Az adatgazda feladata és felelőssége nem szervezhető ki.	DORA 5. cikk (2) c) Ajánlás** 2.3.
Informatikai biztonsági szabályzat	A pénzügyi szervezetek megtervezik, beszerzik és bevezetik azon IKT-biztonsági stratégiákat, szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek célja biztosítani az IKT-rendszerek rezilienciáját, folytonosságát és rendelkezésre állását – különös tekintettel azokra, amelyek kritikus vagy fontos funkciókat támogatnak –, továbbá fenntartani az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normákat, legyen szó használaton kívüli, használatban lévő vagy továbbítás alatt álló adatokról. A pénzügyi szervezetek létrehozzák azon IKT-biztonsági szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek: • garantálják a hálózatok biztonságát; • megfelelő biztosítékokat tartalmaznak a behatolások és az adatokkal való visszaélés ellen; • megőrzik az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét többek között kriptográfiai technikákkal; • garantálják a pontos és gyors, jelentős zavaroktól és indokolatlan késedelemtől mentes adattovábbítást.	DORA 9. cikk (2) RMF RTS*** 3. cikk (1)

	Az IKT-biztonsági szabályzatok: • igazodnak a pénzügyi szervezetnek a digitális működési rezilienciára vonatkozó stratégiában foglalt információbiztonsági célkitűzéseihez; • tartalmazzák az IKT-biztonsági szabályzatok vezető testület általi hivatalos elfogadásának időpontját; • mutatókat és intézkedéseket tartalmazzanak a szabályzatok végrehajtásának nyomon követése, a végrehajtás alóli kivételek rögzítése és annak biztosítása, hogy a kivételek esetén biztosított legyen a pénzügyi szervezet digitális működési rezilienciája; • minden szinten meghatározzák a személyzet felelősségi körét; és a meg nem felelés következményeit, • felsorolják a fenntartandó dokumentációt; • az összeférhetetlenség elkerülése érdekében meghatározzák a feladatok elkülönítését; • figyelembe veszik a jó gyakorlatokat és a vonatkozó szabványokat; • meghatározzák a kapcsolódó szerepeket és felelősségi köröket; • rendelkeznek a felülvizsgálatról; • figyelembe veszik szervezetet érintő lényeges változásokat, beleértve szervezet tevékenységeinek vagy folyamatainak, a kiberfenyegetettségi helyzetnek vagy az alkalmazandó jogi kötelezettségeknek a lényeges változásait.	RMF RTS 2. cikk (2)
	A szabályzatban a kockázatokkal arányos módon ki kell térni legalább: a) az IKT-kockázatkezelésre;	RMF RTS 3. cikk

	b) az IKT-eszközök kezelésére; c) a titkosításra és kriptográfiai ellenőrzésekre és a kriptográfiai kulcsok kezelése; d) az IKT-üzemeltetésre vonatkozó eljárásokra e) a kapacitás- és teljesítménymenedzsmentre f) sérülékenység-menedzsmentre és a javítócsomagok kezelésére g) az adat- és rendszerbiztonságra h) a naplózási eljárásokra, protokollokra és eszközökre i) a hálózatbiztonság kezelésére j) az adattovábbítás védelmére k) az IKT-projektmenedzsmentre l) az IKT-rendszerek beszerzésére, fejlesztésére és karbantartására m) az IKT-változásmenedzsmentre n) a fizikai és környezetbiztonságra o) a humánerőforráshoz kapcsolódó követelményekre p) a felhasználókezelésre q) a hozzáférés-ellenőrzésre r) a rendellenes és az IKT-vonatkozású események észlelésére és kezelésére s) Az IKT-üzletmenet-folytonossági politika elemeire	RMF RTS 4. cikk RMF RTS 6-7. cikk RMF RTS 8. cikk RMF RTS 9. cikk RMF RTS 10. cikk RMF RTS 11. cikk RMF RTS 12. cikk RMF RTS 13. cikk RMF RTS 14. cikk RMF RTS 15. cikk RMF RTS 16. cikk RMF RTS 17. cikk RMF RTS 18. cikk RMF RTS 19. cikk RMF RTS 20. cikk RMF RTS 21. cikk RMF RTS 22-23. cikk RMF RTS 24. cikk
Biztonsági osztályba sorolás rendszere	az IKT-kockázatkezelési keretrendszer részeként azonosítani, osztályozni és megfelelően dokumentálni kell valamennyi, az IKT-ra támaszkodó üzleti funkciót, feladat- és felelősségi kört, az említett funkciókat támogató információs vagyonelemeket és IKT-eszközöket, valamint azok IKT-kockázattal kapcsolatos feladatkörét és függőségeit.	DORA 8. cikk

IT biztonsági kockázatelemzés és kockázatkezelés dokumentumai • Kockázatelemzési módszertan • Kockázati térkép • Értékelés, hiányosságok azonosítása • Feltárt kockázatok kezelése • Kockázatfelvállalás	A pénzügyi szervezetek olyan IKT-kockázatkezelési szabályzatokat és eljárásokat dolgoznak ki, dokumentálnak és hajtanak végre, amelyek a következők mindegyikét tartalmazzák az IKT-kockázatértékelés elvégzésének eljárását és módszertanát, szerepeltetve a következőket: i. a támogatott üzleti funkciókat, az IKT-rendszereket és az e funkciókat támogató IKT-eszközöket érintő vagy esetlegesen érintő sérülékenységek és fenyegetések; ii. az i. alpontban említett sérülékenységek és fenyegetések hatásának és valószínűségének mérésére szolgáló mennyiségi és minőségi mutatók.	RMF RTS 3. cikk
	A pénzügyi szervezeteknek folyamatosan azonosítaniuk kell az IKT-kockázat valamennyi forrását, különösen a más pénzügyi szervezetekkel szembeni és azoktól eredő kockázati kitettséget, továbbá értékelniük kell az IKT-ra támaszkodó üzleti funkcióik, információs vagyonelemeik és IKT-eszközeik szempontjából releváns kiberfenyegetéseket és IKT-sérülékenységeket. A pénzügyi szervezeteknek rendszeresen, de legalább évente felül kell vizsgálniuk az őket érintő kockázati forgatókönyveket.	DORA 8. cikk (2) bekezdés
	Az IKT-kockázatkezelési keretrendszernek magában kell foglalnia egy digitális működési rezilienciára vonatkozó stratégiát is, amely meghatározza, hogy hogyan hajtandó végre a keret. E célból a digitális működési rezilienciára vonatkozó stratégiának magában kell foglalnia az IKT-kockázat kezelésére és a konkrét IKT-célkitűzések megvalósítására irányuló módszereket: • ismertetni kell az IKT-referenciaarchitektúrát az egyes konkrét üzleti célkitűzések eléréséhez szükséges változtatásokkal együtt; • fel kell vázolni azon különböző mechanizmusokat, amelyeket az IKT-vonatkozású események észlelése, hatásaik megelőzése és az azzal szembeni védelem céljából vezettek be	DORA 6. cikk (8) bekezdés

	Meg kell határozni az IKT-kockázati toleranciaszintet a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban, továbbá elemezni kell az IKT-zavarok hatásaival kapcsolatos toleranciát. A pénzügyi szervezetek olyan IKT-kockázatkezelési szabályzatokat és eljárásokat dolgoznak ki, dokumentálnak és hajtanak végre, amelyek tartalmazzák az azonosított és értékelt IKT-kockázatokhoz tartozó IKT-kockázatkezelési intézkedések azonosítására, végrehajtására és dokumentálására szolgáló eljárást, beleértve az ahhoz szükséges IKT-kockázatkezelési intézkedések meghatározását, hogy az IKT-kockázat a kockázati toleranciaszinten belül maradjon. Az eljárásnak biztosítania kell a végrehajtott IKT-kockázatkezelési intézkedések hatékonyságának nyomon követését, annak értékelését, hogy a pénzügyi szervezet elérte-e a megállapított kockázati toleranciaszinteket, valamint annak értékelését, hogy a pénzügyi szervezet szükség esetén tett-e lépéseket ezen intézkedések kijavítására vagy jobbá tételére.	DORA 6. cikk (8) bekezdés 1774/2024/EU Rendelet 3. cikk
	Meg kell határozni az IKT-kockázati toleranciaszintet a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban, továbbá elemezni kell az IKT-zavarok hatásaival kapcsolatos toleranciát. A pénzügyi szervezetek olyan IKT-kockázatkezelési szabályzatokat és eljárásokat dolgoznak ki, dokumentálnak és hajtanak végre, amelyek tartalmazzák az azonosított és értékelt IKT-kockázatokhoz tartozó IKT-kockázatkezelési intézkedések azonosítására, végrehajtására és dokumentálására szolgáló eljárást, beleértve az ahhoz szükséges IKT-kockázatkezelési intézkedések meghatározását, hogy az IKT-kockázat a kockázati toleranciaszinten belül maradjon. Az eljárásnak biztosítania kell a végrehajtott IKT-kockázatkezelési intézkedések hatékonyságának nyomon követését, annak értékelését, hogy a pénzügyi szervezet elérte-e a megállapított kockázati toleranciaszinteket, valamint annak értékelését, hogy a pénzügyi szervezet szükség esetén tett-e lépéseket ezen intézkedések kijavítására vagy jobbá tételére.	DORA 6. cikk (8) bekezdés RMF RTS Rendelet 3. cikk

IT vagyonelemek nyilvántartási dokumentumai	- IKT-ra támaszkodó üzleti funkciók, - feladat- és felelősségi körök, - az üzleti funkciókat támogató információs vagyonelemek, - az üzleti funkciókat támogató IKT-eszközök osztálya, - az IKT-kockázattal kapcsolatos feladatkörök és függőségek	DORA 8. cikk (1) bekezdés
	Információ-nyilvántartás a harmadik fél IKT-szolgáltatókról	DORA 28. cikk (3) bekezdés 2956/2024/EU Rendelet
	Az IKT-eszközök nyilvántartása (Hardver, szoftver, hálózati eszköz stb.)	RMF RTS 4. cikkével összhangban a 4. cikk (2) és (3) bekezdésben foglalt adattartalommal;
	Kriptográfiai kulcsok nyilvántartása	7. cikk (4) bekezdés
Szolgáltatásfolytonossági terv (BCP), Katasztrófát követő helyreállítási terv (DRP)	A pénzügyi szervezeteknek átfogó IKT-üzletmenetfolytonossági politikát kell bevezetniük, amelyet a pénzügyi szervezet átfogó üzletmenet-folytonossági politikájának integráns részét képező célzott egyedi szabályzatként is elfogadhatnak.	DORA 11. cikk (1)-(4)
	Üzleti hatáselemzés (BIA)	DORA 11. cikk (5)
	a biztonsági mentési szabályzatok és eljárások, visszaállítási és helyreállítási eljárások és módszerek, valamint az eljárások végrehajtását biztosító műszaki megoldások leírása	DORA 12. cikke RMF RTS 24-25. cikk
Független ellenőrzés	A digitális működési reziliencia tesztelését szolgáló program és a program keretében végrehajtott tesztek dokumentumai, tapasztaltak kiértékelése, intézkedési terv.	DORA 25. cikk
	Az IKT-kockázatkezelési keretrendszerére ellenőrök általi, rendszeres, a pénzügyi szervezetek ellenőrzési tervével összhangban elkészített belső ellenőrzési terv. Az IKT-ellenőrzést végző belső ellenőröknek megfelelő szakértelmét igazoló dokumentumok.	DORA 6. cikk (6)

	Kiszervezett tevékenységek ellenőrzése	Hpt. 68. § (6) és (10) bekezdése
Adatszolgáltatási teszt dokumentumok, rendszerkapcsolati dokumentumok	Az előírt adatszolgáltatások végrehajtásának sikeres tesztelését igazoló dokumentumok az elvárt adattartalommal és a és rendszerkapcsolatok működőképességét alátámasztó nyilatkozatok és igazolások	(EU) 2024/1772 rendelet, továbbá Hpt. 18. § (5) bekezdés d) pontja, 20. § (2) bekezdés h), j) k) pontjai
Harmadik fél szolgáltatókra vonatkozó dokumentumok *	Az harmadik fél IKT-szolgáltatók tevékenységét szabályozó szerződések vagy megállapodások, továbbá az ilyen szolgáltatások igénybe vételét biztosító belső eljárásrendek; a kockázatok kezelését és a szolgáltatásfolytonosságot, valamint az elszámoltathatóságot biztosító technológiai és szervezési megoldások ismertetése, továbbá a harmadik fél IKT-szolgáltatók szerződései.	DORA 8. cikk (5) bekezdés (EU)2024/1773 rendelet

** Európai Parlament és a Tanács 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 szóló 2022. december 14-i 2022/2554 (EU) rendelete*

***az informatikai rendszer védelméről szóló 1/2025. (I.13.) MNB ajánlás*

****az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-kockázatkezelési eszközöket, módszereket, folyamatokat és szabályzatokat, valamint az egyszerűsített IKT-kockázatkezelési keretrendszert meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló (EU) 2024/1774 rendelet*

2025. január