2024/1774

2024.6.25.

A BIZOTTSÁG (EU) 2024/1774 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2024. március 13.)

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

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, a 909/2014/EU rendelet, valamint az (EU) 2016/1011 rendelet módosításáról szóló, 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendeletre ([1]), és különösen annak 15. cikke negyedik albekezdésére és 16. cikke (3) bekezdésének negyedik albekezdésére,

mivel:

(1) Az (EU) 2022/2554 rendelet a pénzügyi szervezetek széles körére vonatkozik, amelyek méretüket, felépítésüket, belső szervezetüket, valamint tevékenységeik jellegét és összetettségét tekintve eltérőek, és ezáltal megnövekedett vagy csökkent összetettségi vagy kockázati elemekkel rendelkeznek. E változatosság megfelelő figyelembevételének biztosítása érdekében az IKT-biztonsági szabályzatokra, eljárásokra, protokollokra és eszközökre, valamint az egyszerűsített IKT-kockázatkezelési keretrendszerre vonatkozó követelményeknek arányosnak kell lenniük az említett pénzügyi szervezetek méretével, felépítésével, belső szervezetével, jellegével és összetettségével, valamint a kapcsolódó kockázatokkal.

(2) Ugyanezen okból az (EU) 2022/2554 rendelet hatálya alá tartozó pénzügyi szervezetek számára bizonyos rugalmasságot kell biztosítani az IKT-biztonsági szabályzatokra, eljárásokra, protokollokra és eszközökre, valamint az egyszerűsített IKT-kockázatkezelési keretrendszerre vonatkozó követelményeknek való megfelelés módjának tekintetében. Ezért a pénzügyi szervezetek számára engedni kell, hogy az említett követelményekből eredő dokumentációs követelményeknek való megfelelés érdekében felhasználják a már rendelkezésükre álló dokumentumokat. Ebből következik, hogy a konkrét IKT-biztonsági szabályzatok kidolgozását, dokumentálását és végrehajtását csak bizonyos alapvető elemek tekintetében kell előírni, figyelembe véve többek között a vezető ágazati gyakorlatokat és szabványokat. Emellett a konkrét technikai végrehajtási szempontok figyelembevétele érdekében IKT-biztonsági eljárásokat kell kidolgozni, dokumentálni és végrehajtani, beleértve a kapacitás- és teljesítménymenedzsmentet, a sérülékenységek és javítócsomagok kezelését, az adat- és rendszerbiztonságot, valamint a naplózást.

(3) Az e rendelet II. címének I. fejezetében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök idővel helyes végrehajtásának biztosítása érdekében fontos, hogy a pénzügyi szervezetek helyesen osszák ki és tartsák fenn az IKT-biztonsággal kapcsolatos szerep- és felelősségi köröket, és meghatározzák az IKT-biztonsági szabályzatoknak vagy eljárásoknak való meg nem felelés következményeit.

(4) Az összeférhetetlenség kockázatának csökkentése érdekében a pénzügyi szervezeteknek az IKT-szerepek és felelősségi körök kijelölésekor biztosítaniuk kell a feladatok elkülönítését.

(5) A rugalmasság biztosítása és a pénzügyi szervezetek ellenőrzési keretének egyszerűsítése érdekében a pénzügyi szervezetek nem kötelezhetők arra, hogy konkrét rendelkezéseket dolgozzanak ki az e rendelet II. címének I. fejezetében említett IKT-biztonsági szabályzatoknak, eljárásoknak és protokolloknak való meg nem felelés következményeire vonatkozóan, amennyiben másik szabályzat vagy eljárás már meghatároz ilyen rendelkezéseket.

([1]) HL L 333., 2022.12.27., 1. o., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) Olyan dinamikus környezetben, ahol az IKT-kockázatok folyamatosan változnak, fontos, hogy a pénzügyi szervezetek az IKT-biztonsági szabályzataikat vezető gyakorlatok és adott esetben az 1025/2012/EU európai parlamenti és tanácsi rendelet ([2]) 2. cikkének 1. pontjában foglalt meghatározás szerinti szabványok alapján dolgozzák ki. Ennek lehetővé kell tennie az e rendelet II. címében említett pénzügyi szervezetek számára, hogy folyamatosan tájékozottak és felkészültek maradjanak a változó környezetben.

(7) Digitális működési rezilienciájuk biztosítása érdekében az e rendelet II. címében említett pénzügyi szervezeteknek IKT-biztonsági szabályzataik, eljárásaik, protokolljaik és eszközeik részeként az IKT-eszközök kezelésére vonatkozó szabályzatot, a kapacitás- és teljesítménymenedzsmentre vonatkozó eljárásokat, valamint az IKT-műveletekre vonatkozó szabályzatokat és eljárásokat kell kidolgozniuk és végrehajtaniuk. Ezekre a szabályzatokra és eljárásokra azért van szükség, hogy biztosítsák az IKT-eszközök állapotának nyomon követését azok teljes életciklusa során ezen eszközök hatékony használata és karbantartása érdekében (IKT-eszközkezelés). Ezeknek a szabályzatoknak és eljárásoknak biztosítaniuk kell továbbá az IKT-rendszerek működésének optimalizálását, valamint azt, hogy az IKT-rendszerek és -kapacitások teljesítménye megfeleljen a meghatározott üzleti és információbiztonsági célkitűzéseknek (kapacitás- és teljesítménymenedzsment). Végezetül ezeknek a szabályzatoknak és eljárásoknak biztosítaniuk kell az IKT-rendszerek hatékony és zökkenőmentes napi irányítását és működését (IKT-műveletek), ezáltal minimálisra csökkentve az adatok bizalmas jellege, integritása és rendelkezésre állása sérülésének kockázatát. Ezekre a szabályzatokra és eljárásokra ezért szükség van a hálózatok biztonságának garantálásához, a behatolások és az adatokkal való visszaélés elleni megfelelő biztosítékok garantálásához, valamint az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzéséhez.

(8) Az elavult IKT-rendszerekkel kapcsolatos kockázat megfelelő kezelésének biztosítása érdekében a pénzügyi szervezeteknek rögzíteniük kell és nyomon kell követniük a harmadik fél IKT-szolgáltatók támogatási szolgáltatásainak záró időpontját. Az adatok bizalmas jellegének, integritásának és rendelkezésre állásának sérülése által kiváltott lehetséges hatások miatt a pénzügyi szervezeteknek az említett végső határidők rögzítése és nyomon követése során azokra az IKT-eszközökre vagy -rendszerekre kell összpontosítaniuk, amelyek az üzleti tevékenység szempontjából kritikus fontosságúak.

(9) A kriptográfiai ellenőrzések biztosíthatják az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét. Az e rendelet II. címében említett pénzügyi szervezeteknek ezért kockázatalapú megközelítés alapján azonosítaniuk kell és végre kell hajtaniuk ezeket az ellenőrzéseket. E célból a pénzügyi szervezeteknek egy kétágú folyamat – nevezetesen az adatok osztályozása és átfogó IKT-kockázatértékelés – eredményei alapján titkosítaniuk kell az érintett használaton kívüli, továbbítás alatt álló és adott esetben használatban lévő adatokat. Tekintettel a használatban lévő adatok titkosításának összetettségére, az e rendelet II. címében említett pénzügyi szervezeteknek csak akkor kell titkosítaniuk a használatban lévő adatokat, ha ez az IKT-kockázatértékelés eredményei alapján helyénvaló. Az e rendelet II. címében említett pénzügyi szervezeteknek azonban képesnek kell lenniük arra, hogy amennyiben a használatban lévő adatok titkosítása nem kivitelezhető vagy túl bonyolult, más IKT-biztonsági intézkedések révén védjék az érintett adatok bizalmas jellegét, integritását és rendelkezésre állását. Tekintettel a kriptográfiai technikák terén tapasztalható gyors technológiai fejlődésre, az e rendelet II. címében említett pénzügyi szervezeteknek lépést kell tartaniuk a kriptoanalízis releváns fejleményeivel, és figyelembe kell venniük a vezető gyakorlatokat és szabványokat. Az e rendelet II. címében említett pénzügyi szervezeteknek ezért kockázatcsökkentésen és nyomon követésen alapuló rugalmas megközelítést kell alkalmazniuk a kriptográfiai fenyegetések dinamikus környezetének kezelése érdekében, beleértve a kvantumfejlesztésekből eredő fenyegetéseket is.

(10) Az IKT-műveletek biztonsági és működési szabályzatai, eljárásai, protokolljai és eszközei elengedhetetlenek az adatok bizalmas jellegének, integritásának és rendelkezésre állásának biztosításához. Az egyik kulcsfontosságú szempont az éles IKT-környezetek szigorú elkülönítése az IKT-rendszerek fejlesztésének és tesztelésének helyszínéül szolgáló környezetektől és egyéb nem éles környezetektől. Ennek az elkülönítésnek fontos IKT-biztonsági intézkedésként kell szolgálnia az éles környezetben található adatokhoz való nem szándékos és illetéktelen hozzáféréssel, azok ilyen módosításával és törlésével szemben, amelyek jelentős zavarokat okozhatnak az e rendelet II. címében említett pénzügyi szervezetek üzleti tevékenységében. Figyelembe véve azonban a jelenlegi IKT-rendszerfejlesztési gyakorlatokat, kivételes körülmények között a pénzügyi szervezetek számára lehetővé kell tenni, hogy éles környezetben teszteljenek, feltéve, hogy indokolják az ilyen tesztelést, és beszerzik a szükséges jóváhagyást.

([2]) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről (HL L 316., 2012.11.14., 12. o., ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Az IKT-környezetek, az IKT-sérülékenységek és a kiberfenyegetések gyorsan változó jellege proaktív és átfogó megközelítést tesz szükségessé az IKT-sérülékenységek azonosítása, értékelése és kezelése terén. Ilyen megközelítés hiányában a pénzügyi szervezetek, ügyfeleik, felhasználóik és partnereik jelentős mértékben ki lehetnek téve kockázatoknak, ami veszélyeztetné digitális működési rezilienciájukat, hálózataik biztonságát, valamint azon adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét, amelyeket az IKT-biztonsági szabályzatoknak és eljárásoknak védeniük kell. Az e rendelet II. címében említett pénzügyi szervezeteknek ezért azonosítaniuk és orvosolniuk kell IKT-környezetük sérülékenységeit, és mind a pénzügyi szervezeteknek, mind harmadik fél IKT-szolgáltatóiknak koherens, átlátható és felelős sérülékenység-menedzsmentre vonatkozó kerethez kell igazodniuk. Ugyanezen okból a pénzügyi szervezeteknek megbízható erőforrások és automatizált eszközök felhasználásával nyomon kell követniük az IKT-sérülékenységeket, meggyőződve arról, hogy a harmadik fél IKT-szolgáltatók azonnali fellépést biztosítanak a nyújtott IKT-szolgáltatások sérülékenységeivel kapcsolatban.

(12) A javítócsomagok kezelésének kulcsfontosságú részét kell képeznie ezeknek az IKT-biztonsági szabályzatoknak és eljárásoknak, amelyeknek tesztelés és ellenőrzött környezetben történő telepítés révén orvosolniuk kell az azonosított sérülékenységeket, és meg kell előzniük a javítócsomagok telepítéséből eredő zavarokat.

(13) A pénzügyi szervezetet és annak érdekelt feleit esetlegesen érintő potenciális biztonsági fenyegetések időben történő és átlátható kommunikációjának biztosítása érdekében a pénzügyi szervezeteknek eljárásokat kell létrehozniuk az IKT-sérülékenységek ügyfelek, partnerek és a nyilvánosság felé történő felelős közzétételére. Ezen eljárások meghatározásakor a pénzügyi szervezeteknek különböző tényezőket kell figyelembe venniük, többek között a sérülékenység súlyosságát, a sérülékenységnek az érdekelt felekre gyakorolt lehetséges hatását, valamint a javítás vagy a kockázatcsökkentő intézkedések meglétét.

(14) A felhasználói hozzáférési jogosultságok kiosztásának lehetővé tétele érdekében az e rendelet II. címében említett pénzügyi szervezeteknek határozott intézkedéseket kell hozniuk a pénzügyi szervezet információihoz hozzáférő személyek és rendszerek egyedi azonosításának biztosítására. Ennek elmulasztása a pénzügyi szervezeteket potenciálisan illetéktelen hozzáférésnek, adatvédelmi incidenseknek és csalárd tevékenységeknek tenné ki, ezáltal veszélyeztetve az érzékeny pénzügyi adatok bizalmas jellegét, integritását és rendelkezésre állását. Bár az általános vagy közös fiókok használatát kivételesen engedélyezni kell a pénzügyi szervezetek által meghatározott körülmények között, a pénzügyi szervezeteknek biztosítaniuk kell az e fiókokon keresztül tett intézkedésekkel kapcsolatos elszámoltathatóság fenntartását. E biztosíték nélkül a potenciálisan rosszindulatú felhasználók akadályozhatnák a vizsgálati és korrekciós intézkedéseket, ami kiszolgáltatottá tenné a pénzügyi szervezeteket a nem észlelt rosszindulatú tevékenységekkel vagy a meg nem feleléssel kapcsolatos szankciókkal szemben.

(15) Az IKT-környezetek gyors fejlődésének kezelése érdekében az e rendelet II. címében említett pénzügyi szervezeteknek megbízható IKT-projektmenedzsmentre vonatkozó szabályzatokat és eljárásokat kell végrehajtaniuk az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének fenntartása érdekében. Az IKT-projektmenedzsmentre vonatkozó ezen szabályzatoknak és eljárásoknak azonosítaniuk kell az IKT-projektek sikeres irányításához szükséges elemeket, beleértve a pénzügyi szervezet IKT-rendszereinek módosítását, beszerzését, karbantartását és fejlesztését, függetlenül a pénzügyi szervezet által választott IKT-projektmenedzsment módszertanától. E szabályzatok és eljárások összefüggésében a pénzügyi szervezeteknek olyan tesztelési gyakorlatokat és módszereket kell alkalmazniuk, amelyek megfelelnek az igényeiknek, miközben betartják a kockázatalapú megközelítést, és gondoskodnak a biztonságos, megbízható és reziliens IKT-környezet fenntartásáról. Az IKT-projektek biztonságos végrehajtásának garantálása érdekében a pénzügyi szervezeteknek biztosítaniuk kell, hogy a személyzet adott IKT-projekt által befolyásolt vagy érintett konkrét üzleti ágazatokban vagy szerepkörökben dolgozó tagjai képesek biztosítani a szükséges információkat és szakértelmet. A hatékony felvigyázás biztosítása érdekében az IKT-projektekről, különösen a kritikus vagy fontos funkciókat érintő projektekről és az azokhoz kapcsolódó kockázatokról szóló jelentéseket be kell nyújtani a vezető testületnek. A pénzügyi szervezeteknek a rendszeres és folyamatban lévő felülvizsgálatok és jelentések gyakoriságát és részleteit az érintett IKT-projektek jelentőségéhez és méretéhez kell igazítaniuk.

(16) Biztosítani kell, hogy az e rendelet II. címében említett pénzügyi szervezetek által beszerzett és fejlesztett szoftvercsomagokat hatékonyan és biztonságosan integrálják a meglévő IKT-környezetbe, a meghatározott üzleti és információbiztonsági célkitűzésekkel összhangban. A pénzügyi szervezeteknek ezért alaposan értékelniük kell ezeket a szoftvercsomagokat. E célból, valamint a szoftvercsomagokon és a tágabb IKT-rendszereken belüli sérülékenységek és potenciális biztonsági hiányosságok azonosítása érdekében a pénzügyi szervezeteknek IKT-biztonsági tesztelést kell végezniük. A szoftver integritásának értékelése és annak biztosítása érdekében, hogy a szoftver használata ne jelentsen IKT-biztonsági kockázatot, a pénzügyi szervezeteknek a beszerzett szoftverek forráskódjait is felül kell vizsgálniuk, beleértve – amennyiben megvalósítható – a harmadik fél IKT-szolgáltatók által biztosított, zárt forráskódú szoftvereket is, statikus és dinamikus tesztelési módszerek alkalmazásával.

(17) A változások a nagyságrendjüktől függetlenül eredendő kockázatokat hordoznak magukban, és jelentős kockázatot jelentenek az adatok bizalmas jellegének, integritásának és rendelkezésre állásának sérülését illetően, ezért az üzletmenetben okozott súlyos zavarokhoz vezethetnek. A pénzügyi szervezeteknek az olyan potenciális IKT-sérülékenységekkel és -gyengeségekkel szembeni védelme érdekében, amelyek jelentős kockázatoknak tehetik ki őket, szigorú ellenőrzési eljárásra van szükség annak megerősítésére, hogy minden változtatás megfelel a szükséges IKT-biztonsági követelményeknek. Az e rendelet II. címében említett pénzügyi szervezeteknek ezért IKT-biztonsági szabályzataik és eljárásaik alapvető elemeként megbízható IKT-változásmenedzsmentre vonatkozó szabályzatokkal és eljárásokkal kell rendelkezniük. Az IKT-változásmenedzsment folyamata objektivitásának és hatékonyságának fenntartása, az összeférhetetlenség megelőzése, valamint az IKT-vonatkozású változások objektív értékelésének biztosítása érdekében el kell különíteni az e változtatások jóváhagyásáért felelős funkciókat az azokat kérő és végrehajtó funkcióktól. A hatékony átállás, az IKT-vonatkozású változtatás ellenőrzött végrehajtása és az IKT-rendszerek működésének minimális zavarai érdekében a pénzügyi szervezeteknek egyértelmű szerep- és felelősségi köröket kell kijelölniük, amelyek biztosítják az IKT-vonatkozású változtatások megtervezését, megfelelő tesztelését és a minőség biztosítását. Az IKT-rendszerek további hatékony működésének biztosítása és a pénzügyi szervezetek számára biztonsági háló nyújtása érdekében a pénzügyi szervezeteknek tartalékeljárásokat is ki kell dolgozniuk és végre kell hajtaniuk. A pénzügyi szervezeteknek egyértelműen meg kell határozniuk ezeket a tartalékeljárásokat, és ki kell jelölniük a felelősségi köröket annak érdekében, hogy az IKT-vonatkozású változtatások sikertelensége esetén biztosítani lehessen a gyors és hatékony reagálást.

(18) Az IKT-vonatkozású események észlelése, kezelése és bejelentése érdekében az e rendelet II. címében említett pénzügyi szervezeteknek IKT-vonatkozású eseményekre vonatkozó szabályzatot kell kidolgozniuk, amely magában foglalja az IKT-vonatkozású események kezelési folyamatának elemeit. E célból a pénzügyi szervezeteknek azonosítaniuk kell a szervezeten belüli és kívüli valamennyi olyan releváns kapcsolattartót, aki elősegítheti az adott folyamaton belüli különböző fázisok megfelelő koordinációját és végrehajtását. Az IKT-vonatkozású események észlelésének és az azokra való reagálásnak az optimalizálása, valamint ezen események között a tendenciák azonosítása érdekében (ezek értékes információforrást jelentenek a pénzügyi szervezetek számára a kiváltó okok és problémák hatékony azonosítását és kezelését illetően) a pénzügyi szervezeteknek különösen azokat az IKT-vonatkozású eseményeket kell részletesen elemezniük, amelyeket többek között rendszeres megismétlődésük miatt a legjelentősebbnek tartanak.

(19) A rendellenes tevékenységek korai és hatékony észlelésének biztosítása érdekében az e rendelet II. címében említett pénzügyi szervezeteknek össze kell gyűjteniük, nyomon kell követniük és elemezniük kell a különböző információforrásokat, és ki kell jelölniük a kapcsolódó szerep- és felelősségi köröket. Ami a belső információforrásokat illeti, a naplók rendkívül fontos forrást jelentenek, de a pénzügyi szervezetek nem támaszkodhatnak kizárólag a naplókra. Ehelyett a pénzügyi szervezeteknek szélesebb körű információkat kell mérlegelniük, többek között a más belső funkciók által jelentett információkat, mivel ezek a funkciók gyakran értékes információforrások. Ugyanezen okból a pénzügyi szervezeteknek elemezniük kell és nyomon kell követniük a külső forrásokból gyűjtött információkat, beleértve a harmadik fél IKT-szolgáltatók által a rendszereiket és hálózataikat érintő eseményekről szolgáltatott információkat, valamint a pénzügyi szervezetek által relevánsnak ítélt egyéb információforrásokat is. Amennyiben az ilyen információ személyes adatnak minősül, az uniós adatvédelmi jog alkalmazandó. A személyes adatoknak az esemény észleléséhez szükséges mértékre kell korlátozódniuk.

(20) Az IKT-vonatkozású események észlelésének megkönnyítése érdekében a pénzügyi szervezeteknek meg kell őrizniük az ilyen eseményekre vonatkozó bizonyítékokat. Egyrészt az ilyen bizonyítékok kellő ideig történő megőrzésének biztosítása, másrészt a szabályozásból eredő túlzott terhek elkerülése érdekében a pénzügyi szervezeteknek az adatmegőrzési időszakot többek között az adatok kritikusságát és az uniós jogból eredő megőrzési követelményeket figyelembe véve kell meghatározniuk.

(21) Az IKT-vonatkozású események időben történő észlelésének biztosítása érdekében az e rendelet II. címében említett pénzügyi szervezeteknek az IKT-vonatkozású események észlelését és az azokra való reagálást kiváltóként meghatározott kritériumokat nem kimerítőnek kell tekinteniük. Továbbá, bár a pénzügyi szervezeteknek minden egyes kritériumot figyelembe kell venniük, a kritériumokban leírt körülményeknek nem kell egyidejűleg bekövetkezniük, és az érintett IKT-szolgáltatások jelentőségét megfelelően figyelembe kell venni az IKT-vonatkozású események észlelési és válaszfolyamatainak beindításakor.

(22) Az IKT-üzletmenet-folytonossági politika kidolgozása során az e rendelet II. címében említett pénzügyi szervezeteknek figyelembe kell venniük az IKT-kockázatkezelés alapvető elemeit, beleértve az IKT-vonatkozású események kezelésére vonatkozó és a kommunikációs stratégiákat, az IKT-változásmenedzsment folyamatát, valamint a harmadik fél IKT-szolgáltatókkal kapcsolatos kockázatokat.

(23) Meg kell határozni azokat a forgatókönyveket, amelyeket az e rendelet II. címében említett pénzügyi szervezeteknek figyelembe kell venniük mind az IKT-reagálási és -helyreállítási tervek végrehajtása, mind pedig az IKT-üzletmenet-folytonossági tervek tesztelése során. Ezeknek a forgatókönyveknek kiindulópontként kell szolgálniuk a pénzügyi szervezetek számára ahhoz, hogy elemezzék mind az egyes forgatókönyvek relevanciáját és valószínűségét, mind pedig az alternatív forgatókönyvek kidolgozásának szükségességét. A pénzügyi szervezeteknek azokra a forgatókönyvekre kell összpontosítaniuk, amelyekben a rezilienciával kapcsolatos intézkedésekre irányuló beruházások hatékonyabbak és eredményesebbek lehetnek. Az elsődleges IKT-infrastruktúra és a tartalékkapacitás, biztonsági mentések és tartalékeszközök közötti átállás tesztelésével a pénzügyi szervezeteknek értékelniük kell, hogy ez a kapacitás, a biztonsági mentés és ezek az eszközök megfelelő ideig képesek-e hatékonyan működni, és biztosítaniuk kell az elsődleges IKT-infrastruktúra rendes működésének helyreállítását a helyreállítási célkitűzésekkel összhangban.

(24) A 648/2012/EU ([3]), a 600/2014/EU ([4]) és a 909/2014/EU ([5]) európai parlamenti és tanácsi rendeletek értelmében a központi szerződő felekre, a központi értéktárakra és a kereskedési helyszínekre már alkalmazandó követelmények alapján meg kell határozni a működési kockázatra vonatkozó követelményeket, különösen az IKT-projektmenedzsment és -változásmenedzsment, valamint az IKT-üzletmenetfolytonosság-menedzsment követelményeit.

(25) Az (EU) 2022/2554 rendelet 6. cikkének (5) bekezdése előírja a pénzügyi szervezetek számára IKT-kockázatkezelési keretrendszerük felülvizsgálatát és e felülvizsgálatról jelentés benyújtását az illetékes hatóságuknak. Annak érdekében, hogy az illetékes hatóságok könnyen feldolgozhassák az említett jelentésekben szereplő információkat, és garantálni lehessen ezen információk megfelelő továbbítását, a pénzügyi szervezeteknek ezeket a jelentéseket kereshető elektronikus formátumban kell benyújtaniuk.

(26) Az (EU) 2022/2554 rendelet 16. cikkében említett egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezetekre vonatkozó követelményeknek azokra az alapvető területekre és elemekre kell összpontosítaniuk, amelyek az említett pénzügyi szervezetek nagyságrendjére, kockázatára, méretére és összetettségére tekintettel minimumkövetelményként szükségesek az említett pénzügyi szervezetek adatai és szolgáltatásai bizalmas jellegének, integritásának, rendelkezésre állásának és hitelességének biztosításához. Ebben az összefüggésben e pénzügyi szervezeteknek egyértelmű felelősségi körökkel bíró belső irányítási és ellenőrzési keretrendszerrel kell rendelkezniük a hatékony és eredményes kockázatkezelési keretrendszer lehetővé tétele érdekében. Ezenkívül az adminisztratív és működési terhek csökkentése érdekében az említett pénzügyi szervezeteknek csak egyetlen szabályzatot kell kidolgozniuk és dokumentálniuk, vagyis olyan információbiztonsági szabályzatot, amely meghatározza az adatok és az említett pénzügyi szervezetek szolgáltatásai bizalmas jellegének, integritásának, rendelkezésre állásának és hitelességének védelmét szolgáló magas szintű elveket és szabályokat.

(27) E rendelet rendelkezései kapcsolódnak az IKT-kockázatkezelési keretrendszer területéhez azáltal, hogy az (EU) 2022/2554 rendelet 15. cikkével összhangban részletezik a pénzügyi szervezetekre alkalmazandó konkrét elemeket, valamint kialakítják az említett rendelet 16. cikkének (1) bekezdésében meghatározott pénzügyi szervezetekre vonatkozó egyszerűsített IKT-kockázatkezelési keretrendszert. A rendes és az egyszerűsített IKT-kockázatkezelési keretrendszer közötti koherencia biztosítása érdekében, valamint tekintettel arra, hogy ezek a rendelkezések egyidejűleg válnak alkalmazandóvá, helyénvaló ezeket a rendelkezéseket egyetlen jogalkotási aktusba foglalni.

(28) Ez a rendelet az Európai Bankhatóság, az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság és az Európai Értékpapírpiaci Hatóság (európai felügyeleti hatóságok) által az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) egyeztetve a Bizottsághoz benyújtott szabályozástechnikai standardtervezeteken alapul.

([3]) Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o., ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Az Európai Parlament és a Tanács 600/2014/EU rendelete (2014. május 15.) a pénzügyi eszközök piacairól és a 648/2012/EU rendelet módosításáról (HL L 173., 2014.6.12., 84. o., ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Az Európai Parlament és a Tanács 909/2014/EU rendelete (2014. július 23.) az Európai Unión belüli értékpapír-kiegyenlítés javításáról és a központi értéktárakról, valamint 98/26/EK és a 2014/65/EU irányelv, valamint a 236/2012/EU rendelet módosításáról (HL L 257., 2014.8.28., 1. o., ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Az 1093/2010/EU európai parlamenti és tanácsi rendelet ([6]) 54. cikkében, az 1094/2010/EU európai parlamenti és tanácsi rendelet ([7]) 54. cikkében és az 1095/2010/EU európai parlamenti és tanácsi rendelet ([8]) 54. cikkében említett európai felügyeleti hatóságok vegyes bizottsága nyilvános konzultációt folytatott az e rendelet alapját képező szabályozástechnikai standardtervezetekről, elemezte a javasolt standardok esetleges költségeit és hasznát, továbbá kikérte az 1093/2010/EU rendelet 37. cikkével összhangban létrehozott Banki Érdekképviseleti Csoport, az 1094/2010/EU rendelet 37. cikkével összhangban létrehozott Biztosítási és Viszontbiztosítási Érdekképviseleti Csoport és Foglalkoztatói-nyugdíj Érdekképviseleti Csoport, valamint az 1095/2010/EU rendelet 37. cikkével összhangban létrehozott Értékpapírpiaci Érdekképviseleti Csoport tanácsát.

(30) Amennyiben az e jogi aktusban meghatározott kötelezettségek teljesítéséhez személyes adatok kezelése szükséges, teljes mértékben alkalmazni kell az (EU) 2016/679 ([9]) és az (EU) 2018/1725 európai parlamenti és tanácsi rendeletet ([10]). Például tiszteletben kell tartani az adattakarékosság elvét, amikor a személyes adatokat az események megfelelő észlelésének biztosítása érdekében gyűjtik. Az európai adatvédelmi biztossal is konzultációt folytattak e jogi aktus szövegtervezetéről,

ELFOGADTA EZT A RENDELETET:

I. CÍM

ÁLTALÁNOS ELV

1. cikk

Általános kockázati profil és összetettség

A II. címben említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök, valamint a III. címben említett egyszerűsített IKT-kockázatkezelési keretrendszer kidolgozása és végrehajtása során figyelembe kell venni a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és működése jellegét, nagyságrendjét és megnövekedett vagy csökkent összetettségének elemeit, beleértve a következőkkel kapcsolatos elemeket is:

a) titkosítás és kriptográfia;

b) IKT-műveletek biztonsága;

c) hálózatbiztonság;

([6]) Az Európai Parlament és a Tanács 1093/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 12. o., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Az Európai Parlament és a Tanács 1094/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság) létrehozásáról, valamint a 716/2009/EK határozat módosításáról és a 2009/79/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 48. o., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Az Európai Parlament és a Tanács 1095/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Értékpapírpiaci Hatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/77/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 84. o., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)(HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) IKT-projektmenedzsment és -változásmenedzsment;

e) az IKT-kockázat lehetséges hatása az adatok bizalmas jellegére, integritására és rendelkezésre állására, valamint a zavarok lehetséges hatása a pénzügyi szervezetek tevékenységeinek folytonosságára és rendelkezésre állására.

II. CÍM

AZ IKT-KOCKÁZATKEZELÉSI ESZKÖZÖK, MÓDSZEREK, FOLYAMATOK ÉS SZABÁLYZATOK TOVÁBBI HARMONIZÁCIÓJA AZ (EU) 2022/2554 RENDELET 15. CIKKÉVEL ÖSSZHANGBAN

I. FEJEZET

IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök

1. Szakasz

2. cikk

Az IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök általános elemei

(1) A pénzügyi szervezetek biztosítják, hogy az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzataik, információbiztonsági és kapcsolódó eljárásaik, protokolljaik és eszközeik beépüljenek IKT-kockázatkezelési keretrendszerükbe. A pénzügyi szervezetek létrehozzák az e fejezetben meghatározott azon IKT-biztonsági szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek:

a) garantálják a hálózatok biztonságát;

b) megfelelő biztosítékokat tartalmaznak a behatolások és az adatokkal való visszaélés ellen;

c) megőrzik az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét többek között kriptográfiai technikákkal;

d) garantálják a pontos és gyors, jelentős zavaroktól és indokolatlan késedelemtől mentes adattovábbítást.

(2) A pénzügyi szervezetek biztosítják, hogy az (1) bekezdésben említett IKT-biztonsági szabályzatok:

a) igazodjanak a pénzügyi szervezetnek az (EU) 2022/2554 rendelet 6. cikkének (8) bekezdésében említett digitális működési rezilienciára vonatkozó stratégiában foglalt információbiztonsági célkitűzéseihez;

b) feltüntessék az IKT-biztonsági szabályzatok vezető testület általi hivatalos elfogadásának időpontját;

c) mutatókat és intézkedéseket tartalmazzanak a következők céljából:

   i. az IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök végrehajtásának nyomon követése;

   ii. a végrehajtás alóli kivételek rögzítése;

   iii. annak biztosítása, hogy a ii. pontban említett kivételek esetén biztosított legyen a pénzügyi szervezet digitális működési rezilienciája;

d) minden szinten meghatározzák a személyzet felelősségi körét a pénzügyi szervezet IKT-biztonságának garantálása érdekében;

e) meghatározzák, hogy milyen következményekkel jár, ha a pénzügyi szervezet személyzete nem felel meg az IKT-biztonsági szabályzatoknak, amennyiben a pénzügyi szervezet egyéb szabályzatai nem tartalmaznak erre vonatkozó rendelkezéseket;

f) felsorolják a fenntartandó dokumentációt;

g) az összeférhetetlenség elkerülése érdekében meghatározzák a feladatok elkülönítését a három védelmi vonalra épülő modell vagy adott esetben más belső kockázatkezelési és -ellenőrzési modell összefüggésében;

h) figyelembe vegyék a vezető gyakorlatokat és adott esetben az 1025/2012/EU rendelet 2. cikkének 1. pontjában foglalt meghatározás szerinti szabványokat;

i) meghatározzák az IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök kidolgozásával, végrehajtásával és fenntartásával kapcsolatos szerepeket és felelősségi köröket;

j) felülvizsgálata az (EU) 2022/2554 rendelet 6. cikkének (5) bekezdése szerint megtörténjen;

k) figyelembe vegyék a pénzügyi szervezetet érintő lényeges változásokat, beleértve a pénzügyi szervezet tevékenységeinek vagy folyamatainak, a kiberfenyegetettségi helyzetnek vagy az alkalmazandó jogi kötelezettségeknek a lényeges változásait.

2. Szakasz

3. cikk

IKT-kockázatkezelés

A pénzügyi szervezetek olyan IKT-kockázatkezelési szabályzatokat és eljárásokat dolgoznak ki, dokumentálnak és hajtanak végre, amelyek a következők mindegyikét tartalmazzák:

a) az (EU) 2022/2554 rendelet 6. cikke (8) bekezdésének b) pontjával összhangban megállapított IKT-kockázati toleranciaszint jóváhagyásának feltüntetése;

b) az IKT-kockázatértékelés elvégzésének eljárása és módszertana, 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;

c) az azonosított és értékelt IKT-kockázatokhoz tartozó IKT-kockázatkezelési intézkedések azonosítására, végrehajtására és dokumentálására szolgáló eljárás, beleértve az ahhoz szükséges IKT-kockázatkezelési intézkedések meghatározását, hogy az IKT-kockázat az a) pontban említett kockázati toleranciaszinten belül maradjon;

d) a c) pontban említett IKT-kockázatkezelési intézkedések végrehajtását követően még fennálló fennmaradó IKT-kockázatok esetében:

   i. a fennmaradó IKT-kockázatok azonosítására vonatkozó rendelkezések;

   ii. a következőkkel kapcsolatos szerep- és felelősségi körök kijelölése:

      (1) a pénzügyi szervezet a) pontban említett kockázati toleranciaszintjét meghaladó fennmaradó IKT-kockázatok elfogadása;

      (2) az e d) pont iv. alpontjában említett felülvizsgálati eljárás;

   iii. az elfogadott fennmaradó IKT-kockázatok jegyzékének kidolgozása, beleértve elfogadásuk indokolását is;

   iv. az elfogadott fennmaradó IKT-kockázatok legalább évente egyszer történő felülvizsgálatára vonatkozó rendelkezések, beleértve a következőket:

      (1) a fennmaradó IKT-kockázatokban bekövetkező változások azonosítása;

      (2) a rendelkezésre álló kockázatcsökkentő intézkedések értékelése;

      (3) annak értékelése, hogy a fennmaradó IKT-kockázatok elfogadását indokoló okok a felülvizsgálat időpontjában még mindig érvényesek-e és alkalmazandók-e;

e) az alábbiak nyomon követésére vonatkozó rendelkezések:

   i. az IKT-kockázatokban és a kiberfenyegetettségi helyzetben bekövetkező változások;

   ii. belső és külső sérülékenységek és fenyegetések;

   iii. a pénzügyi szervezet IKT-kockázatának nyomon követése, amely lehetővé teszi az IKT-kockázati profilját esetlegesen befolyásoló változások azonnali észlelését;

f) azon folyamatra vonatkozó rendelkezések, amely biztosítja, hogy a pénzügyi szervezet üzleti stratégiájában és digitális működési rezilienciára vonatkozó stratégiájában bekövetkező változásokat figyelembe vegyék.

Az első bekezdés c) pontjának alkalmazásában az említett pontban említett eljárásnak biztosítania kell a következőket:

a) a végrehajtott IKT-kockázatkezelési intézkedések hatékonyságának nyomon követése;

b) annak értékelése, hogy a pénzügyi szervezet elérte-e a megállapított kockázati toleranciaszinteket;

c) annak értékelése, hogy a pénzügyi szervezet szükség esetén tett-e lépéseket ezen intézkedések kijavítására vagy jobbá tételére.

3. Szakasz

IKT-Eszközök kezelése

4. cikk

Az IKT-eszközök kezelésére vonatkozó szabályzat

(1) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-eszközök kezelésére vonatkozó szabályzatot.

(2) Az (1) bekezdésben említett, IKT-eszközök kezelésére vonatkozó szabályzat:

a) előírja az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban azonosított és osztályozott IKT-eszközök életciklusának nyomon követését és kezelését;

b) előírja, hogy a pénzügyi szervezet nyilvántartást vezessen a következők mindegyikéről:

i. az egyes IKT-eszközök egyedi azonosítója;

ii. minden IKT-eszköz fizikai vagy logikai helyére vonatkozó információk;

iii. minden IKT-eszköz (EU) 2022/2254 rendelet 8. cikkének (1) bekezdésében említett osztályozása;

iv. az IKT-eszközök tulajdonosainak személyazonossága;

v. az IKT-eszköz által támogatott üzleti funkciók és szolgáltatások;

vi. az IKT-üzletmenet-folytonossági követelmények, beleértve a helyreállítási időre és helyreállítási pontra vonatkozó célkitűzéseket;

vii. az IKT-eszköz ki lehet-e téve vagy ki van-e téve külső hálózatoknak, beleértve az internetet is;

viii. az IKT-eszközök és az egyes IKT-eszközöket használó üzleti funkciók közötti kapcsolatok és kölcsönös függőségek;

ix. adott esetben valamennyi IKT-eszköz esetében a harmadik fél IKT-szolgáltató rendszeres, kiterjesztett és egyedi támogató szolgáltatásainak záró időpontjai, amelyeket követően ezekhez az IKT-eszközökhöz azok értékesítője vagy egy harmadik fél IKT-szolgáltató már nem nyújt támogatást;

c) a mikrovállalkozásnak nem minősülő pénzügyi szervezetek esetében előírja, hogy az említett pénzügyi szervezeteknek nyilvántartást kell vezetniük az (EU) 2022/2554 rendelet 8. cikkének (7) bekezdésében említett, valamennyi elavult IKT-rendszerre vonatkozó egyedi IKT-kockázatértékelés elvégzéséhez szükséges információkról.

5. cikk

Az IKT-eszközök kezelésére vonatkozó eljárás

(1) A pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-eszközök kezelésére vonatkozó eljárást.

(2) Az (1) bekezdésben említett, IKT-eszközök kezelésére vonatkozó eljárás meghatározza az üzleti funkciókat támogató információs vagyonelemek és IKT-eszközök kritikusságának értékelésére vonatkozó kritériumokat. Az értékelésnek a következőket kell figyelembe vennie:

a) az említett üzleti funkciókhoz és azoknak az információs vagyonelemektől vagy IKT-eszközöktől való függőségéhez kapcsolódó IKT-kockázat;

b) az ilyen információs vagyonelemek és IKT-eszközök bizalmas jellegének, integritásának és rendelkezésre állásának elvesztése hogyan befolyásolná a pénzügyi szervezetek üzleti folyamatait és tevékenységeit.

4. Szakasz

Titkosítás és kriptográfia

6. cikk

Titkosítás és kriptográfiai ellenőrzések

(1) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzataik, eljárásaik, protokolljaik és eszközeik részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják a titkosításra és kriptográfiai ellenőrzésekre vonatkozó szabályzatot.

(2) A pénzügyi szervezetek jóváhagyott adatminősítés és IKT-kockázatértékelés eredményei alapján alakítják ki az (1) bekezdésben említett, titkosításra és kriptográfiai ellenőrzésekre vonatkozó szabályzatot. E szabályzatnak szabályoznia kell az alábbiak mindegyikét:

a) a használaton kívüli és továbbítás alatt álló adatok titkosítása;

b) a használatban lévő adatok titkosítása, szükség esetén;

c) a belső hálózati kapcsolatok és a külső felekkel folytatott forgalom titkosítása;

d) a kriptográfiai kulcsok 7. cikkben említett kezelése, meghatározva a kriptográfiai kulcsok helyes használatára, védelmére és életciklusára vonatkozó szabályokat.

A b) pont alkalmazásában, amennyiben a használatban lévő adatok titkosítása nem lehetséges, a pénzügyi szervezetek a használatban lévő adatokat elkülönített és védett környezetben dolgozzák fel, vagy azzal egyenértékű intézkedéseket hoznak az adatok bizalmas jellegének, integritásának, hitelességének és rendelkezésre állásának biztosítása érdekében.

(3) A pénzügyi szervezetek az (1) bekezdésben említett, titkosításra és kriptográfiai ellenőrzésekre vonatkozó szabályzatba belefoglalják a kriptográfiai technikák és felhasználási gyakorlatok kiválasztására vonatkozó kritériumokat, figyelembe véve a vezető gyakorlatokat és az 1025/2012/EU rendelet 2. cikkének 1. pontjában foglalt meghatározás szerinti szabványokat, valamint a releváns IKT-eszközöknek az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozását. Azok a pénzügyi szervezetek, amelyek nem képesek betartani a vezető gyakorlatokat vagy a szabványokat, vagy nem tudják a legmegbízhatóbb technikákat alkalmazni, olyan kockázatcsökkentő és nyomonkövetési intézkedéseket fogadnak el, amelyek biztosítják a kiberfenyegetésekkel szembeni rezilienciát.

(4) A pénzügyi szervezetek az (1) bekezdésben említett, titkosításra és kriptográfiai ellenőrzésekre vonatkozó szabályzatba belefoglalják a kriptográfiai technológia szükség szerinti, a kriptoanalízis területének fejlődése alapján történő frissítésére vagy megváltoztatására vonatkozó rendelkezéseket. E frissítéseknek vagy változtatásoknak biztosítaniuk kell, hogy a kriptográfiai technológia a 10. cikk (2) bekezdésének a) pontjában előírtaknak megfelelően reziliens maradjon a kiberfenyegetésekkel szemben. Azok a pénzügyi szervezetek, amelyek nem képesek frissíteni vagy megváltoztatni a kriptográfiai technológiát, olyan kockázatcsökkentő és nyomonkövetési intézkedéseket fogadnak el, amelyek biztosítják a kiberfenyegetésekkel szembeni rezilienciát.

(5) A pénzügyi szervezetek az (1) bekezdésben említett, titkosításra és kriptográfiai ellenőrzésekre vonatkozó szabályzatba belefoglalják a (3) és (4) bekezdéssel összhangban elfogadott kockázatcsökkentő és nyomonkövetési intézkedések elfogadásának rögzítésére, és az ilyen intézkedések indokolással ellátott magyarázatának megadására irányuló követelményt.

7. cikk

A kriptográfiai kulcsok kezelése

(1) A pénzügyi szervezetek a 6. cikk (2) bekezdésének d) pontjában említett, kriptográfiai kulcsok kezelésére vonatkozó szabályzatba belefoglalják a kriptográfiai kulcsok teljes életciklusuk során történő kezelésére vonatkozó követelményeket, beleértve e kriptográfiai kulcsok létrehozását, megújítását, tárolását, biztonsági mentését, archiválását, visszakeresését, továbbítását, visszahívását, visszavonását és megsemmisítését.

(2) A pénzügyi szervezetek azonosítják és végrehajtják a kriptográfiai kulcsok teljes életciklusuk során történő, elvesztéssel, illetéktelen hozzáféréssel, közzététellel és módosítással szembeni védelmét szolgáló kontrollokat. A pénzügyi szervezetek jóváhagyott adatminősítés és IKT-kockázatértékelés eredményei alapján alakítják ki az említett kontrollokat.

(3) A pénzügyi szervezetek a kriptográfiai kulcsok cseréjére vonatkozó módszereket dolgoznak ki és hajtanak végre arra az esetre, ha azok elvesznek, megsérülnek vagy biztonságuk veszélybe kerül.

(4) A pénzügyi szervezetek nyilvántartást hoznak létre és vezetnek valamennyi tanúsítványról és tanúsítványt tároló eszközről legalább a kritikus vagy fontos funkciókat támogató IKT-eszközök tekintetében. A pénzügyi szervezetek naprakészen tartják ezt a nyilvántartást.

(5) A pénzügyi szervezetek biztosítják a tanúsítványok azonnali megújítását azok lejárata előtt.

5. Szakasz

IKT-műveletek biztonsága

8. cikk

Az IKT-műveletekre vonatkozó szabályzatok és eljárások

(1) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-műveletekre vonatkozó szabályzatokat és eljárásokat. Ezek a szabályzatok és eljárások meghatározzák, hogy a pénzügyi szervezetek hogyan működtetik, követik nyomon, ellenőrzik és állítják helyre IKT-eszközeiket, beleértve az IKT-műveletek dokumentációját is.

(2) Az (1) bekezdésben említett, IKT-műveletekre vonatkozó szabályzatok és eljárások a következők mindegyikét tartalmazzák:

a) az IKT-eszközök leírása, beleértve a következők mindegyikét:

   i. az IKT-rendszerek biztonságos telepítésére, karbantartására, konfigurálására és leszerelésére vonatkozó követelmények;

   ii. az IKT-eszközök által használt információs vagyonelemek kezelésére vonatkozó követelmények, beleértve azok automatizált és kézi feldolgozását és kezelését is;

   iii. az elavult IKT-rendszerek azonosítására és ellenőrzésére vonatkozó követelmények;

b) az IKT-rendszerek kontrolljai és nyomon követése, beleértve a következők mindegyikét:

   i. az IKT-rendszerek biztonsági mentési és helyreállítási követelményei;

   ii. ütemezési követelmények, figyelembe véve az IKT-rendszerek közötti kölcsönös függőségeket;

   iii. az ellenőrzési nyomvonal és a rendszernaplóra vonatkozó információk protokolljai;

   iv. annak biztosítására vonatkozó követelmények, hogy a belső ellenőrzés és egyéb tesztek elvégzése minimalizálja az üzleti tevékenységek zavarait;

   v. az éles IKT-környezeteknek a fejlesztési, tesztelési és egyéb nem éles környezetektől való elkülönítésére vonatkozó követelmények;

   vi. az éles környezettől elkülönülő környezetben történő fejlesztésre és tesztelésre vonatkozó követelmények;

   vii az éles környezetekben történő fejlesztésre és tesztelésre vonatkozó követelmények;

c) az IKT-rendszereket érintő hibakezelés, beleértve a következők mindegyikét:

i. a hibák kezelésére vonatkozó eljárások és protokollok;

ii. támogatási és eszkalációs kapcsolatok, beleértve a külső támogatási kapcsolatokat is váratlan működési vagy technikai problémák esetére;

iii. az IKT-rendszer zavara esetén alkalmazandó újraindítási, visszavonási és helyreállítási eljárások.

A b) pont v. alpontjának alkalmazásában az elkülönítés során a 13. cikk első albekezdésének a) pontjában előírtak szerint figyelembe kell venni a környezet valamennyi összetevőjét, beleértve a fiókokat, az adatokat és a kapcsolatokat is.

A b) pont vii. alpontjának alkalmazásában az (1) bekezdésben említett szabályzatoknak és eljárásoknak elő kell írniuk, hogy azokat az eseteket, amikor a tesztelést éles környezetben végzik, egyértelműen azonosítani kell és meg kell indokolni, azok csak korlátozott időtartamra vonatkozhatnak, és azokat az érintett funkciónak a 16. cikk (6) bekezdésével összhangban jóvá kell hagynia. A pénzügyi szervezetek biztosítják az IKT-rendszerek és az éles adatok rendelkezésre állását, bizalmas jellegét, integritását és hitelességét az éles környezetben történő fejlesztési és tesztelési tevékenységek során.

9. cikk

Kapacitás- és teljesítménymenedzsment

(1) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják a kapacitás- és teljesítménymenedzsmentre vonatkozó eljárásokat az alábbiak tekintetében:

a) IKT-rendszereik kapacitásigényeinek azonosítása;

b) erőforrás-optimalizálás alkalmazása;

c) az alábbiak fenntartására és javítására szolgáló nyomonkövetési eljárások:

i. az adatok és az IKT-rendszerek rendelkezésre állása;

ii. az IKT-rendszerek hatékonysága;

iii. az IKT-kapacitáshiányok megelőzése.

(2) Az (1) bekezdésben említett, kapacitás- és teljesítménymenedzsmentre vonatkozó eljárásoknak biztosítaniuk kell, hogy a pénzügyi szervezetek megfelelő intézkedéseket hozzanak a hosszú vagy összetett beszerzési vagy jóváhagyási eljárásokkal rendelkező IKT-rendszerek vagy erőforrás-igényes IKT-rendszerek sajátosságainak figyelembevételére.

10. cikk

Sérülékenység-menedzsment és a javítócsomagok kezelése

(1) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják a sérülékenység-menedzsmentre vonatkozó eljárásokat.

(2) A (1) bekezdésben említett, sérülékenység-menedzsmentre vonatkozó eljárások szerepe a következő:

a) a releváns és megbízható információs erőforrások azonosítása és frissítése a sérülékenységekkel kapcsolatos tájékozottság kialakítása és fenntartása érdekében;

b) automatizált sérülékenységfelmérés és -értékelés elvégzésének biztosítása az IKT-eszközökön, amelynek során e tevékenységek gyakoriságának és körének arányban kell állnia az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozással és az IKT-eszköz általános kockázati profiljával;

c) az alábbiak ellenőrzése:

i. a harmadik fél IKT-szolgáltatók kezelik a pénzügyi szervezetnek nyújtott IKT-szolgáltatásokhoz kapcsolódó sérülékenységeket;

ii. az említett szolgáltatók időben jelentést tesznek-e a pénzügyi szervezetnek legalább a kritikus sérülékenységekről, statisztikákról és tendenciákról;

d) az alábbiak használatának nyomon követése:

i. a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások által használt, harmadik fél által készített könyvtárak, beleértve a nyílt forráskódú könyvtárakat is;

ii. a maga a pénzügyi szervezet által kifejlesztett vagy harmadik fél IKT-szolgáltató által kifejezetten a pénzügyi szervezet számára testreszabott vagy kifejlesztett IKT-szolgáltatások;

e) a sérülékenységeknek az ügyfelek, a partnerek és a nyilvánosság felé történő felelős közzétételére vonatkozó eljárások kialakítása;

f) a javítócsomagok telepítésének és az egyéb kockázatcsökkentő intézkedéseknek az előnyben részesítése az azonosított sérülékenységek kezelése érdekében;

g) a sérülékenységek korrekciójának nyomon követése és ellenőrzése;

h) az IKT-rendszereket érintő észlelt sérülékenységek nyilvántartásának és elhárításuk nyomon követésének előírása.

A b) pont alkalmazásában a pénzügyi szervezetek legalább hetente elvégzik a kritikus vagy fontos funkciókat támogató IKT-eszközök automatizált sérülékenységfelmérését és -értékelését.

A c) pont alkalmazásában a pénzügyi szervezetek felkérik a harmadik fél IKT-szolgáltatókat, hogy vizsgálják ki a releváns sérülékenységeket, határozzák meg a kiváltó okokat, és hajtsanak végre megfelelő kockázatcsökkentő intézkedést.

A d) pont alkalmazásában a pénzügyi szervezetek – adott esetben a harmadik fél IKT-szolgáltatóval együttműködve – nyomon követik a harmadik fél által készített könyvtárak verzióját és esetleges frissítéseit. A kritikus vagy fontos funkciókat nem támogató IKT-szolgáltatások működtetése során beszerzett és használt, használatra kész („polcról levehető") IKT-eszközök vagy azok ilyen komponensei esetében a pénzügyi szervezetek a lehető legteljesebb mértékben nyomon követik a harmadik fél által készített könyvtárak, köztük a nyílt forráskódú könyvtárak használatát.

Az f) pont alkalmazásában a pénzügyi szervezetek figyelembe veszik a sérülékenység kritikusságát, az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozást, valamint az azonosított sérülékenységek által érintett IKT-eszközök kockázati profilját.

(3) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják a javítócsomagok kezelésére vonatkozó eljárásokat.

(4) A (3) bekezdésben említett, javítócsomagok kezelésére vonatkozó eljárások szerepe a következő:

a) a rendelkezésre álló szoftver- és hardverhiba-javító csomagok és frissítések azonosítása és értékelése automatizált eszközökkel a lehető legteljesebb mértékben;

b) az IKT-eszközök hibajavítására és frissítésére szolgáló vészhelyzeti eljárások azonosítása;

c) a 8. cikk (2) bekezdése b) pontjának v., vi. és vii. alpontjában említett szoftver- és hardverhiba-javító csomagok és frissítések tesztelése és telepítése;

d) határidők megállapítása a szoftver- és hardverhiba-javító csomagok és frissítések telepítésére, valamint eszkalációs eljárások megállapítása arra az esetre, ha ezen határidők nem tarthatók be.

11. cikk

Adat- és rendszerbiztonság

(1) Az (EU) 2022/2554 rendelet 9. cikkének (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások, protokollok és eszközök részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az adat- és rendszerbiztonsági eljárást.

(2) Az (1) bekezdésben említett adat- és rendszerbiztonsági eljárásnak az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozásnak megfelelően tartalmaznia kell az adatok és az IKT-rendszer biztonságával kapcsolatos alábbi elemek mindegyikét:

a) az e rendelet 21. cikkében említett hozzáférési korlátozások, amelyek támogatják az egyes osztályozási szintekre vonatkozó védelmi követelményeket;

b) olyan biztonságos konfigurációs alapértékek meghatározása az IKT-eszközök számára, amelyek minimalizálják ezen IKT-eszközök kiberfenyegetéseknek való kitettségét, valamint az említett alapértékek hatékony alkalmazásának rendszeres ellenőrzésére irányuló intézkedések;

c) biztonsági intézkedések meghatározása annak biztosítására, hogy az IKT-rendszerekre és a végponti eszközökre csak engedélyezett szoftvereket telepítsenek;

d) rosszindulatú kódok elleni biztonsági intézkedések azonosítása;

e) biztonsági intézkedések azonosítása annak biztosítására, hogy a pénzügyi szervezet adatainak továbbítására és tárolására kizárólag engedélyezett adattárolókat, adathordozókat, rendszereket és végponti eszközöket használjanak;

f) a hordozható végponti eszközök és a magánjellegű nem hordozható végponti eszközök használatának biztosítására vonatkozó következő követelmények:

   i. a végponti eszközök távirányítása és a pénzügyi szervezet adatainak távolról történő törlése tekintetében irányítási megoldás alkalmazására vonatkozó követelmény;

   ii. a személyzet tagjai vagy harmadik fél IKT-szolgáltatók által jogosulatlanul nem módosítható, eltávolítható vagy megkerülhető biztonsági mechanizmusok használatára vonatkozó követelmény;

   iii. követelmény, amely előírja, hogy eltávolítható adattároló eszköz csak akkor használható, ha a fennmaradó IKT-kockázat a pénzügyi szervezet 3. cikk első albekezdésének a) pontjában említett kockázati tolerancia-szintjén belül marad;

g) a pénzügyi szervezet telephelyein található vagy külső helyszínen tárolt olyan adatok biztonságos törlésének folyamata, amelyeket a pénzügyi szervezetnek már nem kell gyűjtenie vagy tárolnia;

h) a pénzügyi szervezet telephelyein található vagy külső helyszínen tárolt, bizalmas információkat tartalmazó adattároló eszközök biztonságos ártalmatlanításának vagy leszerelésének folyamata;

i) a rendszerek és végponti eszközök esetében az adatvesztés és -szivárgás megelőzésére szolgáló biztonsági intézkedések azonosítása és végrehajtása;

j) biztonsági intézkedések végrehajtása annak biztosítása érdekében, hogy a távmunka és a magánjellegű végponti eszközök használata ne befolyásolja hátrányosan a pénzügyi szervezet IKT-biztonságát;

k) a harmadik fél IKT-szolgáltató által üzemeltetett IKT-eszközök és -szolgáltatások esetében a digitális működési reziliencia fenntartására vonatkozó követelmények azonosítása és végrehajtása, az adatminősítés és az IKT-kockázatértékelés eredményeivel összhangban.

A b) pont alkalmazásában az abban a pontban említett biztonságos konfigurációs alapértékeknek figyelembe kell venniük a vezető gyakorlatokat és az 1025/2012/EU rendelet 2. cikkének 1. pontjában foglalt meghatározás szerinti szabványokban lefektetett megfelelő technikákat.

A k) pont alkalmazásában a pénzügyi szervezetek figyelembe veszik a következőket:

a) a beszállító által ajánlott beállítások végrehajtása a pénzügyi szervezet által működtetett elemeken;

b) az információbiztonsággal kapcsolatos szerep- és felelősségi körök egyértelmű megosztása a pénzügyi szervezet és a harmadik fél IKT-szolgáltató között, a pénzügyi szervezetnek az (EU) 2022/2554 rendelet 28. cikke (1) bekezdésének a) pontjában említett, harmadik fél IKT-szolgáltatóval szembeni és az említett rendelet 28. cikkének (2) bekezdésében említett, pénzügyi szervezetekkel szembeni teljeskörű felelőssége elvével összhangban, valamint a pénzügyi szervezetnek a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozó szabályzatával összhangban;

c) a pénzügyi szervezeten belül megfelelő kompetenciák biztosításának és fenntartásának szükségessége az igénybe vett szolgáltatás irányítása és biztonsága terén;

d) a harmadik fél IKT-szolgáltató által az IKT-szolgáltatásaihoz használt infrastruktúrával kapcsolatos kockázatok minimalizálását célzó technikai és szervezeti intézkedések, figyelembe véve a vezető gyakorlatokat és az 1025/2012/EU rendelet 2. cikkének 1. pontjában foglalt meghatározás szerinti szabványokat.

12. cikk

Naplózás

(1) A pénzügyi szervezetek a behatolás és az adatokkal való visszaélés elleni biztosítékok részeként naplózási eljárásokat, protokollokat és eszközöket dolgoznak ki, dokumentálnak és hajtanak végre.

(2) Az (1) bekezdésben említett naplózási eljárások, protokollok és eszközök a következők mindegyikét tartalmazzák:

a) a naplózandó események azonosítása, a naplók megőrzési ideje, valamint a naplóadatok biztonságát és kezelését célzó intézkedések, figyelembe véve a naplók létrehozásának célját;

b) a naplók részletességi szintjének összehangolása céljukkal és felhasználásukkal a 24. cikkben említett rendellenes tevékenységek hatékony észlelésének lehetővé tétele érdekében;

c) az események naplózására vonatkozó követelmény a következők mindegyikével kapcsolatban:

i. a 21. cikkben említett logikai és fizikai hozzáférés-ellenőrzés, valamint a személyazonosság-kezelés;

ii. kapacitásmenedzsment;

iii. változásmenedzsment;

iv. IKT-műveletek, beleértve az IKT-rendszerekkel kapcsolatos tevékenységeket is;

v. hálózati forgalmi tevékenységek, beleértve az IKT-hálózat teljesítményét is;

d) a naplózási rendszerek és a használaton kívüli, továbbítás alatt álló és adott esetben használatban lévő naplóadatok hamisítással, törléssel és jogosulatlan hozzáféréssel szembeni védelmére irányuló intézkedések;

e) a naplózási rendszerek meghibásodásának észlelésére irányuló intézkedések;

f) bármely uniós vagy nemzeti jog alapján alkalmazandó szabályozási követelmény sérelme nélkül, a pénzügyi szervezet valamennyi IKT-rendszere órájának szinkronizálása dokumentált megbízható referencia-időforrás alapján.

Az a) pont alkalmazásában a pénzügyi szervezetek a megőrzési idő meghatározásakor figyelembe veszik az üzleti és információbiztonsági célkitűzéseket, az esemény naplókban való rögzítésének okát és az IKT-kockázatértékelés eredményeit.

6. Szakasz

Hálózatbiztonság

13. cikk

A hálózatbiztonság kezelése

A pénzügyi szervezetek a hálózatok biztonságát a behatolásokkal és az adatokkal való visszaéléssel szemben garantáló biztosítékok részeként kidolgozzák, dokumentálják és végrehajtják a hálózatbiztonság kezelésére vonatkozó szabályzatokat, eljárásokat, protokollokat és eszközöket, beleértve a következők mindegyikét:

a) az IKT-rendszerek és -hálózatok elkülönítése és szegmentálása, figyelembe véve a következőket:

i. ezen IKT-rendszerek és -hálózatok által támogatott funkció kritikussága vagy fontossága;

ii. az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozás;

iii. az említett IKT-rendszereket és -hálózatokat használó IKT-eszközök általános kockázati profilja;

b) a pénzügyi szervezet valamennyi hálózati kapcsolatának és adatáramlásának dokumentálása;

c) külön, erre kijelölt hálózat használata az IKT-eszközök kezelésére;

d) hálózati hozzáférés-ellenőrzések azonosítása és végrehajtása a pénzügyi szervezet hálózatához való, jogosulatlan eszköz vagy rendszer, vagy a pénzügyi szervezet biztonsági követelményeinek nem megfelelő végpont általi kapcsolat megelőzése és észlelése érdekében;

e) a vállalati hálózatokon, nyilvános hálózatokon, belföldi hálózatokon, harmadik felek hálózatain és vezeték nélküli hálózatokon áthaladó hálózati kapcsolatok titkosítása az alkalmazott kommunikációs protokollok esetében, figyelembe véve a jóváhagyott adatminősítés eredményeit, az IKT-kockázatértékelés eredményeit és a hálózati kapcsolatok 6. cikk (2) bekezdésében említett titkosítását;

f) a hálózatoknak a pénzügyi szervezet által meghatározott IKT-biztonsági követelményekkel összhangban történő kialakítása, figyelembe véve a hálózat bizalmas jellegének, integritásának és rendelkezésre állásának biztosítására irányuló vezető gyakorlatokat;

g) a belső hálózatok és az internet és más külső kapcsolatok közötti hálózati forgalom biztosítása;

h) a tűzfalszabályok és kapcsolatszűrők meghatározásával, végrehajtásával, jóváhagyásával, módosításával és felülvizsgálatával kapcsolatos szerep- és felelősségi körök, illetve lépések azonosítása;

i) a hálózati architektúra és a hálózatbiztonság kialakítása felülvizsgálatának elvégzése évente egyszer, illetve mikrovállalkozások esetén rendszeres időközönként, a potenciális sérülékenységek azonosítása érdekében;

j) szükség esetén az alhálózatok, valamint a hálózati összetevők és eszközök ideiglenes elszigetelésére irányuló intézkedések;

k) valamennyi hálózati összetevő biztonságos konfigurációs alapértékeinek végrehajtása, valamint a hálózat és a hálózati eszközök megerősítése a beszállítói utasításokkal, adott esetben az 1025/2012/EU rendelet 2. cikkének 1. pontjában foglalt meghatározás szerinti szabványokkal és a vezető gyakorlatokkal összhangban;

l) a rendszer és a távoli munkamenetek meghatározott inaktivitási időszakot követő korlátozására, lezárására és megszakítására szolgáló eljárások;

m) a hálózati szolgáltatásokról szóló megállapodások esetében:

   i. az IKT- és információbiztonsági intézkedések, a szolgáltatási szintek és az irányítási követelmények azonosítása és részletes meghatározása minden hálózati szolgáltatás tekintetében;

   ii. annak feltüntetése, hogy a szolgáltatásokat csoporton belüli IKT-szolgáltató vagy harmadik fél IKT-szolgáltatók nyújtják-e.

A h) pont alkalmazásában a pénzügyi szervezetek az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozásnak és az érintett IKT-rendszerek általános kockázati profiljának megfelelően rendszeresen elvégzik a tűzfalszabályok és a kapcsolatszűrők felülvizsgálatát. A kritikus vagy fontos funkciókat támogató IKT-rendszerek esetében a pénzügyi szervezetek legalább hathavonta ellenőrzik a meglévő tűzfalszabályok és kapcsolatszűrők megfelelőségét.

14. cikk

A továbbítás alatt álló információk biztonsága

(1) Az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzését szolgáló biztosítékok részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják a továbbítás alatt álló információk védelmét szolgáló szabályzatokat, eljárásokat, protokollokat és eszközöket. A pénzügyi szervezetek különösen a következők mindegyikét biztosítják:

a) az adatok rendelkezésre állása, hitelessége, integritása és bizalmas jellege a hálózati továbbítás során, valamint az ezen követelményeknek való megfelelés értékelésére vonatkozó eljárások megállapítása;

b) az adatszivárgások megelőzése és észlelése, valamint az információk biztonságos továbbítása a pénzügyi szervezet és a külső felek között;

c) a pénzügyi szervezet információvédelemmel kapcsolatos igényeit mind a pénzügyi szervezet, mind a külső felek alkalmazottai tekintetében tükröző titoktartási megállapodásokra vonatkozó követelmények végrehajtása, dokumentálása és rendszeres felülvizsgálata.

(2) A pénzügyi szervezetek a jóváhagyott adatminősítés és az IKT-kockázatértékelés eredményei alapján alakítják ki az (1) bekezdésben említett, a továbbítás alatt álló információk védelmét szolgáló szabályzatokat, eljárásokat, protokollokat és eszközöket.

7. Szakasz

IKT-projektmenedzsment és -változásmenedzsment

15. cikk

IKT-projektmenedzsment

(1) Az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzését szolgáló biztosítékok részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-projektmenedzsmentre vonatkozó szabályzatot.

(2) Az (1) bekezdésben említett, IKT-projektmenedzsmentre vonatkozó szabályzatban meg kell határozni azokat az elemeket, amelyek biztosítják a pénzügyi szervezet IKT-rendszereinek beszerzéséhez, karbantartásához és adott esetben fejlesztéséhez kapcsolódó IKT-projektek hatékony irányítását.

(3) Az (1) bekezdésben említett, IKT-projektmenedzsmentre vonatkozó szabályzat a következők mindegyikét tartalmazza:

a) az IKT-projekt célkitűzései;

b) az IKT-projekt irányítása, beleértve a szerep- és felelősségi köröket;

c) az IKT-projekt tervezése, időkerete és lépései;

d) az IKT-projekt kockázatértékelése;

e) a releváns mérföldkövek;

f) a változásmenedzsmenttel kapcsolatos követelmények;

g) valamennyi követelmény, köztük a biztonsági követelmények tesztelése, valamint a vonatkozó jóváhagyási eljárás az IKT-rendszer éles környezetben történő telepítésekor.

(4) Az (1) bekezdésben említett, IKT-projektmenedzsmentre vonatkozó szabályzatnak biztosítania kell az IKT-projekt biztonságos végrehajtását azáltal, hogy biztosítja a szükséges információt és szakértelmet az IKT-projekt által érintett üzleti területtől vagy funkcióktól.

(5) Az IKT-projekt (3) bekezdés d) pontjában említett kockázatértékelésével összhangban az (1) bekezdésben említett, IKT-projektmenedzsmentre vonatkozó szabályzatnak elő kell írnia, hogy a pénzügyi szervezet kritikus vagy fontos funkcióit érintő IKT-projektek létrehozását és előrehaladását, valamint az azokhoz kapcsolódó kockázatokat a következők szerint kell jelenteni a vezető testületnek:

a) önállóan vagy összesítve, az IKT-projektek jelentőségétől és méretétől függően;

b) rendszeres időközönként és szükség esetén eseti alapon.

16. cikk

IKT-rendszerek beszerzése, fejlesztése és karbantartása

(1) Az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzését szolgáló biztosítékok részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-rendszerek beszerzésére, fejlesztésére és karbantartására irányadó szabályzatot. E szabályzat a következőkre szolgál:

a) az IKT-rendszerek beszerzésével, fejlesztésével és karbantartásával kapcsolatos biztonsági gyakorlatok és módszerek azonosítása;

b) a következők azonosításának előírása:

   i. az 1025/2012/EU rendelet 2. cikkének 4. és 5. pontjában foglalt meghatározás szerinti műszaki előírások és IKT műszaki előírások;

   ii. az IKT-rendszerek beszerzésére, fejlesztésére és karbantartására vonatkozó követelmények, különös tekintettel az IKT-biztonsági követelményekre, valamint azoknak az érintett üzleti funkció és az IKT-eszköz tulajdonosa által a pénzügyi szervezet belső irányítási rendszereivel összhangban történő jóváhagyására;

c) olyan intézkedések meghatározása, amelyek csökkentik az IKT-rendszerek nem szándékos megváltoztatásának vagy szándékos manipulálásának kockázatát az ezen IKT-rendszerek éles környezetben történő fejlesztése, karbantartása és telepítése alatt.

(2) A pénzügyi szervezetek a 8. cikk (2) bekezdése b) pontjának v., vi. és vii. alpontjával összhangban kidolgozzák, dokumentálják és végrehajtják az IKT-rendszerek beszerzési, fejlesztési és karbantartási eljárását valamennyi IKT-rendszer használat előtti és karbantartás utáni tesztelésére és jóváhagyására vonatkozóan. A tesztelés szintjének arányosnak kell lennie az érintett üzleti eljárások és IKT-eszközök kritikusságával. A tesztelést úgy kell megtervezni, hogy a segítségével ellenőrizhető legyen, hogy az új IKT-rendszerek megfelelőek-e a rendeltetésszerű működésre, beleértve a belső fejlesztésű szoftver minőségét is.

A központi szerződő felek az első albekezdésben meghatározott követelményeken túl adott esetben a következő feleket is bevonják az első albekezdésben említett tesztelés megtervezésébe és végrehajtásába:

a) klíringtagok és ügyfelek;

b) interoperábilis központi szerződő felek;

c) egyéb érdekelt felek.

A központi értéktárak az első albekezdésben meghatározott követelményeken túl adott esetben a következő feleket is bevonják az első albekezdésben említett tesztelés megtervezésébe és végrehajtásába:

a) felhasználók;

b) kritikus közüzemi szolgáltatók és kritikus szolgáltatók;

c) egyéb központi értéktárak;

d) más piaci infrastruktúrák;

e) bármely egyéb intézmény, amellyel kapcsolatban a központi értéktárak kölcsönös függőségeket azonosítottak az üzletmenet-folytonossági politikájukban.

(3) A (2) bekezdésben említett eljárás magában foglalja mind a statikus, mind a dinamikus tesztelésre kiterjedő forráskódvizsgálatok elvégzését. E tesztelésnek magában kell foglalnia az internetnek kitett rendszerek és alkalmazások biztonsági tesztelését a 8. cikk (2) bekezdése b) pontjának v., vi. és vii. alpontjával összhangban. A pénzügyi szervezetek:

a) azonosítják és elemzik a forráskódban található sérülékenységeket és rendellenességeket;

b) cselekvési tervet fogadnak el e sérülékenységek és rendellenességek kezelésére;

c) nyomon követik e cselekvési terv végrehajtását.

(4) A (2) bekezdésben említett eljárás magában foglalja a szoftvercsomagok biztonsági tesztelését legkésőbb az integrációs szakaszban, a 8. cikk (2) bekezdése b) pontjának v., vi. és vii. alpontjával összhangban.

(5) A (2) bekezdésben említett eljárás előírja a következőket:

a) a nem éles környezetek csak anonimizált, álnevesített vagy randomizált éles adatokat tárolnak;

b) a pénzügyi szervezetek védik az adatok integritását és bizalmas jellegét a nem éles környezetekben.

(6) Az (5) bekezdéstől eltérve a (2) bekezdésben említett eljárás előírhatja, hogy éles adatokat csak meghatározott tesztelési alkalmak esetén, korlátozott ideig lehessen tárolni, az érintett funkció jóváhagyását és az ilyen alkalmak IKT-kockázatkezelési funkciónak való bejelentését követően.

(7) A (2) bekezdésben említett eljárás magában foglalja a házon belül vagy harmadik fél IKT-szolgáltató által kifejlesztett és harmadik fél IKT-szolgáltató által a pénzügyi szervezetnek nyújtott IKT-rendszerek forráskódja integritásának védelmét szolgáló kontrollok végrehajtását.

(8) A (2) bekezdésben említett eljárás előírja, hogy a zárt forráskódú szoftvereket és – amennyiben megvalósítható – a harmadik fél IKT-szolgáltatók által biztosított vagy nyílt forráskódú projektekből származó forráskódot a (3) bekezdéssel összhangban elemezni és tesztelni kell, mielőtt azokat éles környezetben telepítenék.

(9) E cikk (1)–(8) bekezdése az IKT-funkción kívüli felhasználók által kifejlesztett vagy kezelt IKT-rendszerekre is alkalmazandó, kockázatalapú megközelítést alkalmazva.

17. cikk

IKT-változásmenedzsment

(1) Az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzését szolgáló biztosítékok részeként a pénzügyi szervezetek az (EU) 2022/2554 rendelet 9. cikke (4) bekezdésének e) pontjában említett, IKT-változásmenedzsmentre vonatkozó eljárásokba a szoftver-, hardver-, belsővezérlőprogram-összetevők, rendszerek és biztonsági paraméterek valamennyi változása tekintetében belefoglalják a következő elemek mindegyikét:

a) annak ellenőrzése, hogy az IKT-biztonsági követelmények teljesültek-e;

b) a változtatásokat jóváhagyó funkciók, valamint a változtatások kérelmezéséért és végrehajtásáért felelős funkciók függetlenségét biztosító mechanizmusok;

c) a szerep- és felelősségi körök egyértelmű leírása az alábbiak biztosítása érdekében:

   i. a változtatások részletes meghatározása és megtervezése;

   ii. a megfelelő átállás kidolgozása;

   iii. a változtatások tesztelése és véglegesítése ellenőrzött módon;

   iv. hatékony minőségbiztosítás;

d) a változtatás részleteinek dokumentálása és közlése, beleértve a következőket:

   i. a változtatás célja és hatóköre;

   ii. a változtatás végrehajtásának ütemterve;

   iii. a várt eredmények;

e) a tartalékeljárások és felelősségi körök meghatározása, beleértve a változtatások megszakítására vagy a nem sikeresen végrehajtott változtatásokból való helyreállításra vonatkozó eljárásokat és felelősségi köröket;

f) a vészhelyzeti változtatások kezelésére szolgáló eljárások, protokollok és eszközök, amelyek megfelelő biztosítékokat nyújtanak;

g) a vészhelyzeti változtatások dokumentálására, újraértékelésére, értékelésére és jóváhagyására vonatkozó eljárások a végrehajtásukat követően, beleértve a megkerülő megoldásokat és a javítócsomagokat is;

h) a változtatás meglévő IKT-biztonsági intézkedésekre gyakorolt lehetséges hatásának azonosítása, valamint annak értékelése, hogy az ilyen változtatás szükségessé teszi-e további IKT-biztonsági intézkedések elfogadását.

(2) IKT-rendszereik jelentős változtatásait követően a központi szerződő felek és a központi értéktárak stresszhelyzetek szimulálásával szigorú tesztelésnek vetik alá IKT-rendszereiket.

A központi szerződő felek adott esetben a következő feleket is bevonják az első albekezdésben említett tesztelés megtervezésébe és végrehajtásába:

a) klíringtagok és ügyfelek;

b) interoperábilis központi szerződő felek;

c) egyéb érdekelt felek.

A központi értéktárak adott esetben a következő feleket is bevonják az első albekezdésben említett tesztelés megtervezésébe és végrehajtásába:

a) felhasználók;

b) kritikus közüzemi szolgáltatók és kritikus szolgáltatók;

c) egyéb központi értéktárak;

d) más piaci infrastruktúrák;

e) bármely egyéb intézmény, amellyel kapcsolatban a központi értéktárak kölcsönös függőségeket azonosítottak az IKT-üzletmenet-folytonossági politikájukban.

8. Szakasz

18. cikk

Fizikai és környezetbiztonság

(1) Az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzését szolgáló biztosítékok részeként a pénzügyi szervezetek részletesen meghatározzák, dokumentálják és végrehajtják a fizikai és környezetbiztonsági szabályzatot. A pénzügyi szervezetek ezt a szabályzatot a kiberfenyegetettségi helyzet fényében, az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozásnak megfelelően, valamint az IKT-eszközök és a hozzáférhető információs vagyonelemek általános kockázati profiljának fényében alakítják ki.

(2) Az (1) bekezdésben említett fizikai és környezetbiztonsági szabályzat a következők mindegyikét tartalmazza:

a) hivatkozás a hozzáférés-kezelési jogosultságok ellenőrzésére vonatkozó szabályzat 21. cikk első albekezdésének g) pontjában említett szakaszára;

b) a pénzügyi szervezet IKT-eszközöknek és információs vagyonelemeknek helyet adó telephelyei és adatközpontjai, valamint az IKT-eszközöknek és információs vagyonelemeknek helyet adó, a pénzügyi szervezet által kijelölt érzékeny területek támadásokkal, balesetekkel és környezeti fenyegetésekkel és veszélyekkel szembeni védelmet célzó intézkedések;

c) az IKT-eszközöknek mind a pénzügyi szervezet telephelyén belüli, mind azon kívüli védelmét célzó intézkedések, figyelembe véve a releváns IKT-eszközökhöz kapcsolódó IKT-kockázatértékelés eredményeit;

d) a pénzügyi szervezet IKT-eszközeinek, információs vagyonelemeinek és fizikai hozzáférés-ellenőrzési eszközeinek rendelkezésre állását, hitelességét, integritását és bizalmas jellegét a megfelelő karbantartás révén biztosító intézkedések;

e) az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megőrzését szolgáló intézkedések, beleértve a következőket:

   i. üres asztal politika a dokumentumokra vonatkozóan;

   ii. tiszta képernyő politika az információfeldolgozó létesítményekre vonatkozóan.

A b) pont alkalmazásában a környezeti fenyegetésekkel és veszélyekkel szembeni védelmet célzó intézkedéseknek arányban kell állniuk a telephelyek, adatközpontok és kijelölt érzékeny területek fontosságával, valamint az ott végzett műveletek vagy ott található IKT-rendszerek kritikusságával.

A c) pont alkalmazásában az (1) bekezdésben említett fizikai és környezetbiztonsági szabályzat tartalmazza a felügyelet nélküli IKT-eszközök megfelelő védelmét biztosító intézkedéseket.

II. FEJEZET

Humánerőforrás-politika és hozzáférés-ellenőrzés

19. cikk

Humánerőforrás-politika

A pénzügyi szervezetek humánerőforrás-politikájukban vagy más vonatkozó szabályzataikban feltüntetik az IKT-biztonsággal kapcsolatos alábbi elemek mindegyikét:

a) az IKT-biztonsággal kapcsolatos valamennyi konkrét felelősségi kör azonosítása és kijelölése;

b) a pénzügyi szervezetnek és a harmadik fél IKT-szolgáltatóknak a pénzügyi szervezet IKT-eszközeit használó vagy azokhoz hozzáféréssel rendelkező személyzetére vonatkozó követelmények az alábbiak tekintetében:

i. tájékoztatás a pénzügyi szervezet IKT-biztonsági szabályzatairól, eljárásairól és protokolljairól, és azok betartása;

ii. a pénzügyi szervezet által a rendellenes magatartásformák felderítésére létrehozott bejelentési csatornák ismerete, beleértve adott esetben az (EU) 2019/1937 európai parlamenti és tanácsi irányelvvel [11] összhangban létrehozott bejelentési csatornákat is;

iii. a személyzet munkaviszonyának megszűnésekor a birtokukban lévő összes olyan IKT-eszköz és tárgyi információs vagyonelem visszaszolgáltatása a pénzügyi szervezetnek, amely a pénzügyi szervezet tulajdona.

20. cikk

Személyazonosság-kezelés

(1) A hozzáférés-kezelési jogosultságok ellenőrzésének részeként a pénzügyi szervezetek olyan személyazonosság-kezelési szabályzatokat és eljárásokat dolgoznak ki, dokumentálnak és hajtanak végre, amelyek biztosítják a pénzügyi szervezetek információihoz hozzáféréssel rendelkező természetes személyek és rendszerek egyedi azonosítását és hitelesítését a felhasználói hozzáférési jogosultságok 21. cikkel összhangban történő kiosztásának lehetővé tétele érdekében.

(2) Az (1) bekezdésben említett személyazonosság-kezelési szabályzatok és eljárások a következők mindegyikét tartalmazzák:

a) a 21. cikk első albekezdése c) pontjának sérelme nélkül egyedi felhasználói fióknak megfelelő egyedi azonosítót kell rendelni a pénzügyi szervezet és a harmadik fél IKT-szolgáltatók személyzetének a pénzügyi szervezet információs vagyonelemeihez és IKT-eszközeihez hozzáféréssel rendelkező valamennyi tagjához;

b) a valamennyi fiók létrehozását, módosítását, felülvizsgálatát és frissítését, ideiglenes inaktiválását és megszüntetését kezelő személyazonosságok és fiókok életciklus-kezelési folyamata.

Az a) pont alkalmazásában a pénzügyi szervezetek nyilvántartást vezetnek valamennyi személyazonosság kiosztásáról. Ezeket a nyilvántartásokat a pénzügyi szervezet átszervezését követően vagy a szerződéses jogviszony megszűnését követően is meg kell őrizni, az alkalmazandó uniós és nemzeti jogban meghatározott megőrzési követelmények sérelme nélkül.

A b) pont alkalmazásában a pénzügyi szervezetek – amennyiben megvalósítható és helyénvaló – automatizált megoldásokat alkalmaznak az életciklus-alapú személyazonosság-kezelési folyamatra.

21. cikk

Hozzáférés-ellenőrzés

A hozzáférés-kezelési jogosultságok ellenőrzésének részeként a pénzügyi szervezetek a következők mindegyikét tartalmazó szabályzatot dolgoznak ki, dokumentálnak és hajtanak végre:

a) az IKT-eszközökhöz való hozzáférési jogosultságok kiosztása a szükséges ismeret elve, a szükséges használat elve és a legkisebb jogosultság elve alapján, beleértve a távoli és vészhelyzeti hozzáférést is;

b) a feladatok elkülönítése, amelynek célja a kritikus adatokhoz való indokolatlan hozzáférés megakadályozása és a hozzáférési jogosultságok olyan kombinációi kiosztásának megakadályozása, amelyek felhasználhatók az ellenőrzések megkerülésére;

c) a felhasználói elszámoltathatóságról szóló rendelkezés, amely a lehető legnagyobb mértékben korlátozza az általános és közös felhasználói fiókok használatát, és biztosítja, hogy a felhasználók mindenkor azonosíthatók legyenek az IKT-rendszerekben végzett tevékenységek tekintetében;

[11] Az Európai Parlament és a Tanács (EU) 2019/1937 irányelve (2019. október 23.) az uniós jog megsértését bejelentő személyek védelméről (HL L 305., 2019.11.26., 17. o., ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) az IKT-eszközökhöz való hozzáférés korlátozására vonatkozó rendelkezés, amely meghatározza a jogosulatlan hozzáférés megakadályozását célzó ellenőrzéseket és eszközöket;

e) a felhasználói és általános fiókokhoz, köztük az általános rendszergazdai fiókokhoz való hozzáférési jogosultságok megadására, módosítására vagy visszavonására vonatkozó fiókkezelési eljárások, beleértve a következők mindegyikére vonatkozó rendelkezést:

i. a hozzáférési jogosultságok megadásával, felülvizsgálatával és visszavonásával kapcsolatos szerep- és felelősségi körök kijelölése

ii. a kiemelt, vészhelyzeti és rendszergazdai hozzáférés kiosztása a szükséges használat elve alapján vagy eseti alapon minden IKT-rendszer esetében;

iii. a hozzáférési jogosultságok indokolatlan késedelem nélküli visszavonása a munkaviszony megszűnésekor, vagy ha a hozzáférésre már nincs szükség;

iv. a hozzáférési jogosultságok aktualizálása, amennyiben módosításra van szükség, illetve a kritikus vagy fontos funkciókat támogató IKT-rendszerektől eltérő valamennyi IKT-rendszer esetében legalább évente egyszer, a kritikus vagy fontos funkciókat támogató IKT-rendszerek esetében pedig legalább hathavonta.

f) hitelesítési módszerek, beleértve a következők mindegyikét:

i. az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozással és az IKT-eszközök általános kockázati profiljával arányos hitelesítési módszerek alkalmazása, figyelembe véve a vezető gyakorlatokat;

ii. a vezető gyakorlatokkal és technikákkal összhangban erős hitelesítési módszerek alkalmazása a pénzügyi szervezet hálózatához való távoli hozzáféréshez, a kiemelt hozzáféréshez, a kritikus vagy fontos funkciókat támogató IKT-eszközökhöz vagy a nyilvánosan hozzáférhető IKT-eszközökhöz való hozzáféréshez;

g) fizikai hozzáférés-ellenőrzési intézkedések, beleértve a következőket:

i. azon természetes személyek azonosítása és naplózása, akik beléphetnek a pénzügyi szervezet IKT-eszközöknek és információs vagyonelemeknek helyet adó telephelyeire és adatközpontjaiba, valamint az IKT-eszközöknek és információs vagyonelemeknek helyet adó, a pénzügyi szervezet által kijelölt érzékeny területekre;

ii. a kritikus IKT-eszközökhöz való fizikai hozzáférési jogosultságok biztosítása kizárólag az arra jogosult személyek számára, a szükséges ismeret és a legkisebb jogosultság elvével összhangban, és eseti alapon;

iii. a pénzügyi szervezet IKT-eszközöknek és információs vagyonelemeknek helyet adó telephelyeihez és adatközpontjaihoz, valamint az IKT-eszközöknek és információs vagyonelemeknek helyet adó, a pénzügyi szervezet által kijelölt érzékeny területekhez való fizikai hozzáférés nyomon követése;

iv. a fizikai hozzáférési jogosultságok felülvizsgálata a szükségtelen hozzáférési jogosultságok haladéktalan visszavonásának biztosítása érdekében.

Az e) pont i. alpontjának alkalmazásában a pénzügyi szervezetek a megőrzési idő meghatározásakor figyelembe veszik az üzleti és információbiztonsági célkitűzéseket, az esemény naplókban való rögzítésének okait és az IKT-kockázatértékelés eredményeit.

Az e) pont ii. alpontjának alkalmazásában a pénzügyi szervezetek lehetőség szerint külön fiókokat használnak az IKT-rendszerekkel kapcsolatos rendszergazdai feladatok ellátásához. Amennyiben megvalósítható és helyénvaló, a pénzügyi szervezetek automatizált megoldásokat alkalmaznak a kiemelt hozzáférések kezelésére.

A g) pont i. alpontjának alkalmazásában a személyazonosításnak és a naplózásnak arányban kell állnia a telephelyek, adatközpontok és kijelölt érzékeny területek fontosságával, valamint az ott végzett műveletek vagy ott található IKT-rendszerek kritikusságával.

A g) pont iii. alpontjának alkalmazásában a nyomon követésnek arányban kell állnia az (EU) 2022/2554 rendelet 8. cikkének (1) bekezdésével összhangban megállapított osztályozással és a hozzáféréssel érintett terület kritikusságával.

III. FEJEZET

IKT-vonatkozású események észlelése és az azokra való reagálás

22. cikk

IKT-vonatkozású események kezelésére vonatkozó szabályzat

A rendellenes tevékenységek – többek között az IKT-hálózat teljesítményével kapcsolatos problémák és az IKT-vonatkozású események – észlelésére szolgáló mechanizmusok részeként a pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-vonatkozású eseményekre vonatkozó szabályzatot, amelyen keresztül:

a) dokumentálják az IKT-vonatkozású események (EU) 2022/2554 rendelet 17. cikkében említett kezelési folyamatát;

b) összeállítják a releváns kapcsolatoknak az IKT-műveletek biztonságában közvetlenül érintett belső funkciókat és külső érdekelt feleket tartalmazó jegyzékét, beleértve a következőket:

   i. a kiberfenyegetések észlelése és nyomon követése;

   ii. a rendellenes tevékenységek észlelése;

   iii. változásmenedzsment;

c) technikai, szervezeti és működési mechanizmusokat hoznak létre, hajtanak végre és működtetnek az IKT-vonatkozású események kezelési folyamatának támogatása érdekében, beleértve azokat a mechanizmusokat is, amelyek lehetővé teszik a rendellenes tevékenységek és magatartásformák azonnali észlelését e rendelet 23. cikkével összhangban;

d) az (EU) 2024/1772 felhatalmazáson alapuló bizottsági rendelet ([12]) 15. cikkével és az uniós jog szerinti bármely alkalmazandó megőrzési követelménnyel összhangban megőrzik az IKT-vonatkozású eseményekkel kapcsolatos valamennyi bizonyítékot az adatgyűjtés céljaihoz szükségesnél nem hosszabb ideig, az érintett üzleti funkciók, támogató folyamatok, valamint IKT-eszközök és információs vagyonelemek kritikusságával arányosan;

e) mechanizmusokat hoznak létre és hajtanak végre a jelentős vagy ismétlődő IKT-vonatkozású események, valamint az IKT-vonatkozású események számában és előfordulásában fellelhető minták elemzésére.

A d) pont alkalmazásában a pénzügyi szervezetek biztonságos módon őrzik a hivatkozott pontban említett bizonyítékokat.

23. cikk

Rendellenes tevékenységek észlelése és az IKT-vonatkozású események észlelésére és az azokra való reagálásra vonatkozó kritériumok

(1) A pénzügyi szervezetek egyértelmű szerep- és felelősségi köröket határoznak meg az IKT-vonatkozású események és rendellenes tevékenységek hatékony észlelése és az azokra való reagálás érdekében.

(2) A rendellenes tevékenységek – többek között az IKT-hálózat teljesítményével kapcsolatos problémák és az IKT-vonatkozású események – azonnali észlelésére szolgáló, az (EU) 2022/2554 rendelet 10. cikkének (1) bekezdésében említett mechanizmusnak lehetővé kell tennie a pénzügyi szervezetek számára a következőket:

a) az alábbiak mindegyikének gyűjtése, nyomon követése és elemzése:

   i. belső és külső tényezők, beleértve legalább az e rendelet 12. cikkével összhangban gyűjtött naplókat, az üzleti és IKT-funkcióktól származó információkat, valamint a pénzügyi szervezet felhasználói által jelentett problémákat;

   ii. lehetséges belső és külső kiberfenyegetések, figyelembe véve a fenyegető szereplők által általában használt forgatókönyveket és a fenyegetettséggel kapcsolatos hírszerzési tevékenység alapján lehetséges forgatókönyveket;

([12]) A Bizottság (EU) 2024/1772 felhatalmazáson alapuló rendelete (2024. március 13.) az (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek az IKT-vonatkozású események és kiberfenyegetések osztályozására vonatkozó kritériumokat, a lényegességi küszöbértékeket és a jelentős eseményekkel kapcsolatos bejelentések részleteit meghatározó szabályozástechnikai standardok tekintetében történő kiegészítéséről (HL L, 2024/1772, 2024.6.25., ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii. a pénzügyi szervezet harmadik fél IKT-szolgáltatója által küldött, a harmadik fél IKT-szolgáltató IKT-rendszereiben és hálózataiban észlelt és a pénzügyi szervezetet esetlegesen érintő IKT-vonatkozású eseményekkel kapcsolatos értesítés;

b) a rendellenes tevékenységek és magatartásformák azonosítása, és olyan eszközök alkalmazása, amelyek riasztanak a rendellenes tevékenységek és magatartásformák esetén, legalább a kritikus vagy fontos funkciókat támogató IKT-eszközök és információs vagyonelemek tekintetében;

c) a b) pontban említett riasztások előre sorolása annak érdekében, hogy az észlelt IKT-vonatkozású eseményeket munkaidőben és azon kívül is a pénzügyi szervezetek által meghatározott várható megoldási időn belül kezelni lehessen;

d) bármely releváns információ automatikus vagy kézi rögzítése, elemzése és értékelése valamennyi rendellenes tevékenységgel és magatartásformával kapcsolatban.

A b) pont alkalmazásában az abban a pontban említett eszközök magukban foglalják azokat az eszközöket, amelyek előre meghatározott szabályok alapján automatikusan riasztanak az adatforrások teljességét és integritását vagy a naplógyűjtést érintő rendellenességek azonosítása érdekében.

(3) A pénzügyi szervezetek védik a rendellenes tevékenységek használaton kívüli, továbbítás alatt álló és adott esetben használatban lévő nyilvántartását a hamisítással és a jogosulatlan hozzáféréssel szemben.

(4) A pénzügyi szervezetek valamennyi releváns információt naplóznak minden egyes észlelt anomáliára vonatkozóan, lehetővé téve a következőket:

a) a rendellenes tevékenység előfordulása napjának és időpontjának azonosítása;

b) a rendellenes tevékenység észlelése napjának és időpontjának azonosítása;

c) a rendellenes tevékenység típusának azonosítása.

(5) A pénzügyi szervezetek az IKT-vonatkozású események (EU) 2022/2554 rendelet 10. cikkének (2) bekezdésében említett észlelési és válaszfolyamatait kiváltó következő kritériumok mindegyikét figyelembe veszik:

a) arra utaló jelek, hogy rosszindulatú tevékenységet folytathattak valamely IKT-rendszerben vagy -hálózatban, vagy hogy az ilyen IKT-rendszer vagy -hálózat veszélybe kerülhetett;

b) az adatok rendelkezésre állásával, hitelességével, integritásával és bizalmas jellegével kapcsolatban észlelt adatvesztések;

c) a pénzügyi szervezet ügyleteivel és műveleteivel kapcsolatban észlelt káros hatás;

d) az IKT-rendszerek és a hálózat rendelkezésre nem állása;

(6) Az (5) bekezdés alkalmazásában a pénzügyi szervezeteknek az érintett szolgáltatások kritikusságát figyelembe kell venniük.

IV. FEJEZET

IKT-üzletmenetfolytonosság-menedzsment

24. cikk

Az IKT-üzletmenet-folytonossági politika elemei

(1) A pénzügyi szervezetek az (EU) 2022/2554 rendelet 11. cikkének (1) bekezdésében említett IKT-üzletmenet-folytonossági politikájukban feltüntetik a következők mindegyikét:

a) az alábbiak leírása:

i. az IKT-üzletmenet-folytonossági politika célkitűzései, beleértve az IKT és az általános üzletmenet-folytonosság közötti kapcsolatot, valamint figyelembe véve az (EU) 2022/2554 rendelet 11. cikkének (5) bekezdésében említett üzleti hatáselemzés (BIA) eredményeit;

ii. az IKT-üzletmenet-folytonossági intézkedések, tervek, eljárások és mechanizmusok hatóköre, beleértve a korlátozásokat és kizárásokat is;

iii. az IKT-üzletmenet-folytonossági intézkedések, tervek, eljárások és mechanizmusok által lefedett időkeret;

iv. az IKT-üzletmenet-folytonossági terveket, az IKT-reagálási és -helyreállítási terveket, valamint a válsághelyzeti kommunikációs terveket életbe léptető és deaktiváló kritériumok;

b) az alábbiakkal kapcsolatos rendelkezések:

i. az IKT-üzletmenet-folytonossági politika végrehajtásának irányítása és szervezete, beleértve a szerepköröket, a felelősségi köröket és az eszkalációs eljárásokat, biztosítva, hogy elegendő erőforrás álljon rendelkezésre;

ii. az IKT-üzletmenet-folytonossági tervek és az általános üzletmenet-folytonossági tervek összehangolása, legalább a következők mindegyike tekintetében:

1. potenciális meghibásodási forgatókönyvek, beleértve az e rendelet 26. cikkének (2) bekezdésében említett forgatókönyveket is;

2. helyreállítási célkitűzések, amelyek meghatározzák, hogy a pénzügyi szervezetnek képesnek kell lennie arra, hogy zavarokat követően a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzésen belül helyreállítsa kritikus vagy fontos funkcióinak műveleteit;

iii. az üzletmenetben okozott súlyos zavarokra vonatkozó IKT-üzletmenet-folytonossági tervek kidolgozása e tervek részeként, valamint az IKT-üzletmenet-folytonossági intézkedések kockázatalapú megközelítés alkalmazásával történő rangsorolása;

iv. IKT-reagálási és -helyreállítási tervek kidolgozása, tesztelése és felülvizsgálata e rendelet 25. és 26. cikkével összhangban;

v. a végrehajtott IKT-üzletmenet-folytonossági intézkedések, tervek, eljárások és mechanizmusok hatékonyságának felülvizsgálata e rendelet 26. cikkével összhangban;

vi. az IKT-üzletmenet-folytonossági politika összehangolása a következőkkel:

1. az (EU) 2022/2554 rendelet 14. cikkének (2) bekezdésében említett kommunikációs szabályzat;

2. az (EU) 2022/2554 rendelet 11. cikke (2) bekezdésének e) pontjában említett kommunikációs és válsághelyzeti kommunikációs intézkedések.

(2) Az (1) bekezdésben említett követelményeken túlmenően a központi szerződő felek IKT-üzletmenet-folytonossági politikájuk vonatkozásában biztosítják a következőket:

a) az a kritikus funkcióik tekintetében legfeljebb 2 óra helyreállítási időt tartalmaz;

b) figyelembe veszi a külső kapcsolatokat, valamint a pénzügyi infrastruktúrán belüli kölcsönös függéseket, ideértve azon kereskedési helyszíneket, amelyekre vonatkozóan a központi szerződő fél elszámolást végez, és a központi szerződő fél vagy valamely kapcsolódó központi szerződő fél által használt értékpapír-kiegyenlítési és -kifizetési rendszereket és hitelintézeteket;

c) előírja a következők érdekében hozott intézkedések meglétét:

i. a központi szerződő fél kritikus vagy fontos funkciói folytonosságának biztosítása vészhelyzeti forgatókönyvek alapján;

ii. az elsődleges helyszínnel megegyező olyan másodlagos adatfeldolgozási helyszín fenntartása, amely képes a központi szerződő fél kritikus vagy fontos funkcióinak folyamatosságát biztosítani;

iii. másodlagos üzleti helyszín fenntartása vagy ahhoz közvetlen hozzáférés, amely lehetővé teszi a személyzet számára a szolgáltatás folytonosságának biztosítását, amennyiben az elsődleges üzleti helyszín nem áll rendelkezésre;

iv. további adatfeldolgozási helyszínek szükségességének mérlegelése, különösen abban az esetben, ha az elsődleges és másodlagos helyszínek kockázati profiljának különbözősége nem biztosítja kellő mértékben, hogy a központi szerződő fél üzletmenet-folytonossági célkitűzései minden forgatókönyv esetén megvalósuljanak.

Az a) pont alkalmazásában a központi szerződő felek minden körülmények között az előírt időpontban és napon elvégzik a napzárási eljárásokat és a fizetéseket.

A c) pont i. alpontjának alkalmazásában az abban a pontban említett intézkedéseknek kezelniük kell a megfelelő humán erőforrás rendelkezésre állását, a kritikus funkciók maximális állásidejét, valamint a hiba miatti átkapcsolást és helyreállítást egy másodlagos helyszínen.

A c) pont ii. alpontjának alkalmazásában az abban a pontban említett másodlagos adatfeldolgozási helyszín földrajzi kockázati profilja különbözik az elsődleges helyszínétől.

(3) Az (1) bekezdésben említett követelményeken túlmenően a központi értéktárak IKT-üzletmenet-folytonossági politikájuk vonatkozásában biztosítják a következőket:

a) az figyelembe veszi a felhasználókkal, a kritikus közművekkel és a kritikus szolgáltatókkal, más központi értéktárakkal és egyéb piaci infrastruktúrákkal való kapcsolatokat és kölcsönös függőségeket;

b) megköveteli IKT-üzletmenet-folytonossági intézkedéseitől annak biztosítását, hogy a kritikus vagy fontos funkcióik helyreállítási idejére vonatkozó célkitűzés ne haladja meg a 2 órát.

(4) Az (1) bekezdésben említett követelményeken túlmenően a kereskedési helyszínek gondoskodnak arról, hogy IKT-üzletmenet-folytonossági politikájuk biztosítsa a következőket:

a) a kereskedés a rendszerzavart követően 2 órán belül vagy ahhoz közeli időtartamon belül helyreállítható;

b) a rendszerzavart követően a kereskedési helyszín informatikai szolgáltatásából esetlegesen elveszett maximális adatmennyiség a nullához közelít.

25. cikk

Az IKT-üzletmenet-folytonossági tervek tesztelése

(1) Az IKT-üzletmenet-folytonossági terveknek az (EU) 2022/2554 rendelet 11. cikkének (6) bekezdése szerinti tesztelése során a pénzügyi szervezetek figyelembe veszik a pénzügyi szervezet üzleti hatáselemzését (BIA) és az e rendelet 3. cikke (1) bekezdésének b) pontjában említett IKT-kockázatértékelést.

(2) A pénzügyi szervezetek az IKT-üzletmenet-folytonossági terveik (1) bekezdésben említett tesztelése révén értékelik, hogy képesek-e biztosítani a pénzügyi szervezet kritikus vagy fontos funkcióinak folytonosságát. Az említett tesztelésre a következők vonatkoznak:

a) azt olyan tesztforgatókönyvek alapján kell elvégezni, amelyek szimulálják a lehetséges zavarokat, beleértve a súlyos, de valószerű forgatókönyvek megfelelő csoportját;

b) adott esetben magában foglalja a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások tesztelését;

c) az (EU) 2022/2554 rendelet 11. cikke (6) bekezdésének második albekezdésében említett, mikrovállalkozásnak nem minősülő pénzügyi szervezetek esetében magában foglalja az elsődleges IKT-infrastruktúráról a tartalékkapacitásra, biztonsági mentésekre és tartalékeszközökre való átállás forgatókönyveit;

d) úgy kell kialakítani, hogy megkérdőjelezze azokat a feltételezéseket, amelyeken az üzletmenet-folytonossági tervek alapulnak, beleértve az irányítási rendszereket és a válsághelyzeti kommunikációs terveket is;

e) az eljárásokat tartalmaz annak ellenőrzésére, hogy a pénzügyi szervezetek személyzete, a harmadik fél IKT-szolgáltatók, az IKT-rendszerek és az IKT-szolgáltatások képesek-e megfelelően reagálni a 26. cikk (2) bekezdésével összhangban megfelelően figyelembe vett forgatókönyvekre.

Az a) pont alkalmazásában a pénzügyi szervezeteknek mindig bele kell foglalniuk a tesztekbe az üzletmenet-folytonossági tervek kidolgozásához figyelembe vett forgatókönyveket.

A b) pont alkalmazásában a pénzügyi szervezeteknek megfelelően figyelembe kell venniük a harmadik fél IKT-szolgáltatók fizetésképtelenségéhez vagy hiányosságaihoz, vagy adott esetben a harmadik fél IKT-szolgáltatók joghatóságában fennálló politikai kockázatokhoz kapcsolódó forgatókönyveket.

A c) pont alkalmazásában a tesztelés során ellenőrizni kell, hogy legalább a kritikus vagy fontos funkciók megfelelő módon működtethetők-e elegendő ideig, és hogy a rendes működés helyreállítható-e.

(3) A (2) bekezdésben említett követelményeken túlmenően a központi szerződő felek az (1) bekezdésben említett IKT-üzletmenet-folytonossági terveik tesztelésébe bevonják a következőket:

a) klíringtagok;

b) külső szolgáltatók;

c) a pénzügyi infrastruktúra olyan releváns intézményei, amelyekkel kapcsolatban a központi szerződő felek kölcsönös függőségeket azonosítottak az üzletmenet-folytonossági politikájukban.

(4) A (2) bekezdésben említett követelményeken túlmenően a központi értéktárak az (1) bekezdésben említett IKT-üzletmenet-folytonossági terveik tesztelésébe adott esetben bevonják a következőket:

a) a központi értéktárak felhasználói;

b) kritikus közüzemi szolgáltatók és kritikus szolgáltatók;

c) egyéb központi értéktárak;

d) más piaci infrastruktúrák;

e) bármely egyéb intézmény, amellyel kapcsolatban a központi értéktárak kölcsönös függőségeket azonosítottak az üzletmenet-folytonossági politikájukban.

(5) A pénzügyi szervezetek dokumentálják az (1) bekezdésben említett tesztelés eredményeit. A tesztelés eredményeként feltárt hiányosságokat elemzik, kezelik és jelentik a vezető testületnek.

26. cikk

IKT-reagálási és helyreállítási tervek

(1) Az (EU) 2022/2554 rendelet 11. cikkének (3) bekezdésében említett IKT-reagálási és helyreállítási tervek kidolgozása során a pénzügyi szervezetek figyelembe veszik a pénzügyi szervezet üzleti hatáselemzését (BIA). Az említett IKT-reagálási és helyreállítási tervekre a következők vonatkoznak:

a) azok meghatározzák az ezen tervek életbe léptetését vagy deaktiválását kiváltó feltételeket, valamint az ilyen életbe léptetésre vagy inaktiválásra vonatkozó kivételeket;

b) ismertetik, hogy milyen intézkedéseket kell hozni legalább a pénzügyi szervezet kritikus vagy fontos funkcióit támogató IKT-rendszerek és -szolgáltatások rendelkezésre állásának, integritásának, folytonosságának és helyreállításának biztosítása érdekében;

c) kialakításuk megfelel a pénzügyi szervezetek műveleteire vonatkozó helyreállítási célkitűzéseknek;

d) dokumentáltak és elérhetők az IKT-reagálási és -helyreállítási tervek végrehajtásában részt vevő személyzet számára, valamint vészhelyzet esetén könnyen hozzáférhetők;

e) rövid és hosszú távú helyreállítási lehetőségeket is biztosítanak, beleértve a rendszerek részleges helyreállítását is;

f) meghatározzák az IKT-reagálási és -helyreállítási tervek célkitűzéseit, valamint azokat a feltételeket, amelyek esetén kijelenthető, hogy a tervek végrehajtása sikeres volt.

A d) pont alkalmazásában a pénzügyi szervezetek egyértelműen meghatározzák a szerep- és felelősségi köröket.

(2) Az (1) bekezdésben említett IKT-reagálási és -helyreállítási tervekben azonosítani kell a releváns forgatókönyveket, beleértve az üzletmenetben okozott súlyos zavarokkal és a zavarok bekövetkezésének fokozott valószínűségével járó forgatókönyveket. E terveknek a fenyegetésekre vonatkozó aktuális információk és az üzletmenetben okozott zavarok korábbi előfordulásaiból levont tanulságok alapján kell forgatókönyveket kidolgozniuk. A pénzügyi szervezetek megfelelően figyelembe veszik a következő forgatókönyvek mindegyikét:

a) kibertámadások, valamint az elsődleges IKT-infrastruktúra és a tartalékkapacitás, biztonsági mentések és tartalékeszközök közötti átállások;

b) olyan forgatókönyvek, amelyek szerint valamely kritikus vagy fontos funkció ellátása elfogadhatatlan színvonalúra csökken vagy meghiúsul, és amely kellőképpen tekintetbe veszi bármely releváns harmadik fél IKT-szolgáltató fizetésképtelenségének vagy egyéb hiányosságainak potenciális hatásait;

c) a telephelyek – beleértve az irodákat és az üzlethelyiségeket is – és az adatközpontok részleges vagy teljes meghibásodása;

d) az IKT-eszközök vagy a kommunikációs infrastruktúra jelentős meghibásodása;

e) a személyzet hiánya kritikus létszámban, vagy a működés folytonosságának biztosításáért felelős személyzet hiánya;

f) az éghajlatváltozással és a környezetkárosodással kapcsolatos események, természeti katasztrófák, világjárványok és fizikai támadások, többek között behatolások és terrortámadások hatása;

g) bennfentes támadások;

h) politikai és társadalmi instabilitás, többek között adott esetben a harmadik fél IKT-szolgáltató joghatóságában és az adatok tárolásának és feldolgozásának helyszínén;

i) széles körű feszültség-kimaradások.

(3) Az (1) bekezdésben említett IKT-reagálási és -helyreállítási terveknek alternatív lehetőségeket kell mérlegelniük azokra az esetekre, amikor az elsődleges helyreállítási intézkedések a költségek, a kockázatok, a logisztika vagy előre nem látható körülmények miatt rövid távon nem kivitelezhetők.

(4) Az (1) bekezdésben említett IKT-reagálási és -helyreállítási tervek részeként a pénzügyi szervezetek mérlegelik és végrehajtják a pénzügyi szervezet kritikus vagy fontos funkcióit támogató harmadik fél IKT-szolgáltatók hiányosságainak enyhítésére irányuló folytonossági intézkedéseket.

V. FEJEZET

Az IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés

27. cikk

Az IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés formátuma és tartalma

(1) A pénzügyi szervezetek kereshető elektronikus formátumban nyújtják be az (EU) 2022/2554 rendelet 6. cikkének (5) bekezdésében említett jelentést az IKT-kockázatkezelési keretrendszer felülvizsgálatáról.

(2) A pénzügyi szervezetek a következő információk mindegyikét feltüntetik az (1) bekezdésben említett jelentésben:

a) bevezető rész, amelynek szerepe a következő:

   i. a jelentés tárgyát képező pénzügyi szervezet egyértelmű azonosítása, és adott esetben a csoportfelépítésének ismertetése;

   ii. a jelentés hátterének leírása a pénzügyi szervezet szolgáltatásainak, tevékenységeinek és műveleteinek jellege, nagyságrendje és összetettsége, valamint szervezete, azonosított kritikus funkciói, stratégiája, folyamatban lévő főbb projektjei és tevékenységei, kapcsolatai és a házon belüli és megbízásba adott IKT-szolgáltatásoktól és -rendszerektől való függősége, illetve az ilyen rendszerek teljes elvesztése vagy súlyos romlása által a kritikus vagy fontos funkciókra és a piaci hatékonyságra gyakorolt hatások tekintetében;

   iii. az IKT-kockázatkezelési keretrendszerben az előző jelentés benyújtása óta bekövetkezett jelentős változások összefoglalása;

   iv. átfogó összefoglaló biztosítása a jelenlegi és rövid távú IKT-kockázati profilról, a fenyegetettségi helyzetről, a kontrollok értékelt hatékonyságáról és a pénzügyi szervezet kiberbiztonsági helyzetéről;

b) a jelentés pénzügyi szervezet vezető testülete általi jóváhagyásának időpontja;

c) az IKT-kockázatkezelési keretrendszer (EU) 2022/2554 rendelet 6. cikkének (5) bekezdése szerinti felülvizsgálata okának ismertetése;

d) a felülvizsgálati időszak kezdő és záró időpontja;

e) a felülvizsgálatért felelős funkció megjelölése;

f) az IKT-kockázatkezelési keretrendszerben az előző felülvizsgálat óta bekövetkezett jelentős változások és fejlesztések leírása;

g) a felülvizsgálat megállapításainak összefoglalása, valamint az IKT-kockázatkezelési keretrendszerben a felülvizsgálati időszak alatt talált gyengeségek, hiányosságok és lefedetlenségek súlyosságának részletes elemzése és értékelése;

h) az azonosított gyengeségek, hiányosságok és lefedetlenségek kezelésére irányuló intézkedések leírása, beleértve a következők mindegyikét:

   i. a feltárt gyengeségek, hiányosságok és lefedetlenségek orvoslása érdekében hozott intézkedések összefoglalása;

   ii. az intézkedések végrehajtásának várható időpontja és a végrehajtás belső kontrolljával kapcsolatos időpontok, beleértve az ezen intézkedések végrehajtásának előrehaladására vonatkozó információkat a jelentés elkészítésének időpontjában, adott esetben kifejtve, hogy fennáll-e a határidők be nem tartásának kockázata;

   iii. az alkalmazandó eszközök és az intézkedések végrehajtásáért felelős funkció azonosítása, részletezve, hogy belső vagy külső eszközökről és funkciókról van-e szó;

   iv. annak leírása, hogy az intézkedésekben tervezett változások milyen hatást gyakorolnak a pénzügyi szervezet költségvetési, humán és anyagi erőforrásaira, beleértve a korrekciós intézkedések végrehajtására szánt forrásokat is;

   v. adott esetben az illetékes hatóság tájékoztatásának folyamatára vonatkozó információk;

   vi. amennyiben a feltárt gyengeségekre, hiányosságokra és lefedetlenségekre nem vonatkoznak korrekciós intézkedések, az ezen gyengeségek, hiányosságok és lefedetlenségek hatásának elemzéséhez, a kapcsolódó fennmaradó IKT-kockázat értékeléséhez, valamint a kapcsolódó fennmaradó kockázat elfogadásához használt kritériumok részletes magyarázata;

i) információk az IKT-kockázatkezelési keretrendszer tervezett további fejlesztéseiről;

j) az IKT-kockázatkezelési keretrendszer felülvizsgálatának eredményeként leszűrt következtetések;

k) a múltbeli felülvizsgálatokra vonatkozó információk, beleértve a következőket:

   i. az eddigi felülvizsgálatok jegyzéke;

   ii. adott esetben az utolsó jelentésben meghatározott korrekciós intézkedések végrehajtásának állapota;

   iii. amennyiben a korábbi felülvizsgálatok során javasolt korrekciós intézkedések eredménytelennek bizonyultak vagy váratlan kihívásokat teremtettek, annak ismertetése, hogy miként lehetne javítani ezeket a korrekciós intézkedéseket, illetve e váratlan kihívások bemutatása;

l) a jelentés elkészítéséhez felhasznált információforrások, beleértve a következők mindegyikét:

   i. az (EU) 2022/2554 rendelet 6. cikkének (6) bekezdésében említett, mikrovállalkozásnak nem minősülő pénzügyi szervezetek esetében a belső ellenőrzések eredményei;

   ii. a megfelelőség értékeléseinek eredményei;

   iii. a digitális működési reziliencia tesztelésének eredményei, és adott esetben az IKT-eszközök, -rendszerek és -folyamatok fenyegetés alapú behatolási tesztelésére (TLPT) épülő fejlett tesztelésének eredményei;

   iv. külső források.

A c) pont alkalmazásában, amennyiben a felülvizsgálatot felügyeleti utasítások, illetve a releváns digitális működési reziliencia teszteléséből vagy ellenőrzési folyamataiból levont következtetések alapján kezdeményezték, a jelentésnek kifejezett hivatkozásokat kell tartalmaznia az ilyen utasításokra vagy következtetésekre, lehetővé téve a felülvizsgálat kezdeményezése okának azonosítását. Amennyiben a felülvizsgálatot IKT-vonatkozású eseményeket követően kezdeményezték, a jelentésnek tartalmaznia kell az összes IKT-vonatkozású esemény jegyzékét, az események okának elemzését is beleértve.

Az f) pont alkalmazásában a leírásnak tartalmaznia kell a változások által a pénzügyi szervezet digitális működési rezilienciára vonatkozó stratégiájára, belső IKT-ellenőrzési rendszerére és IKT-kockázatkezelési irányítására gyakorolt hatás elemzését.

III. CÍM

AZ (EU) 2022/2554 RENDELET 16. CIKKÉNEK (1) BEKEZDÉSÉBEN EMLÍTETT PÉNZÜGYI SZERVEZETEKRE VONATKOZÓ EGYSZERŰSÍTETT IKT-KOCKÁZATKEZELÉSI KERETRENDSZER

I. FEJEZET

Egyszerűsített IKT-kockázatkezelési keretrendszer

28. cikk

Irányítás és szervezet

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezeteknek olyan belső irányítási és ellenőrzési keretrendszerrel kell rendelkezniük, amely biztosítja az IKT-kockázat hatékony és prudens kezelését a digitális működési reziliencia magas szintjének elérése érdekében.

(2) Az (1) bekezdésben említett pénzügyi szervezetek egyszerűsített IKT-kockázatkezelési keretrendszerük részeként biztosítják, hogy vezető testületük:

a) viselje az általános felelősséget annak biztosításáért, hogy az egyszerűsített IKT-kockázatkezelési keretrendszer lehetővé tegye a pénzügyi szervezet üzleti stratégiájának megvalósítását az adott pénzügyi szervezet kockázatvállalási hajlandóságával összhangban, és biztosítsa, hogy az IKT-kockázatot ebben az összefüggésben figyelembe vegyék;

b) egyértelmű szerep- és felelősségi köröket jelöljön ki minden IKT-vonatkozású feladattal összefüggésben;

c) meghatározza az információbiztonsági célkitűzéseket és az IKT-követelményeket;

d) jóváhagyja, felügyelje és rendszeres időközönként felülvizsgálja a következőket:

   i. a pénzügyi szervezet információs vagyonelemeinek e rendelet 30. cikkének (1) bekezdésében említett osztályozása, az azonosított fő kockázatok jegyzéke, valamint az üzleti hatáselemzés és a kapcsolódó politikák;

   ii. a pénzügyi szervezet üzletmenet-folytonossági tervei, valamint az (EU) 2022/2554 rendelet 16. cikke (1) bekezdésének f) pontjában említett reagálási és helyreállítási intézkedések;

e) 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-készségeket;

f) meghatározza és végrehajtja az e cím I., II. és III. fejezetében foglalt szabályzatokat és intézkedéseket a pénzügyi szervezetet érintő IKT-kockázat azonosítása, értékelése és kezelése érdekében;

g) azonosítja és végrehajtja az információs vagyonelemek és IKT-eszközök védelméhez szükséges eljárásokat, IKT-protokollokat és eszközöket;

h) biztosítja, hogy a pénzügyi szervezet személyzete megfelelő ismeretekkel és készségekkel rendelkezzen ahhoz, hogy megértse és értékelje az IKT-kockázatot és annak a pénzügyi szervezet működésére gyakorolt hatását, a kezelt IKT-kockázattal arányos mértékben;

i) megállapítja a jelentéstételi intézkedéseket, beleértve a vezető testületnek benyújtott, az információbiztonsággal és a digitális működési rezilienciával kapcsolatos jelentések gyakoriságát, formáját és tartalmát.

(3) Az (1) bekezdésben említett pénzügyi szervezetek az uniós és a nemzeti ágazati jogszabályokkal összhangban kiszervezhetik az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzésével kapcsolatos feladatokat csoporton belüli IKT-szolgáltatóknak vagy harmadik fél IKT-szolgáltatóknak. Ilyen kiszervezés esetén a pénzügyi szervezetek továbbra is teljes felelősséggel tartoznak az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzéséért.

(4) Az (1) bekezdésben említett pénzügyi szervezetek biztosítják a kontrollfunkciók és a belső ellenőrzési funkciók megfelelő elkülönítését és függetlenségét.

(5) Az (1) bekezdésben említett pénzügyi szervezetek biztosítják, hogy egyszerűsített IKT-kockázatkezelési keretrendszerüket ellenőrzési terveikkel összhangban ellenőrök által végzett belső ellenőrzésnek vessék alá. Az ellenőröknek elegendő ismerettel, készségekkel és szakértelemmel kell rendelkezniük az IKT-kockázat terén, és függetlennek kell lenniük. Az IKT-ellenőrzések gyakoriságának és fókuszának igazodnia kell a pénzügyi szervezet IKT-kockázatához.

(6) Az (5) bekezdésben említett ellenőrzés eredménye alapján az (1) bekezdésben említett pénzügyi szervezetek biztosítják az IKT-ellenőrzés kritikus megállapításainak időben történő ellenőrzését és orvoslását.

29. cikk

Információbiztonsági szabályzat és intézkedések

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek az egyszerűsített IKT-kockázatkezelési keretrendszerrel összefüggésben kidolgozzák, dokumentálják és végrehajtják 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.

(2) Az (1) bekezdésben említett pénzügyi szervezetek az (1) bekezdésben említett információbiztonsági szabályzatuk alapján IKT-biztonsági intézkedéseket hoznak és hajtanak végre az IKT-kockázatnak való kitettségük csökkentése érdekében, beleértve a harmadik fél IKT-szolgáltatók által végrehajtott kockázatcsökkentő intézkedéseket is.

Az IKT-biztonsági intézkedéseknek magukban kell foglalniuk a 30–38. cikkben említett valamennyi intézkedést.

30. cikk

Az információs vagyonelemek és IKT-eszközök osztályozása

(1) Az (EU) 2022/2554 rendelet 16. cikke (1) bekezdésének a) pontjában említett egyszerűsített IKT-kockázatkezelési keretrendszer részeként a hivatkozott cikk (1) bekezdésében említett pénzügyi szervezetek azonosítják, osztályozzák és dokumentálják valamennyi kritikus vagy fontos funkciót, az azokat támogató információs vagyonelemeket és IKT-eszközöket, valamint azok kölcsönös függőségeit. A pénzügyi szervezetek szükség szerint felülvizsgálják ezt az azonosítást és osztályozást.

(2) Az (1) bekezdésben említett pénzügyi szervezetek azonosítják a harmadik fél IKT-szolgáltatók által támogatott valamennyi kritikus vagy fontos funkciót.

31. cikk

IKT-kockázatkezelés

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek egyszerűsített IKT-kockázatkezelési keretrendszerükbe belefoglalják a következőket mindegyikét:

a) az IKT-kockázatra vonatkozó kockázati toleranciaszintek meghatározása a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban;

b) azon IKT-kockázatok azonosítása és értékelése, amelyeknek a pénzügyi szervezet ki van téve;

c) kockázatcsökkentési stratégiák meghatározása legalább azokra az IKT-kockázatokra vonatkozóan, amelyek nem a pénzügyi szervezet kockázati toleranciaszintjein belül vannak;

d) a c) pontban említett kockázatcsökkentési stratégiák hatékonyságának nyomon követése;

e) 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.

(2) Az (1) bekezdésben említett pénzügyi szervezetek az IKT-kockázati profiljukkal arányosan időközönként elvégzik és dokumentálják az IKT-kockázatértékelést.

(3) Az (1) bekezdésben említett pénzügyi szervezetek folyamatosan nyomon követik a kritikus vagy fontos funkcióik, valamint információs vagyonelemeik és IKT-eszközeik szempontjából releváns fenyegetéseket és sérülékenységeket, és rendszeresen felülvizsgálják az e kritikus vagy fontos funkciókat érintő kockázati forgatókönyveket.

(4) Az (1) bekezdésben említett pénzügyi szervezetek az IKT-vonatkozású események válaszfolyamatait kiváltó és elindító riasztási értékhatárokat és kritériumokat határoznak meg.

32. cikk

Fizikai és környezetbiztonság

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek meghatározzák és végrehajtják a fenyegetettségi helyzet alapján, valamint az e rendelet 30. cikkének (1) bekezdésében említett osztályozással, az IKT-eszközök általános kockázati profiljával és a hozzáférhető információs vagyonelemekkel összhangban kidolgozott fizikai biztonsági intézkedéseket.

(2) Az (1) bekezdésben említett intézkedéseknek védeniük kell a pénzügyi szervezetek IKT-eszközöknek és információs vagyonelemeknek helyet adó telephelyeit és adott esetben adatközpontjait az illetéktelen hozzáféréssel, támadásokkal és balesetekkel, valamint a környezeti fenyegetésekkel és veszélyekkel szemben.

(3) A környezeti fenyegetésekkel és veszélyekkel szembeni védelemnek arányban kell állnia az érintett telephelyek és adott esetben adatközpontok fontosságával, valamint az ott végzett műveletek vagy ott található IKT-rendszerek kritikusságával.

II. FEJEZET

Az IKT-kockázat hatásának minimalizálását célzó rendszerek, protokollok és eszközök további elemei

33. cikk

Hozzáférés-ellenőrzés

Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják a logikai és fizikai hozzáférés ellenőrzésére szolgáló eljárásokat, valamint érvényre juttatják, nyomon követik és rendszeresen felülvizsgálják ezeket az eljárásokat. Ezek az eljárások a logikai és fizikai hozzáférés ellenőrzésének következő elemeit tartalmazzák:

a) az információs vagyonelemekhez, az IKT-eszközökhöz és azok támogatott funkcióihoz, valamint a pénzügyi szervezet kritikus működési helyszíneihez való hozzáférési jogosultságok kezelése a szükséges ismeret elve, a szükséges használat elve és a legkisebb jogosultság elve alapján, beleértve a távoli és vészhelyzeti hozzáférést is;

b) felhasználói elszámoltathatóság, ami biztosítja, hogy a felhasználók azonosíthatók az IKT-rendszerekben végzett tevékenységek tekintetében;

c) a felhasználói és általános fiókokhoz, köztük az általános rendszergazdai fiókokhoz való hozzáférési jogosultságok megadására, módosítására vagy visszavonására vonatkozó fiókkezelési eljárások;

d) a 30. cikk (1) bekezdésében említett osztályozással és az IKT-eszközök általános kockázati profiljával arányos hitelesítési módszerek, amelyek vezető gyakorlatokon alapulnak;

e) a hozzáférési jogosultságok rendszeres felülvizsgálata és visszavonása, ha már nincs szükség rájuk.

A c) pont alkalmazásában a pénzügyi szervezet valamennyi IKT-rendszer esetében a szükséges használat elve alapján vagy eseti alapon osztja ki a kiemelt, vészhelyzeti és rendszergazdai hozzáférést, és azt a 34. cikk első albekezdésének f) pontjával összhangban naplózza.

A d) pont alkalmazásában a pénzügyi szervezetek vezető gyakorlatokon alapuló, erős hitelesítési módszereket alkalmaznak a pénzügyi szervezetek hálózatához való távoli hozzáféréshez, a kiemelt hozzáféréshez, valamint a kritikus vagy fontos funkciókat támogató, nyilvánosan elérhető IKT-eszközökhöz való hozzáféréshez.

34. cikk

Az IKT-műveletek biztonsága

Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek a következőket teszik rendszereik, protokolljaik és eszközeik részeként, valamint valamennyi IKT-eszköz tekintetében:

a) valamennyi IKT-eszköz életciklusának nyomon követése és kezelése;

b) adott esetben annak nyomon követése, hogy az IKT-eszközöket a pénzügyi szervezetek harmadik fél IKT-szolgáltatói támogatják-e;

c) IKT-eszközeik kapacitásigényeinek azonosítása, és intézkedések meghozatala az IKT-rendszerek rendelkezésre állásának és hatékonyságának fenntartása és javítása, valamint az IKT-kapacitáshiányoknak azok bekövetkezése előtti megelőzése érdekében;

d) az IKT-eszközök automatizált sérülékenységfelmérése és -értékelése a 30. cikk (1) bekezdésében említett osztályozásukkal és az IKT-eszköz általános kockázati profiljával arányos módon, és javítások telepítése az azonosított sérülékenységek kezelésére;

e) az idejétmúlt, nem támogatott vagy elavult IKT-eszközökhöz kapcsolódó kockázatok kezelése;

f) a logikai és fizikai hozzáférés-ellenőrzéssel, IKT-műveletekkel – beleértve a rendszer- és hálózati forgalmi tevékenységeket – és az IKT-változásmenedzsmenttel kapcsolatos események naplózása;

g) a kritikus vagy fontos IKT-műveletekkel kapcsolatos rendellenes tevékenységekre és magatartásformákra vonatkozó információk nyomon követésére és elemzésére irányuló intézkedések meghatározása és végrehajtása;

h) a kiberfenyegetésekre vonatkozó releváns és naprakész információk nyomon követésére irányuló intézkedések végrehajtása;

i) a lehetséges információszivárgások, rosszindulatú kódok és egyéb biztonsági fenyegetések, valamint a szoftverek és hardverek közismert sérülékenységeinek azonosítására, és a megfelelő új biztonsági frissítések ellenőrzésére irányuló intézkedések végrehajtása.

Az f) pont alkalmazásában a pénzügyi szervezetek összehangolják a naplók részletességi szintjét azok céljával és a naplókat előállító IKT-eszköz használatával.

35. cikk

Adat-, rendszer- és hálózatbiztonság

Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek rendszereik, protokolljaik és eszközeik részeként olyan biztosítékokat dolgoznak ki és hajtanak végre, amelyek garantálják a hálózatok biztonságát a behatolásokkal és az adatokkal való visszaéléssel szemben, és amelyek megőrzik az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét. A pénzügyi szervezetek – figyelembe véve az e rendelet 30. cikkének (1) bekezdésében említett osztályozást – meghatározzák különösen a következők mindegyikét:

a) a használatban lévő, továbbítás alatt álló és használaton kívüli adatok védelmét szolgáló intézkedések azonosítása és végrehajtása;

b) biztonsági intézkedések azonosítása és végrehajtása a pénzügyi szervezet adatait továbbító és tároló szoftverek, adattárolók, adathordozók, rendszerek és végponti eszközök tekintetében;

c) a pénzügyi szervezet hálózatához való jogosulatlan csatlakozások megelőzésére és észlelésére, valamint a pénzügyi szervezet belső hálózatai és az internet és más külső kapcsolatok közötti hálózati forgalom biztosítására irányuló intézkedések azonosítása és végrehajtása;

d) az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét a hálózati továbbítás során biztosító intézkedések azonosítása és végrehajtása;

e) a telephelyeken található vagy külső helyszínen tárolt olyan adatok biztonságos törlésének folyamata, amelyeket a pénzügyi szervezetnek már nem kell gyűjtenie vagy tárolnia;

f) a telephelyeken található vagy külső helyszínen tárolt, bizalmas információkat tartalmazó adattároló eszközök biztonságos ártalmatlanításának vagy leszerelésének folyamata;

g) olyan intézkedések azonosítása és végrehajtása, amelyek biztosítják, hogy a távmunka és a magánjellegű végponti eszközök használata ne befolyásolja hátrányosan a pénzügyi szervezet azon képességét, hogy kritikus tevékenységeit megfelelően, időben és biztonságosan végezze.

36. cikk

IKT-biztonsági tesztelés

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek IKT-biztonsági tesztelési tervet dolgoznak ki és hajtanak végre az e rendelet 33., 34. és 35. cikkével, valamint 37. és 38. cikkével összhangban kidolgozott IKT-biztonsági intézkedéseik hatékonyságának validálása céljából. A pénzügyi szervezetek biztosítják, hogy a terv figyelembe vegye az e rendelet 31. cikkében említett egyszerűsített IKT-kockázatkezelési keretrendszer részeként azonosított fenyegetéseket és sérülékenységeket.

(2) Az (1) bekezdésben említett pénzügyi szervezetek felülvizsgálják, értékelik és tesztelik az IKT-biztonsági intézkedéseket, figyelembe véve a pénzügyi szervezet IKT-eszközeinek általános kockázati profilját.

(3) Az (1) bekezdésben említett pénzügyi szervezetek a kritikus vagy fontos funkciókat támogató IKT-rendszerek esetében nyomon követik és értékelik a biztonsági tesztek eredményeit, és annak megfelelően indokolatlan késedelem nélkül frissítik biztonsági intézkedéseiket.

37. cikk

IKT-rendszerek beszerzése, fejlesztése és karbantartása

Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek adott esetben kockázatalapú megközelítést követve kidolgozzák és végrehajtják az IKT-rendszerek beszerzését, fejlesztését és karbantartását szabályozó eljárást. Az eljárás szerepe a következő:

a) annak biztosítása, hogy az IKT-rendszerek beszerzése és fejlesztése előtt az érintett üzleti funkció egyértelműen meghatározza és jóváhagyja a funkcionális és nem funkcionális követelményeket, beleértve az információbiztonsági követelményeket is;

b) az IKT-rendszerek tesztelésének és jóváhagyásának biztosítása azok első használata előtt, valamint a változtatásoknak az éles környezetben történő bevezetése előtt;

c) olyan intézkedések azonosítása, amelyek csökkentik az IKT-rendszerek nem szándékos megváltoztatásának vagy szándékos manipulálásának kockázatát az éles környezetben történő fejlesztés és végrehajtás alatt.

38. cikk

IKT-projektmenedzsment és -változásmenedzsment

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-projektmenedzsmentre vonatkozó eljárást, és meghatározzák a végrehajtásához szükséges szerep- és felelősségi köröket. Ez az eljárás az IKT-projektek valamennyi szakaszára kiterjed, azok kezdeményezésétől a lezárásukig.

(2) Az (1) bekezdésben említett pénzügyi szervezetek kidolgozzák, dokumentálják és végrehajtják az IKT-változásmenedzsmentre vonatkozó eljárást annak biztosítása érdekében, hogy az IKT-rendszerek minden módosítását ellenőrzött módon és a pénzügyi szervezet digitális működési rezilienciájának megőrzése érdekében megfelelő biztosítékok mellett rögzítsék, teszteljék, értékeljék, hagyják jóvá, hajtsák végre és ellenőrizzék.

III. FEJEZET

IKT-üzletmenetfolytonosság-menedzsment

39. cikk

Az IKT-üzletmenet-folytonossági terv elemei

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek kidolgozzák IKT-üzletmenet-folytonossági terveiket, figyelembe véve az üzletmenetben okozott súlyos zavaroknak való kitettségükre 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.

(2) Az (1) bekezdésben említett üzletmenet-folytonossági tervekre a következők vonatkoznak:

a) azokat a pénzügyi szervezet vezető testületének kell jóváhagynia;

b) dokumentáltak és közvetlenül hozzáférhetők vészhelyzet vagy válság esetén;

c) elegendő forrást különítenek el a végrehajtásukhoz;

d) meghatározzák a tervezett helyreállítási szinteket és időkereteket a funkciók és a kulcsfontosságú belső és külső függőségek helyreállításához és újraindításához, beleértve a harmadik fél IKT-szolgáltatókat is;

e) meghatározzák azokat a feltételeket, amelyek kiválthatják az IKT-üzletmenet-folytonossági tervek aktiválását, és azokat az intézkedéseket, amelyeket meg kell hozni a pénzügyi szervezetek kritikus vagy fontos funkciókat támogató IKT-eszközeinek rendelkezésre állásának, folytonosságának és helyreállításának biztosítása érdekében;

f) a pénzügyi szervezetek működésére gyakorolt káros hatások elkerülése érdekében azonosítják a kritikus vagy fontos üzleti funkciókra, a támogató folyamatokra, az információs vagyonelemekre és azok kölcsönös függőségeire vonatkozó visszaállítási és helyreállítási intézkedéseket;

g) azonosítják 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;

h) mérlegelik az alternatív lehetőségeket azokra az esetekre, amikor a helyreállítás nem kivitelezhető rövid távon a költségek, a kockázatok, a logisztika vagy előre nem látható körülmények miatt;

i) meghatározzák a belső és külső kommunikációs intézkedéseket, többek között az eszkalációs terveket;

j) azokat az eseményekből levont tanulságokkal, a tesztekkel, az új kockázatokkal és az azonosított fenyegetésekkel, a megváltozott helyreállítási célkitűzésekkel, a pénzügyi szervezet szervezetében, valamint a kritikus vagy üzleti funkciókat támogató IKT-eszközökben bekövetkező jelentős változásokkal összhangban aktualizálják.

Az f) pont alkalmazásában az abban a pontban említett intézkedéseknek rendelkezniük kell a kritikus harmadik fél szolgáltatók hiányosságainak mérsékléséről.

40. cikk

Az üzletmenet-folytonossági tervek tesztelése

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek a biztonsági mentési és helyreállítási eljárások esetében legalább évente egyszer, illetve az üzletmenet-folytonossági terv minden jelentős változásakor tesztelik az e rendelet 39. cikkében említett üzletmenet-folytonossági terveiket, beleértve a hivatkozott cikkben említett forgatókönyveket is.

(2) Az üzletmenet-folytonossági tervek (1) bekezdésben említett tesztelése során bizonyítani kell, hogy a hivatkozott bekezdésben említett pénzügyi szervezetek képesek fenntartani üzleti tevékenységük életképességét a kritikus fontosságú műveletek helyreállításáig, és a tesztelésnek azonosítania kell e tervek esetleges hiányosságait.

(3) Az (1) bekezdésben említett pénzügyi szervezetek dokumentálják az üzletmenet-folytonossági tervek tesztelésének eredményeit, és a tesztelés eredményeként feltárt hiányosságokat elemzik, kezelik és jelentik a vezető testületnek.

IV. FEJEZET

Az egyszerűsített IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés

41. cikk

Az egyszerűsített IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés formátuma és tartalma

(1) Az (EU) 2022/2554 rendelet 16. cikkének (1) bekezdésében említett pénzügyi szervezetek kereshető elektronikus formátumban nyújtják be a hivatkozott cikk (2) bekezdésében említett jelentést az IKT-kockázatkezelési keretrendszer felülvizsgálatáról.

(2) Az (1) bekezdésben említett jelentésnek az alábbi információk mindegyikét tartalmaznia kell:

a) bevezető rész, amelyben szerepelnek a következők:

   i. a jelentés hátterének leírása a pénzügyi szervezet szolgáltatásainak, tevékenységeinek és műveleteinek jellege, nagyságrendje és összetettsége, a pénzügyi szervezet szervezete, azonosított kritikus funkciói, stratégiája, folyamatban lévő főbb projektjei vagy tevékenységei és kapcsolatai, a pénzügyi szervezet házon belüli és kiszervezett IKT-szolgáltatásoktól és -rendszerektől való függősége, illetve az ilyen rendszerek teljes elvesztése vagy súlyos romlása által a kritikus vagy fontos funkciókra és a piaci hatékonyságra gyakorolt hatások tekintetében;

   ii. átfogó összefoglaló az azonosított jelenlegi és rövid távú IKT-kockázatról, a fenyegetettségi helyzetről, a kontrollok értékelt hatékonyságáról és a pénzügyi szervezet kiberbiztonsági helyzetéről;

   iii. a jelentés tárgyát képező területre vonatkozó információk;

   iv. az IKT-kockázatkezelési keretrendszerben az előző jelentés óta bekövetkezett jelentős változások összefoglalása;

   v. az előző jelentés óta bekövetkezett jelentős változások egyszerűsített IKT-kockázatkezelési keretrendszerre gyakorolt hatásának összefoglalása és leírása;

b) adott esetben a jelentés pénzügyi szervezet vezető testülete általi jóváhagyásának időpontja;

c) a felülvizsgálat okainak ismertetése, beleértve a következőket:

   i. amennyiben a felülvizsgálatot felügyeleti utasítások alapján kezdeményezték, az utasítások bizonyítéka;

   ii. amennyiben a felülvizsgálatot IKT-vonatkozású események előfordulását követően kezdeményezték, az összes IKT-vonatkozású esemény jegyzéke, az események okának elemzését is beleértve;

d) a felülvizsgálati időszak kezdő és záró időpontja;

e) a felülvizsgálatért felelős személy;

f) a felülvizsgálat megállapításainak összefoglalása, valamint az IKT-kockázatkezelési keretrendszerben a felülvizsgálati időszak tekintetében talált gyengeségek, hiányosságok és lefedetlenségek súlyosságának önértékelése, beleértve azok részletes elemzését is;

g) az egyszerűsített IKT-kockázatkezelési keretrendszer gyengeségeinek, hiányosságainak és lefedetlenségeinek kezelése érdekében azonosított korrekciós intézkedések, valamint ezen intézkedések végrehajtásának várható időpontja, beleértve a korábbi jelentésekben azonosított gyengeségek, hiányosságok és lefedetlenségek nyomon követését, amennyiben ezeket a gyengeségeket, hiányosságokat és lefedetlenségeket még nem orvosolták;

h) általános következtetések az egyszerűsített IKT-kockázatkezelési keretrendszer felülvizsgálatáról, beleértve a további tervezett fejlesztéseket is.

IV. CÍM

ZÁRÓ RENDELKEZÉSEK

42. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2024. március 13-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN