Segédlet a pénzügyi vállalkozások informatikai tárgyú szabályzatainak és dokumentumainak elkészítéséhez

Az MNB a pénzügyi vállalkozások alapítási és tevékenységi engedélykérelmei összeállításának megkönnyítése céljából elkészített egy segédletet, mely az egyes informatikai szabályzatok tartalmi elemeinek felsorolását rögzíti. Felhívjuk a figyelmet arra, hogy ezen segédlet csak a jogszabályok és egyéb szabályozó eszközök által előírt legfontosabb tartalmi elemek felsorolására szorítkozik, a kérelmezőnek azokat egyediesítenie kell saját szervezetének, az általa végezni kívánt tevékenységeknek és üzleti modelljének megfelelően. Amennyiben a kérelmező informatikai szabályzatai a jogszabályoknak vagy egyéb szabályozó eszközöknek nem felelnek meg vagy a szabályzatok egymással nincsenek összhangban, az MNB hiánypótlási felhívást rendelhet el.

Dokumentum megnevezése	Tartalmi elemek	Tartalmi elemet előíró norma
Üzleti stratégia	Az egyszerűsített IKT-kockázatkezelési keretrendszer a kockázatvállalási hajlandósággal összhangban biztosítja a pénzügyi szervezet üzleti stratégiájának megvalósítását.	RMF RTS* 28. cikk (2) a) pont;
Információbiztonsági stratégia	Meghatározza az információbiztonsági célkitűzéseket és az IKT-követelményeket.	RMF RTS 28. cikk (2) c)
Éves informatikai beruházási és költség tervek	Megállapítja és legalább évente egyszer felülvizsgálja a pénzügyi szervezet digitális működési rezilienciával kapcsolatos szükségleteinek kielégítését biztosító költségvetést minden erőforrástípus tekintetében, ideértve a személyzet valamennyi tagja számára biztosítandó, releváns, IKT-biztonsági tájékozottságot elősegítő programokat és digitális működési rezilienciával kapcsolatos képzéseket, valamint IKT-készségeke	RMF RTS 28. cikk (2) e)
Szervezeti és működési szabályzat	Egyértelmű szerep- és felelősségi körök kijelölése minden IKT-vonatkozású feladattal összefüggésben	RMF RTS 28. cikk (2) b)
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.	RMF RTS 28. cikk (2) b) Ajánlás** 2.3.

Információbiztonsági szabályzat	A pénzügyi szervezet meghatározza és végrehajtja az egyszerűsített IKT-kockázatkezelési keretrendszer részeként a szükséges szabályzatokat és intézkedéseket a pénzügyi szervezetet érintő IKT-kockázat azonosítása, értékelése és kezelése érdekében, azonosítja és végrehajtja az információs vagyonelemek és IKT-eszközök védelméhez szükséges eljárásokat, IKT-protokollokat és eszközöket.	RMF RTS 28. cikk RMF RTS 29. és 30-38. cikkek
	Az IKT-biztonsági szabályzatok: A pénzügyi szervezet az egyszerűsített IKT-kockázatkezelési keretrendszerrel összefüggésben kidolgozza dokumentálja és végrehajtja az információbiztonsági szabályzatot. Ez az információbiztonsági szabályzat meghatározza az adatok és az ezen pénzügyi szervezetek által nyújtott szolgáltatások bizalmas jellegének, integritásának, rendelkezésre állásának és hitelességének védelmét szolgáló magas szintű elveket és szabályokat. A pénzügyi szervezet az információbiztonsági szabályzat alapján IKT-biztonsági intézkedéseket hoz és hajt végre az IKT-kockázatnak való kitettség csökkentése érdekében, beleértve a harmadik fél IKT-szolgáltatók által végrehajtott kockázatcsökkentő intézkedéseket is.	RMF RTS 29. és 30-38. cikkek

	A szabályzatban a kockázatokkal arányos módon ki kell térni legalább:	
	i.) az információs vagyonelemek és IKT-eszközök osztályozása	RMF RTS 30. cikk
	ii.) IKT-kockázatkezelés	RMF RTS 31. cikk
	iii.) fizikai és környezetbiztonság	RMF RTS 32. cikk
	iv.) hozzáférés-ellenőrzés	RMF RTS 33. cikk
	v.) IKT-műveletek biztonsága: a. IKT-eszközök nyilvántartása b. beleértve a harmadik fél IKT-szolgáltatók által nyújtott szolgáltatásokat; c. IKT-eszközök kapacitásmenedzsmentje d. sérülékenység menedzsment; e. patch menedzsment; f. IKT-események naplózása; g. IKT-műveletekkel kapcsolatos rendellenes tevékenység monitoring és kezelés; h. kiberfenyegetések nyomon követése; i. adatszivárgás megelőzése, vírus- és kártékonykód elleni védelem	RMF RTS 34. cikk
	vi.) adat-, rendszer- és hálózatbiztonság: a. adatbiztonsági intézkedések; b. adattárolás és adatfeldolgozás biztonsága; c. külső és belső adatkapcsolatok védelme; d. adattovábbítás biztonsága; e. adatok biztonságos törlése; f. adattárolók megsemmisítése; g. távmunka és privát eszközök használatának biztonsága	RMF RTS 35. cikk
	vii.) IKT-biztonsági tesztelés;	RMF RTS 36. cikk
	viii.) IKT-rendszerek beszerzése, fejlesztése és karbantartása;	RMF RTS 37. cikk
	ix.) IKT-projektmenedzsment és -változásmenedzsment;	RMF RTS 38. cikk

Biztonsági osztályba sorolás rendszere és adatvagyon leltár	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. Az egyszerűsített IKT-kockázatkezelési keretrendszer részeként azonosítani, osztályozni és megfelelően dokumentálni kell valamennyi kritikus vagy fontos funkciót, az azokat támogató információs vagyonelemeket és IKT-eszközöket, valamint azok kölcsönös függőségeit; ennek részeként a harmadik fél IKT-szolgáltatók által támogatott valamennyi kritikus vagy fontos funkciót is.	RMF RTS 30. cikk (1)-(2)
IT biztonsági kockázatelemzés és kockázatkezelés dokumentumai • Kockázatkezelési módszertan • Kockázati térkép • Értékelés, hiányosságok azonosítása • Feltárt kockázatok kezelése • Kockázatfelvállalás	A pénzügyi szervezet az egyszerűsített IKT-kockázatkezelési keretrendszerbe belefoglalja a következők mindegyikét: • az IKT-kockázatra vonatkozó kockázati toleranciaszintek meghatározása a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban; • az IKT-kockázatok azonosítása és értékelése • kockázatcsökkentési stratégiák meghatározása legalább azokra az IKT-kockázatokra vonatkozóan, amelyek nem a szervezet kockázati toleranciaszintjén belül vannak; • a kockázatcsökkentési stratégiák hatékonyságának nyomon követése; az IKT-rendszerben vagy IKT-szolgáltatásokban, -folyamatokban vagy -eljárásokban bekövetkező jelentős változásokból, valamint az IKT-biztonsági tesztelések eredményeiből és bármely jelentős IKT-vonatkozású eseményből eredő bármely IKT- és információbiztonsági kockázat azonosítása és értékelése. A szervezet az IKT-kockázati profiljukkal arányosan időközönként elvégzi és dokumentálja az IKT-kockázatértékelést. A kockázatkezelési módszertan részeként: • a szervezet folyamatosan nyomon követi a kritikus vagy fontos funkcióik, valamint információs vagyonelemeik és IKT-eszközeik szempontjából releváns fenyegetéseket és sérülékenységeket, és rendszeresen felülvizsgálja a kritikus vagy fontos funkciókat érintő kockázati forgatókönyveket. • az IKT-vonatkozású események válaszfolyamatait kiváltó és elindító riasztási értékhatárokat és kritériumokat határoz meg.	RMF RTS 31. cikk

IT vagyonelemek nyilvántartási dokumentumai	Az IKT-rendszerek vagyonelemeinek nyilvántartási szabályai és az elemek aktuális nyilvántartásai A szervezetek azonosítják, osztályozzák és dokumentálják az IKT-eszközöket (Hardver, szoftver, hálózati eszköz stb.)	RMF RTS 30.
	Információ-nyilvántartás a harmadik fél IKT-szolgáltatókról	2956/2024/EU Rendelet
Szolgáltatásfolytonossági terv (BCP), Katasztrófát követő helyreállítási terv (DRP) **Kibertámadási forgatókönyv** **Mentési terv**	A pénzügyi szervezet kidolgozza az IKT-üzletmenet-folytonossági terveket, figyelembe véve az üzletmenetben okozott súlyos zavaroknak való kitettségre és azok lehetséges hatására vonatkozó elemzés eredményeit, valamint azokat a forgatókönyveket, amelyeknek a kritikus vagy fontos funkciókat támogató IKT-eszközeik ki lehetnek téve, ideértve a kibertámadási forgatókönyvet is. A tervezett helyreállítási szintek és időkeretek meghatározása a funkciók és a kulcsfontosságú belső és külső függőségek helyreállításához és újraindításához, beleértve a harmadik fél IKT-szolgáltatókat is; Azon feltételek meghatározása, amelyek kiválthatják az IKT-üzletmenet-folytonossági tervek aktiválását. Az intézkedések meghatározása, amelyeket meg kell hozni a szervezet kritikus vagy fontos funkciókat támogató IKT-eszközeinek rendelkezésre állásának, folytonosságának és helyreállításának biztosítása érdekében; a szervezetek azonosítják a szükséges visszaállítási és helyreállítási intézkedéseket.	RMF RTS 30. cikk (1)-(2) RMF RTS 39. cikk (2)
	Üzleti hatáselemzés (BIA)	RMF RTS 30. cikk (1)-(2) és 39. cikk (2)

	A szervezet azonosítja a biztonsági mentési eljárásokat és intézkedéseket, amelyek meghatározzák a biztonsági mentés tárgyát képező adatok körét és a biztonsági mentés minimális gyakoriságát az ezeket az adatokat felhasználó funkció kritikussága alapján	RMF RTS 39. cikk (2) g)
Független ellenőrzési tervek	A pénzügyi szervezetek kiszervezhetik az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzésével kapcsolatos feladatokat csoporton belüli IKT-szolgáltatóknak vagy harmadik fél IKT-szolgáltatóknak, azonban a pénzügyi szervezetek teljes felelősséggel tartoznak az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzéséért. A pénzügyi szervezetek biztosítják a kontrollfunkciók és a belső ellenőrzési funkciók megfelelő elkülönítését és függetlenségét. Az egyszerűsített IKT-kockázatkezelési keretrendszerrel összhangban megvalósított és az IKT-kockázatokhoz igazodó ellenőrzési tervek. Az ellenőröknek elegendő ismerettel, készségekkel és szakértelemmel kell rendelkezniük az IKT-kockázat terén, és függetlennek kell lenniük.	RMF RTS 28. cikk (3)-(5)
Kiszervezés ellenőrzési tervek	Kiszervezett tevékenységek ellenőrzése Hpt. szerint.	Hpt. 68. § (6) és (10) bekezdése
Adatszolgáltatási teszt dokumentumok, rendszerkapcsolati dokumentumok	Az előírt adatszolgáltatások végrehajtásának sikeres tesztelését igazoló dokumentumok az elvárt adattartalommal.	(EU) 2024/1772 rendelet

Harmadik fél szolgáltatókra vonatkozó dokumentumok *	Az harmadik fél IKT-szolgáltatók tevékenységét szabályozó szerződések vagy megállapodások, továbbá az ilyen szolgáltatások igénybevételét 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.	(EU)2024/1773 rendelet

**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*

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

2025. január