I

(Jogalkotási aktusok)

RENDELETEK

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

(2022. december 14.)

a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Központi Bank véleményére ([1]),

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([2]),

rendes jogalkotási eljárás keretében ([3]),

mivel:

(1) A digitális korban a mindennapos tevékenységek során alkalmazott összetett rendszereket információs és kommunikációs technológia (IKT) támogatja. Ez biztosítja a gazdaság folyamatos működését az ágazatokban, többek között a pénzügyi ágazatban, és javítja a belső piac működését is. A megnövekedett digitalizáció és az összekapcsoltság felerősíti az IKT-kockázatot is, kiszolgáltatottabbá téve a társadalom egészét és különösen a pénzügyi rendszert, a kiberfenyegetésekkel és az IKT-zavarokkal szemben. Míg az IKT-rendszerek általános alkalmazása, valamint a nagy fokú digitalizáció és összekapcsoltság ma az uniós pénzügyi szervezetek tevékenységeire alapvetően jellemző, a digitális rezilienciájukkal többet kell még foglalkozni, és azt jobban kell integrálni a tágabb működési kereteikbe.

(2) Az IKT használata az elmúlt évtizedekben lényeges szerepet nyert a pénzügyi szolgáltatások nyújtása terén, egészen addig a pontig, hogy mára kritikus fontosságra tett szert a valamennyi pénzügyi szervezet által ellátott tipikus mindennapos funkciók működésében. A digitalizáció mostanra kiterjed például a fizetésekre amelyek a készpénz- és papíralapú módszerektől mind inkább a digitális megoldások alkalmazása felé mozdultak el , valamint az értékpapírok elszámolására és kiegyenlítésére, az elektronikus és algoritmikus kereskedésre, a hitelnyújtási és finanszírozási műveletekre, a személyközi finanszírozásra, a hitelminősítésekre, a követeléskezelésre és a háttértevé-

([1]) HL C 343., 2021.8.26., 1. o.
([2]) HL C 155., 2021.4.30., 38. o.
([3]) Az Európai Parlament 2022. november 10-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2022. november 28-i határozata.

kenységekre. Az IKT-technológia használata a biztosítási ágazatot is átalakította, az InsturTech-hel működő, szolgáltatásaikat online kínáló biztosításközvetítők megjelenésétől kezdve a digitális biztosítási kockázatvállalásig. Amellett, hogy a pénzügyi szolgáltatások az ágazat egészében nagyrészt digitálissá váltak, a digitalizáció fokozottabb összekapcsoltságot és kölcsönös függést is eredményezett a pénzügyi ágazaton belül, valamint a harmadik felektől igénybe vett infrastruktúrák és szolgáltatások terén.

(3) Az Európai Rendszerkockázati Testület (ERKT) a rendszerszintű kiberkockázattal foglalkozó 2020. évi jelentésében megerősítette, hogy a pénzügyi szervezetek, a pénzügyi piacok és a pénzügyi piaci infrastruktúrák meglévő nagy fokú összekapcsoltsága és különösen az IKT-rendszereik kölcsönös függései miképpen jelenthetnek rendszerszintű sérülékenységet amiatt, hogy a lokalizált kiberbiztonsági események a mintegy 22 000 uniós pénzügyi szervezet bármelyikéről gyorsan, földrajzi határoktól függetlenül átterjedhetnek a teljes pénzügyi rendszerre. Súlyos IKT-biztonsági sérülések, amelyek előfordulnak a pénzügyi ágazatban, nem csak elszigetelt pénzügyi szervezeteket érintenek. Lehetővé teszik a lokalizált sérülékenységek pénzügyi transzmissziós csatornákon keresztüli zavartalan terjedését is, és potenciálisan kedvezőtlen következményekkel járhatnak az Unió pénzügyi rendszerének stabilitására nézve, így például likviditáselvonási hullámokat és a pénzügyi piacokkal szembeni általános bizalomvesztést kelthetnek.

(4) Az elmúlt években az IKT-kockázat magára vonzotta a nemzetközi, uniós és nemzeti szakpolitikai döntéshozók, szabályozó és standardalkotó szervek figyelmét, arra törekedve, hogy fokozzák a digitális rezilienciát, rögzítsenek standardokat, és koordinálják a szabályozói és felügyeleti munkát. Nemzetközi szinten a Bázeli Bankfelügyeleti Bizottság, a Fizetési és Piaci Infrastruktúra Bizottság, a Pénzügyi Stabilitási Tanács, a Pénzügyi Stabilitási Intézet, valamint a G7 és a G20 célja az, hogy a különböző joghatóságokban az illetékes hatóságokat és a piaci szereplőket olyan eszközökhöz juttassák, amelyek támogatják pénzügyi rendszereik rezilienciáját. Az említett munkát annak szükségessége is vezérli, hogy az IKT-kockázatot – egy nagymértékben összekapcsolt globális pénzügyi rendszer összefüggésében – megfelelően figyelembe vegyék, és a releváns legjobb gyakorlatok terén nagyobb következetességre törekedjenek.

(5) Az uniós és nemzeti célzott szakpolitikai és jogalkotási kezdeményezések ellenére az IKT-kockázat továbbra is kihívást jelent az uniós pénzügyi rendszer digitális működési rezilienciája, teljesítménye és stabilitása szempontjából. A 2008. évi pénzügyi válságot követő reformok elsősorban az uniós pénzügyi ágazat pénzügyi rezilienciáját erősítették, és arra irányultak, hogy – gazdasági és prudenciális szempontból, valamint a piaci magatartás tekintetében – megóvják az Unió versenyképességét és stabilitását. Bár az IKT-biztonság és a digitális reziliencia a működési kockázat részei, a pénzügyi válság utáni szabályozási menetrendben kisebb hangsúlyt kaptak, és fejlesztésükre az Unió pénzügyi szolgáltatásokkal kapcsolatos szakpolitikájának és szabályozási környezetének csak egyes területein vagy csak néhány tagállamban került sor.

(6) A „Pénzügyi technológiai cselekvési terv: Egy versenyképesebb és innovatívabb európai pénzügyi ágazat felé” című, 2018. március 8-i közleményében a Bizottság kiemelte annak kiemelkedő fontosságát, hogy az uniós pénzügyi ágazatot – többek között működési szempontból is – reziliensebbé kell tenni annak érdekében, hogy garantált legyen technológiai biztonsága és megfelelő működése, az IKT-biztonsági sérüléseket és eseményeket követő gyors helyreállítása, ami végső soron lehetővé teszi a pénzügyi szolgáltatások hatékony és zökkenőmentes nyújtását az Unió egészében stresszkörülmények között is, egyúttal hozzájárul a fogyasztói és piaci bizalom megóvásához is.

(7) 2019 áprilisában az 1093/2010/EU európai parlamenti és tanácsi rendelettel ([4]) létrehozott európai felügyeleti hatóság (Európai Bankhatóság, EBH), az 1094/2010/EU európai parlamenti és tanácsi rendelettel ([5]) létrehozott európai felügyeleti hatóság (Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság, EIOPA) és az 1095/2010/EU

([4]) 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.).

([5]) 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.).

európai parlamenti és tanácsi rendelettel ([6]) létrehozott európai felügyeleti hatóság (Európai Értékpapírpiaci Hatóság, ESMA) (a továbbiakban együttesen: európai felügyeleti hatóságok vagy EFH-k) együttes szakvéleményt adtak ki, szorgalmazva a pénzügyi szolgáltatási ágazat IKT-kockázatához való koherens megközelítést, és javaslatot téve a pénzügyi szolgáltatási ágazat digitális működési rezilienciájának egy ágazatspecifikus uniós kezdeményezésen keresztül, arányos módon történő megerősítésére.

(8) Az uniós pénzügyi ágazatot egységes szabálykönyv szabályozza, és a Pénzügyi Felügyeletek Európai Rendszere irányítja. Mindazonáltal a digitális működési rezilienciára és az IKT-biztonságra vonatkozó rendelkezések egyelőre nem teljesen, vagy nem következetesen harmonizáltak annak ellenére, hogy a digitális korban a digitális működési reziliencia létfontosságú a pénzügyi stabilitás és a piaci integritás biztosításához, és legalább olyan fontos, mint például a prudenciális vagy a piaci magatartásra vonatkozó általános előírások. Az egységes szabálykönyvet és a felügyeleti rendszert ezért olyan módon kell továbbfejleszteni, hogy azok a digitális működési rezilienciára is kiterjedjenek; ehhez meg kell erősíteni az illetékes hatóságok megbízatását, hogy e hatóságok – a belső piac integritásának és hatékonyságának védelme, valamint a piac szabályos működésének elősegítése érdekében – felügyelni tudják az IKT-kockázat kezelését a pénzügyi ágazatban.

(9) A jogszabályi eltérések, valamint az IKT-kockázattal kapcsolatos heterogén nemzeti szabályozási és felügyeleti megközelítések akadályozzák a pénzügyi szolgáltatások belső piacának működését, és megnehezítik a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára a letelepedés és a szolgáltatásnyújtás szabadságának zavartalan gyakorlását. Torzulhat a verseny a különböző tagállamokban tevékenységet folytató, azonos típusú pénzügyi szervezetek között is. Különösen igaz ez olyan területeken, ahol az uniós harmonizáció eddig nagyon korlátozottan valósult meg, így például a digitális működési reziliencia tesztelése tekintetében, vagy ahol hiányzik, így például a harmadik féltől eredő IKT-kockázat nyomon követése tekintetében. A nemzeti szintű tervezett fejlesztésekből adódó eltérések további akadályokat képezhetnek a belső piac működésében a piaci szereplők és a pénzügyi stabilitás kárára.

(10) Annak köszönhetően, hogy az IKT-kockázattal kapcsolatos rendelkezéseket uniós szinten csak részben kezelték, máig hiányosságok vagy átfedések mutatkoznak olyan fontos területeken, mint az IKT-vonatkozású események bejelentése és a digitális működési reziliencia tesztelése, továbbá következetlenségek is a megjelenő, egymástól eltérő nemzeti szabályoknak vagy az egymást átfedő szabályok nem költséghatékony alkalmazásának eredményeként. Ez különösen hátrányos az IKT olyan, intenzív felhasználóira nézve, mint a pénzügyi ágazat, mivel a technológiai kockázatok nem ismernek határokat, és a pénzügyi ágazat az Unión belül és azon kívül kiterjedt, határokon átnyúló jelleggel kínálja szolgáltatásait. Egyedi pénzügyi szervezetek, amelyek határokon átnyúló tevékenységet végeznek, vagy több engedéllyel is rendelkeznek (például ugyanaz a pénzügyi szervezet bankként, befektetési vállalkozásként és pénzforgalmi intézményként is rendelkezhet működési engedéllyel, amelyek mindegyikét más-más illetékes hatóság adta ki egy vagy több tagállamban), működési kihívásokkal szembesülnek az IKT-kockázat önálló, koherens és költséghatékony kezelése, valamint az IKT-vonatkozású események káros hatásainak enyhítése során.

(11) mivel az egységes szabálykönyvet nem egészítette ki átfogó IKT- vagy működésikockázat-kezelési keret, a digitális működési rezilienciára vonatkozó követelmények további harmonizációjára van szükség valamennyi pénzügyi szervezet tekintetében. Az IKT-képességek és az általános reziliencia pénzügyi szervezetek általi, az említett alapkövetelményeken alapuló, az üzemszünetek elviselése céljából történő fejlesztése elősegítené az uniós pénzügyi piacok stabilitásának és integritásának megőrzését, és így hozzájárulna a befektetők és fogyasztók magas szintű védelmének biztosításához az Unióban. Mivel e rendelet célja, hogy hozzájáruljon a belső piac zavartalan működéséhez, annak az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkében foglalt, az Európai Unió Bíróságának (Bíróság) állandó ítélkezési gyakorlatával összhangban értelmezett rendelkezéseken kell alapulnia.

(12) E rendelet célja az, hogy egységes szerkezetbe foglalja és korszerűsítse a működési kockázatokra vonatkozó követelmények részét képező, az IKT-kockázatra vonatkozó követelményeket, amelyekkel eddig a különböző uniós jogi aktusokban külön foglalkoztak. Míg az említett jogi aktusok lefedték a pénzügyi kockázatok fő kategóriáit (pl. a hitelkockázatot, a piaci kockázatot, a partnerkockázatot, a likviditási kockázatot és a piaci magatartási kockázatot), elfogadásuk időpontjában nem kezelték átfogóan a digitális működési reziliencia valamennyi összetevőjét. A működési kockázatra vonatkozó szabályokat az említett uniós jogi aktusok gyakran a kockázatkezelés hagyományos kvantitatív megközelítését előnyben részesítve (nevezetesen az IKT-kockázat fedezését célzó tőkekövetelmény előírásával) fejlesztették tovább az IKT-vonatkozású eseményekhez kapcsolódó védelmi, észlelési,

([6]) 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.).

elszigetelési és helyreállítási képességekre, vagy a bejelentési és digitális tesztelési képességekre vonatkozó célzott kvalitatív szabályok helyett. Az említett jogi aktusok elsődleges célja a prudenciális felügyeletre, a piaci integritásra és a piaci magatartásra vonatkozó alapvető szabályok meghatározása és naprakésszé tétele volt.Az IKT-kockázatra vonatkozó különböző szabályok egységes szerkezetbe foglalása és korszerűsítése révén első alkalommal foglalnák következetes módon egyetlen jogalkotási aktusba a pénzügyi ágazatban rejlő digitális kockázatokra vonatkozó valamennyi rendelkezést. Ezért e rendelet egyes korábbi jogi aktusokban pótolja a hiányosságokat, vagy orvosolja a következetlenségeket, többek között az azokban használt terminológia kapcsán, és az IKT-kockázatkezelési képességekre, az események bejelentésére, a működési reziliencia tesztelésére és a harmadik féltől eredő IKT-kockázat nyomon követésére vonatkozó célzott szabályok révén kifejezetten utal az IKT-kockázatra. E rendeletnek tehát az IKT-kockázatra is fel kell hívnia a figyelmet, továbbá el kell ismernie, hogy az IKT-vonatkozású események és a működési reziliencia hiánya veszélyeztethetik a pénzügyi szervezetek megbízhatóságát.

(13) A pénzügyi szervezeteknek az IKT-kockázat kezelésekor ugyanazon megközelítést és ugyanazon elvalapú szabályokat kell alkalmazniuk, figyelembe véve méretüket és általános kockázati profiljukat, valamint szolgáltatásaik, tevékenységeik és műveleteik jellegét, nagyságrendjét és összetettségét. A következetesség hozzájárul a pénzügyi rendszerrel szembeni bizalom erősítéséhez és a rendszer stabilitásának megőrzéséhez, különösen az IKT-rendszerekre, -platformokra és -infrastruktúrákra való nagy fokú támaszkodás idején, amely megnövekedett digitális kockázattal jár. Az alapvető kiberhigiénia betartásával egyidejűleg – az IKT-zavarok hatásának és költségeinek minimalizálása révén – elkerülhetők a súlyos gazdasági áldozatok is.

(14) Egy rendelet elősegíti a szabályozás összetettségének csökkentését, előmozdítja a felügyeleti konvergenciát, és növeli a jogbiztonságot, továbbá hozzájárul a megfelelési költségek csökkentéséhez – különösen a határokon átnyúló tevékenységet végző pénzügyi szervezetek esetében – és a versenytorzulások mérsékléséhez. Ezért a pénzügyi szervezetek digitális működési rezilienciájára vonatkozó közös keret létrehozása céljából a leginkább megfelelő eszköz a rendelet, amellyel garantálható, hogy az uniós pénzügyi ágazat egységesen és koherensen alkalmazza az IKT-kockázatkezelés valamennyi összetevőjét.

(15) Az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([7]) volt a kiberbiztonságra vonatkozó első olyan, uniós szinten elfogadott horizontális keret, amely a pénzügyi szervezetek három típusára, nevezetesen a hitelintézetekre, a kereskedési helyszínekre, valamint a központi szerződő felekre is vonatkozott. Mivel azonban az (EU) 2016/1148 irányelv az alapvető szolgáltatásokat nyújtó gazdasági szereplők azonosítására nemzeti szintű mechanizmust határozott meg, csak egyes olyan hitelintézetek, kereskedési helyszínek és központi szerződő felek, amelyeket a tagállamok azonosítottak, kerültek a gyakorlatban annak hatálya alá, és így azok számára írták elő az IKT-biztonságra és események bejelentésére vonatkozóan az irányelvben megállapított követelményeknek való megfelelést. Az (EU) 2022/2555 európai parlamenti és tanácsi irányelv ([8]) egységes kritériumot ír elő annak meghatározására, hogy mely szervezetek tartoznak az irányelv hatálya alá (méretkorlát-szabály), miközben a pénzügyi szervezetek három típusát továbbra is a hatálya alatt tartja.

(16) mivel azonban ez a rendelet a digitális reziliencia különböző összetevői tekintetében fokozza a harmonizáció szintjét azáltal, hogy az IKT-kockázatkezelés és az IKT-vonatkozású események bejelentése tekintetében a pénzügyi szolgáltatásokra vonatkozó jelenlegi uniós jogban foglaltakhoz képest szigorúbb kötelezettségeket vezet be, ez a magasabb szintű harmonizáció az (EU) 2022/2555 irányelvben foglalt követelményeknél is fokozottabb harmonizációt jelent. Következésképpen ez a rendelet különös szabályt képez az (EU) 2022/2555 irányelv tekintetében. Ugyanakkor alapvető fontosságú a pénzügyi ágazat és a jelenleg az (EU) 2022/2555 irányelvben meghatározott uniós horizontális kiberbiztonsági keret közötti erős kapcsolat fenntartása ahhoz, hogy biztosított legyen a tagállamok által már elfogadott kiberbiztonsági stratégiákkal való összhang, valamint ahhoz, hogy a pénzügyi felügyeletek értesülhessenek az említett irányelv hatálya alá tartozó egyéb ágazatokat érintő kiberbiztonsági eseményekről.

([7]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

([8]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (lásd e Hivatalos Lap 80. oldalát).

(17) Az Európai Unióról szóló szerződés 4. cikkének (2) bekezdésével összhangban és a Bíróság által végzett bírósági felülvizsgálat sérelme nélkül, ez a rendelet nem érintheti a tagállamoknak a közbiztonságra, a védelemre és a nemzetbiztonság védelmére vonatkozó alapvető állami funkciók – például a nemzetbiztonság védelmével ellentétes információszolgáltatás – tekintetében fennálló felelősségét.

(18) Az ágazatközi tanulás lehetővé tétele, és annak érdekében, hogy eredményesen hasznosíthatók legyenek más ágazatok tapasztalatai a kiberfenyegetések kezelése terén, az (EU) 2022/2555 irányelvben említett pénzügyi szervezeteknek továbbra is az említett irányelv „ökoszisztémájának" részét kell képezniük (például az együttműködési csoport és a számítógép-biztonsági eseményekre reagáló csoportok [CSIRT-ek]). Az EFH-knak és az illetékes nemzeti hatóságoknak részt kell tudniuk venni az említett irányelv szerinti Együttműködési Csoport szakpolitikai jellegű stratégiai egyeztetéseiben és technikai tevékenységében, továbbá információt cserélni és továbbra is együttműködni az említett irányelvvel összhangban kijelölt vagy létrehozott egyedüli kapcsolattartó pontokkal. Az e rendelet szerinti illetékes hatóságoknak egyeztetniük is kell és együttműködniük a CSIRT-ekkel. Az illetékes hatóságok számára lehetővé kell tenni azt is, hogy szakvéleményt kérjenek az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságoktól, valamint hogy együttműködési megállapodásokat kössenek a hatékony és gyors reagálású koordinációs mechanizmusok biztosítása céljából.

(19) Tekintettel a pénzügyi szervezetek digitális rezilienciája és fizikai rezilienciája közötti szoros kapcsolatokra, e rendeletben és az (EU) 2022/2557 európai parlamenti és tanácsi irányelvben ([9]) koherens megközelítésre van szükség a kritikus fontosságú szervezetek rezilienciájával kapcsolatban. Mivel az e rendelet hatálya alá tartozó IKT-kockázatkezelési és bejelentési kötelezettségek révén átfogó módon kezelik a pénzügyi szervezetek fizikai rezilienciáját, az (EU) 2022/2557 irányelv III. és IV. fejezetében meghatározott kötelezettségek az említett irányelv hatálya alá tartozó pénzügyi szervezetekre nem alkalmazandók.

(20) A felhőszolgáltatók alkotják az (EU) 2022/2555 irányelv hatálya alá tartozó digitális infrastruktúra egyik kategóriáját. Az e rendelettel létrehozott uniós felvigyázási keretrendszer (a továbbiakban: felvigyázási keretrendszer) a kritikus harmadik fél IKT-szolgáltatók mindegyikére, köztük a pénzügyi szervezetek részére IKT-szolgáltatásokat nyújtó felhőszolgáltatókra is vonatkozik, és azt az (EU) 2022/2555 irányelv alapján végzett felügyelet kiegészítésének kell tekinteni. Emellett az e rendelettel létrehozott felvigyázási keretrendszernek – a digitális felügyeleti hatóságot létrehozó horizontális uniós keret hiányában – ki kell terjednie a felhőszolgáltatókra is.

(21) Az IKT-kockázat feletti teljes kontroll megőrzése érdekében a pénzügyi szervezeteknek az erőteljes és eredményes IKT-kockázatkezelést megalapozó átfogó képességekkel, továbbá valamennyi IKT-vonatkozású esemény kezelésére és a jelentős IKT-vonatkozású események bejelentésére vonatkozó konkrét mechanizmusokkal és politikákkal kell rendelkezniük. Hasonlóképpen, a pénzügyi szervezeteknek az IKT-rendszerek, -kontrollok és -folyamatok tesztelésére, valamint a harmadik féltől eredő IKT-kockázat kezelésére vonatkozó politikákkal kell rendelkezniük. A digitális működési reziliencia-alapértéket növelni kell a pénzügyi szervezetek tekintetében, lehetővé téve ugyanakkor meghatározott pénzügyi szervezetek számára, különösen a mikrovállalkozások, valamint az egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezetek számára a követelmények arányos alkalmazását. A foglalkoztatói nyugellátást szolgáltató intézmények olyan, hatékony felügyeletének elősegítése érdekében, amely arányos, és reagál arra, hogy az illetékes hatóságokra háruló adminisztratív terheket csökkenteni kell, az ilyen pénzügyi szervezetek tekintetében a releváns nemzeti felügyeleti rendszereknek figyelembe kell venniük azok méretét és általános kockázati profilját, valamint szolgáltatásaik, tevékenységeik és műveleteik jellegét, nagyságrendjét és összetettségét, még akkor is, amikor az (EU) 2016/2341 európai parlamenti és tanácsi irányelv ([10]) 5. cikkében megállapított releváns küszöbértékek túllépésére kerül sor. Így különösen a felügyeleti tevékenységeknek azon súlyos kockázatok kezelésének szükségességére kell összpontosítaniuk, amelyek egy adott szervezet IKT-kockázatkezeléséhez társíthatók.

([9]) Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus fontosságú szervezetek rezilienciájáról és a 2008/114/EC tanácsi irányelv hatályon kívül helyezéséről (lásd e Hivatalos Lap 164. oldalát).

([10]) Az Európai Parlament és a Tanács (EU) 2016/2341 irányelve (2016. december 14.) a foglalkoztatói nyugellátást szolgáltató intézmények tevékenységéről és felügyeletéről (HL L 354., 2016.12.23., 37. o.).

Az illetékes hatóságoknak éber, de arányos megközelítést kell fenntartaniuk a foglalkoztatói nyugellátást szolgáltató olyan intézmények felügyeletével kapcsolatban is, amelyek fő tevékenységük jelentős részét – például az eszközkezelést, a biztosításmatematikai számításokat, a számvitelt és az adatgazdálkodást – az (EU) 2016/2341 irányelv 31. cikkének megfelelően – szolgáltatókhoz szervezik ki.

(22) Az IKT-vonatkozású események bejelentésének küszöbértékei és taxonómiái tagállamonként jelentősen eltérnek. Míg az (EU) 2019/881 európai parlamenti és tanácsi rendelettel ([11]) létrehozott Európai Uniós Kiberbiztonsági Ügynökség (ENISA) és az (EU) 2022/2555 irányelv szerinti Együttműködési Csoport által végzett releváns munka révén közös alap teremthető, a többi pénzügyi szervezet tekintetében a küszöbértékek meghatározása és a taxonómiák alkalmazása terén továbbra is maradhatnak vagy megjelenhetnek tagállamonként eltérő megközelítések. Az említett eltérések miatt a pénzügyi szervezeteknek többszörös követelményeknek kell megfelelniük, különösen akkor, ha több tagállamban működnek, és akkor, ha egy pénzügyi csoport részét képezik. Továbbá az ilyen eltérések potenciálisan akadályozhatják olyan további egységes vagy központosított uniós mechanizmusok létrehozását, amelyek felgyorsítják a bejelentési folyamatot, és támogatják az illetékes hatóságok közötti gyors és zavartalan információcserét, ami elengedhetetlen az IKT-kockázat kezeléséhez a kiterjedt, potenciálisan rendszerszintű következményekkel járó támadások esetén.

(23) Ahhoz, hogy csökkenteni lehessen egyes pénzügyi szervezetek adminisztratív terheit és potenciálisan duplikatív bejelentési kötelezettségeit, indokolt, hogy az (EU) 2015/2366 európai parlamenti és tanácsi irányelv ([12]) alapján fennálló esemény bejelentési követelmény többé ne legyen alkalmazandó az e rendelet hatálya alá tartozó pénzforgalmi szolgáltatókra. Következésképpen az említett irányelv 33. cikkének (1) bekezdésében hivatkozott hitelintézeteknek, elektronikuspénz-kibocsátó intézményeknek, pénzforgalmi intézményeknek és számlainformációkat összesítő szolgáltatóknak e rendelet alkalmazásának kezdőnapjától e rendelet alapján kell bejelenteniük valamennyi olyan pénzforgalmi vonatkozású működési vagy biztonsági eseményt, amelyet korábban az említett irányelv alapján jelentettek be, függetlenül attól, hogy az ilyen események IKT-vonatkozásúak-e.

(24) Annak érdekében, hogy az illetékes hatóságok az IKT-vonatkozású események jellegére, gyakoriságára, jelentőségére és hatására vonatkozó teljes áttekintés megszerzése révén képesek legyenek ellátni felügyeleti szerepüket, továbbá a releváns hatóságok, ezen belül a bűnüldöző hatóságok és a szanálási hatóságok közötti információcsere fokozása érdekében e rendeletnek olyan, az IKT-vonatkozású események bejelentésére vonatkozó szilárd rendszert kell létrehoznia, ahol a releváns követelmények kezelik a pénzügyi szolgáltatásokra vonatkozó jogszabályok jelenlegi hiányosságait, és a költségek mérséklése érdekében megszüntetnék a fennálló átfedéseket és párhuzamosságokat. Elengedhetetlen az IKT-vonatkozású események bejelentési rendszerének harmonizálása olyan módon, hogy minden pénzügyi szervezetnek az e rendeletben meghatározott egységes, egyszerűsített keretben legyen bejelentési kötelezettsége az illetékes hatósága felé. Ezenkívül az EFH-knak felhatalmazást kell kapniuk arra, hogy részletesen meghatározzák az IKT-vonatkozású események bejelentési keretének releváns elemeit, köztük a taxonómiákat, az időkereteket, az adatállományokat, a mintadokumentumokat, valamint az alkalmazandó küszöbértékeket. Az (EU) 2022/2555 irányelvvel való teljes összhang biztosítása érdekében a pénzügyi szervezetek számára lehetővé kell tenni, hogy önkéntes alapon értesíthessék a releváns illetékes hatóságot a jelentős kiberfenyegetésekről, amennyiben úgy ítélik meg, hogy a kiberfenyegetés relevanciával bír a pénzügyi rendszer, a szolgáltatást használók vagy az ügyfelek számára.

(25) Egyes pénzügyi szolgáltatási alágazatokban ugyan kidolgoztak a digitális működési reziliencia tesztelésére vonatkozó követelményeket, de olyan keretek meghatározásával, amelyeket nem minden esetben hangoltak össze teljes mértékben. Ez a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára a költségek esetleges halmozódásához vezet, emellett bonyolítja a digitális működési reziliencia tesztléséből származó eredmények kölcsönös elismerését is, ami viszont a belső piac széttagolódásával járhat.

([11]) Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

([12]) Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és az 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).

(26) Emellett, kötelező IKT-tesztelés hiányában a sérülékenységek észlelésére nem kerül sor, ami azt eredményezi, hogy a pénzügyi szervezet IKT-kockázatnak van kitéve, és végső soron nagyobb kockázatot jelent a pénzügyi ágazat stabilitására és integritására nézve. Uniós beavatkozás nélkül a digitális működési reziliencia tesztelése továbbra sem lenne egységes, és az IKT-teszteredmények különböző joghatóságok közötti kölcsönös elismerési rendszere sem valósulna meg. Emellett, mivel valószínűleg más pénzügyi szolgáltatási alágazatok nem vezetnének be ilyen tesztelési rendszereket érdemi nagyságrendben, nem használnák ki a tesztelési keret potenciális előnyeit az IKT-sérülékenységek és kockázatok feltárása, valamint a védelmi képességek és az üzletmenet-folytonosság tesztelése tekintetében sem, ami hozzájárul az ügyfelek, a beszállítók és az üzleti partnerek bizalmának növeléséhez. Az említett átfedések, eltérések és hiányosságok kiküszöbölése céljából meg kell állapítani a koordinált tesztelési rendszerre vonatkozó szabályokat, és ezáltal megkönnyíteni a fejlett tesztelés kölcsönös elismerését az e rendeletben meghatározott kritériumoknak megfelelő pénzügyi szervezetek számára.

(27) A pénzügyi szervezeteket részben az motiválja IKT-szolgáltatások igénybevételére, hogy képesek legyenek alkalmazkodni a kialakulóban lévő versengő digitális világgazdasághoz, növeljék üzleti hatékonyságukat, és megfeleljenek a fogyasztói keresletnek. Az igénybevétel jellege és mértéke az elmúlt években folyamatosan alakult, csökkentve a pénzügyi közvetítés költségeit, lehetővé téve az üzleti tevékenység bővítését és skálázhatóságát a pénzügyi tevékenységek kiépítése során, ugyanakkor az összetett belső folyamatok kezeléséhez is hozzáférhetővé téve az IKT-eszközök széles körét.

(28) Az IKT-szolgáltatások kiterjedt felhasználását bizonyítják azon összetett szerződéses megállapodások is, amelyeknél a pénzügyi szervezetek gyakran szembesülnek nehézségekkel a rájuk vonatkozó prudenciális előírásokhoz vagy egyéb szabályozási követelményekhez igazodó szerződési feltételek kitárgyalása terén, vagy egyébként, konkrét jogosultságok – így például hozzáférési vagy audit jogosultságok – érvényesítése terén, még akkor is, ha ez utóbbiakat a szerződéses megállapodásaik rögzítik. Emellett az említett szerződéses megállapodások közül sok nem nyújt elegendő biztosítékot az alvállalkozói folyamatok teljeskörű nyomon követésére, ezáltal megfosztva a pénzügyi szervezetet azon képességétől, hogy értékelje a kapcsolódó kockázatokat. Ezenkívül, mivel a harmadik fél IKT-szolgáltatók gyakran nyújtanak szabványosított szolgáltatásokat különböző típusú ügyfeleknek, az ilyen szerződéses megállapodások nem minden esetben felelnek meg a pénzügyi ágazati szereplők egyedi vagy sajátos igényeinek.

(29) Bár a pénzügyi szolgáltatásokra vonatkozó uniós jogszabályok tartalmaznak bizonyos általános kiszervezési szabályokat, a szerződéses dimenzió nyomon követése nem épült be teljes mértékben az uniós jogba. A harmadik fél IKT-szolgáltatókkal kötött szerződéses megállapodásokra vonatkozó egyértelmű és célzott uniós előírások hiányában az IKT-kockázat külső forrásainak átfogó kezelése nem valósul meg. Következésképpen szükséges bizonyos, a pénzügyi szervezetek harmadik féltől eredő IKT-kockázatának kezelésére irányadó alapelveket rögzíteni, amelyek különös fontosságúak, amikor a pénzügyi szervezetek harmadik fél IKT-szolgáltatókat vesznek igénybe kritikus vagy lényeges funkcióik támogatása érdekében. Az említett elveket a szerződéses megállapodások teljesítésének és megszüntetésének számos elemével kapcsolatban egy sor alapvető szerződéses joggal kell kiegészíteni bizonyos minimális biztosítékok biztosítása céljából, annak érdekében, hogy erősítsék a pénzügyi szervezetek azon képességét, hogy eredményesen nyomon kövessék a harmadik fél IKT-szolgáltatók szintjén felmerülő valamennyi IKT-kockázatot. Az említett elvek kiegészítik a kiszervezésre alkalmazandó ágazati jogot.

(30) Mára nyilvánvalóvá vált a harmadik féltől eredő IKT-kockázat és a harmadik féltől való IKT-függőség nyomon követése tekintetében a homogenitás és a konvergencia bizonyos fokú hiánya. A kiszervezés kezelésére irányuló erőfeszítések így például a felhőszolgáltatókhoz történő kiszervezésről szóló 2019-es EBH-iránymutatások és a felhőszolgáltatókhoz történő kiszervezésről szóló 2021-es ESMA-iránymutatások ellenére az uniós jog nem foglalkozik elégséges módon az olyan rendszerszintű kockázat elleni fellépés tágabb kérdésével, amelyet a pénzügyi ágazatnak egy korlátozott számú kritikus harmadik fél IKT-szolgáltatóval szembeni kitettsége idézhet elő. Az uniós szintű szabályok hiányát súlyosbítja az, hogy hiányoznak az olyan felhatalmazásra és eszközökre vonatkozó nemzeti szabályok, amelyek lehetővé tennék a pénzügyi felügyeletek számára, hogy behatóan megismerhessék a harmadik féltől való IKT-függőségeket, és megfelelően nyomon követhessék a harmadik féltől való IKT-függőségek koncentrációjából eredő kockázatokat.

(31) Figyelembe véve a kiszervezés egyre elterjedtebb gyakorlatával és a harmadik fél IKT-szolgáltatók koncentrációjával járó potenciális rendszerszintű kockázatokat, továbbá szem előtt tartva az olyan nemzeti mechanizmusok elégtelenségét, amelyek megfelelő eszközöket bocsátanának a pénzügyi felügyeletek rendelkezésére a kritikus harmadik fél IKT-szolgáltatóknál felmerülő IKT-kockázat mennyiségi és minőségi értékeléséhez, valamint hatásaik elhárításához, megfelelő felvigyázási keretrendszert szükséges létrehozni, amely lehetővé teszi azon harmadik fél IKT-szolgáltatók tevékenységének folyamatos nyomon követését, amelyek pénzügyi szervezetek kritikus harmadik fél IKT-szolgáltatói, miközben biztosítja a pénzügyi szervezetektől eltérő ügyfelek bizalmas kezelésének és biztonságának megőrzését. Miközben az IKT-szolgáltatások csoporton belüli nyújtása sajátos kockázatokkal és előnyökkel jár, nem tekinthető automatikusan kevésbé kockázatosnak, mint az IKT-szolgáltatások pénzügyi csoporton kívüli szolgáltatók általi nyújtása, és ezért ugyanazon szabályozási keret hatálya alá kell tartoznia. Azonban amennyiben az IKT-szolgáltatásokat ugyanazon pénzügyi csoporton belül nyújtják, a pénzügyi szervezetek magasabb szintű kontrollt gyakorolhatnak a csoporton belüli szolgáltatók felett, amit az általános kockázatértékelés során figyelembe kell venni.

(32) Amint az IKT-kockázat egyre összetettebbé és fejlettebbé válik, az IKT-kockázat észlelésére és megelőzésére irányuló megfelelő intézkedések nagymértékben függenek a fenyegetéssel és sérülékenységgel kapcsolatos hírszerzés pénzügyi szervezetek közötti rendszeres megosztásától. Az információk megosztása hozzájárul a kiberfenyegetésekkel kapcsolatos fokozott tudatosság megteremtéséhez. Ez viszont javítja a pénzügyi szervezetek képességét annak megelőzésére, hogy a kiberfenyegetésekből valóban IKT-vonatkozású események váljanak, emellett lehetővé teszi a pénzügyi szervezetek számára az IKT-vonatkozású események hatásainak eredményesebb elszigetelését, továbbá a gyorsabb helyreállítást. Uniós szintű iránymutatás hiányában az eddigiek során a jelek szerint több tényező is gátolta az ilyen hírszerzés-megosztást, különösen az adatvédelmi, trösztellenes és felelősségi szabályokkal való összeegyeztethetőséggel kapcsolatos bizonytalanság.

(33) Emellett a hasznos információk visszatartásához vezetnek az olyan típusú információkkal kapcsolatos kétségek, amelyek megoszthatók más piaci szereplőkkel vagy nem felügyeleti hatóságokkal (így például elemzési input céljából az ENISA-val, vagy bűnüldözési célból az Europollal). Ezért az információmegosztás terjedelme és minősége továbbra is korlátozott és széttagolt, a releváns információk átadására többnyire helyi szinten (nemzeti kezdeményezések útján) kerül sor, és nincsenek az integrált pénzügyi rendszer igényeihez igazodó, egységes uniós szintű információmegosztási megállapodások. Ezért fontos megerősíteni az említett kommunikációs csatornákat.

(34) A pénzügyi szervezeteket ösztönözni kell arra, hogy – információmegosztási megállapodásokban való részvétel révén – kiberfenyegetettségi információkat és hírszerzést osszanak meg egymással, és hogy stratégiai, taktikai és operatív szinten is együttesen használják ki az egyes szervezeteknél meglévő ismereteket és gyakorlati tapasztalatokat annak érdekében, hogy növeljék képességüket a kiberfenyegetések megfelelő értékelésére, nyomon követésére, kivédésére és az arra való reagálásra. Ezért lehetővé kell tenni az önkéntes információmegosztási megállapodások mechanizmusainak uniós szintű megjelenését, mivel a megbízható környezetben átadott információk segítségével a pénzügyi szolgáltatási ágazat közössége megelőzhetné a kiberfenyegetéseket és együttesen háríthatná el azokat az IKT-kockázat terjedésének gyors lehatárolásával, valamint a pénzügyi csatornákon keresztüli esetleges átterjedés megakadályozásával. Az említett mechanizmusoknak meg kell felelniük az „Iránymutatás az Európai Unió működéséről szóló szerződés 101. cikkének a horizontális együttműködési megállapodásokra való alkalmazhatóságáról” című, 2011. január 14-i bizottsági közleményben meghatározott uniós alkalmazandó versenyjogi szabályoknak, valamint az uniós adatvédelmi szabályoknak, különösen az (EU) 2016/679 európai parlamenti és tanácsi rendeletnek ([13]). Működésüknek az említett rendelet 6. cikkében foglalt egy vagy több jogalap használatán kell alapulnia, így például a személyes adatok olyan kezelésével összefüggésben, amely az említett rendelet 6. cikke (1) bekezdésének f) pontjában említettek szerint az adatkezelő vagy valamely harmadik fél jogos érdekének céljából szükséges, valamint a személyes adatok olyan kezelésével összefüggésben is, amely az említett rendelet 6. cikke (1) bekezdésének c), illetve e) pontjában említettek szerint szükséges az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez, illetve szükséges valamely közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához.

([13]) 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

(35) Annak érdekében, hogy a teljes pénzügyi ágazat magas szintű digitális működési rezilienciával rendelkezzen, ugyanakkor lépést tartson a technológiai fejlődéssel, e rendeletnek az IKT-szolgáltatások valamennyi típusából eredő kockázatokkal foglalkoznia kell. E célból az IKT-szolgáltatások fogalommeghatározását e rendelet összefüggésében tágan kell értelmezni, úgy, hogy az magában foglalja az IKT-rendszer útján egy vagy több belső vagy külső felhasználó részére folyamatosan nyújtott digitális és adatszolgáltatásokat. Az említett fogalommeghatározásnak például magában kell foglalnia az – elektronikus hírközlési szolgáltatások kategóriájába tartozó – úgynevezett „over-the-top" szolgáltatásokat is. A fogalommeghatározásból kizárólag a közcélú kapcsolt távbeszélő-hálózati szolgáltatásoknak, vezetékes szolgáltatásoknak, hagyományos telefonszolgáltatásoknak vagy vezetékes telefonszolgáltatásoknak minősülő, hagyományos analóg telefonszolgáltatások korlátozott kategóriáját kell kizárni.

(36) Az e rendeletben tervezett kiterjedt hatály ellenére a digitális működési rezilienciára vonatkozó szabályok alkalmazásakor figyelembe kell venni a pénzügyi szervezetek között a méretük és az általános kockázati profiljuk tekintetében fennálló jelentős különbségeket. Általános elvként az IKT-kockázatkezelési keretrendszer végrehajtására szánt erőforrások és képességek felosztásakor a pénzügyi szervezeteknek megfelelő egyensúlyt kell teremteniük IKT-szükségleteik, valamint méretük és általános kockázati profiljuk, továbbá szolgáltatásaik, tevékenységeik és műveleteik jellege, nagyságrendje és összetettsége között, míg az illetékes hatóságoknak folytatniuk kell az ilyen felosztási megközelítés értékelését és felülvizsgálatát.

(37) Az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett, számlainformációkat összesítő szolgáltatók – figyelembe véve tevékenységeik sajátos jellegét és az azokból eredő kockázatokat – kifejezetten e rendelet hatálya alá tartoznak. Emellett a 2009/110/EK európai parlamenti és tanácsi irányelv ([14]) 9. cikkének (1) bekezdése és az (EU) 2015/2366 irányelv 32. cikkének (1) bekezdése alapján mentesített elektronikuspénz-kibocsátó intézmények és pénzforgalmi intézmények is e rendelet hatálya alá tartoznak, még akkor is, ha nem kaptak a 2009/110/EK irányelvnek megfelelően engedélyt elektronikus pénz kibocsátására, vagy ha nem kaptak az (EU) 2015/2366 irányelvnek megfelelően engedélyt pénzforgalmi szolgáltatások nyújtására és teljesítésére. Azonban a 2013/36/EU európai parlamenti és tanácsi ([15]) irányelv 2. cikke (5) bekezdésének 3. pontjában említett postai elszámolóközpontok ki vannak zárva e rendelet hatálya alól. Az (EU) 2015/2366 irányelv alapján mentesített pénzforgalmi intézmények, a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmények és az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett, számlainformációkat összesítő szolgáltatók illetékes hatósága az (EU) 2015/2366 irányelv 22. cikkével összhangban kijelölt illetékes hatóság.

(38) mivel a nagyobb pénzügyi szervezeteknek az erőforrások szélesebb köre állhat a rendelkezésére, és gyorsabban mozgósíthatnak forrásokat irányítási struktúrák kialakítására és különféle vállalati stratégiák kidolgozására, csak az e rendelet értelmében vett mikrovállalkozásnak nem minősülő pénzügyi szervezetek számára kell kötelezővé tenni az összetettebb irányítási rendszerek kidolgozását. Az ilyen szervezetek jobban képesek különösen arra, hogy célzott vezetői funkciókat alakítsanak ki a harmadik fél IKT-szolgáltatókkal kötött megállapodások felügyelete vagy a válságkezelés céljából, hogy a három védelmi vonalra épülő modell szerint szervezzék meg IKT-kockázatkezelésüket, vagy hogy kialakítsanak egy belső kockázatkezelési és kontrollmodellt, és hogy az IKT-kockázatkezelési keretrendszerüket belső auditoknak vessék alá.

(39) Egyes pénzügyi szervezetek mentességeket élveznek, vagy a releváns ágazatspecifikus uniós jogszabályok alapján nagyon enyhe szabályozási keret hatálya alá tartoznak. Az említett pénzügyi szervezetek közé tartoznak a 2011/61/EU európai parlamenti és tanácsi irányelv ([16]) 3. cikkének (2) bekezdésében említett alternatívbefektetésialap-kezelők, a 2009/138/EK európai parlamenti és tanácsi irányelv ([17]) 4. cikkében említett biztosítók és viszontbiztosítók, valamint azon foglalkoztatói nyugellátást szolgáltató intézmények, amelyek összesen legfeljebb 15 taggal rendelkező nyugdíjrendszereket működtetnek. E mentességek fényében nem lenne arányos az ilyen

([14]) Az Európai Parlament és a Tanács 2009/110/EK irányelve (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről (HL L 267., 2009.10.10., 7. o.).

([15]) Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.).

([16]) Az Európai Parlament és a Tanács 2011/61/EU irányelve (2011. június 8.) az alternatívbefektetésialap-kezelőkről, valamint a 2003/41/EK és a 2009/65/EK irányelv, továbbá az 1060/2009/EK és az 1095/2010/EU rendelet módosításáról (HL L 174., 2011.7.1., 1. o.).

([17]) Az Európai Parlament és a Tanács 2009/138/EK irányelve (2009. november 25.) a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról (Szolvencia II) (HL L 335., 2009.12.17., 1. o.).

pénzügyi szervezeteket e rendelet hatálya alá vonni. Emellett ez a rendelet elismeri a biztosításközvetítési piac szerkezetének sajátosságait, így a mikrovállalkozásnak vagy kis- vagy középvállalkozásnak minősülő biztosítás-közvetítők, viszontbiztosítás-közvetítők és kiegészítő biztosításközvetítői tevékenységet végző személyek nem tartozhatnak e rendelet hatálya alá.

(40) mivel a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett jogalanyok nem tartoznak az említett irányelv hatálya alá, a tagállamok számára következésképpen lehetővé kell tenni annak eldöntését, hogy mentesítik-e e rendelet alkalmazása alól a saját területükön működő ilyen jogalanyokat.

(41) Hasonlóképpen, e rendeletnek a 2014/65/EU európai parlamenti és tanácsi irányelv ([18]) hatályához való hozzáigazítása érdekében helyénvaló kizárni e rendelet hatálya alól az említett irányelv 2. és 3. cikkében említett azon természetes és jogi személyeket is, akik vagy amelyek anélkül jogosultak befektetési szolgáltatások nyújtására, hogy a 2014/65/EU irányelv szerinti engedélyt meg kellene szerezniük. Azonban a 2014/65/EU irányelv 2. cikke azon szervezeteket – így a központi értéktárakat, a kollektív befektetési vállalkozásokat, vagy a biztosítókat és viszontbiztosítókat – is kizárja az irányelv hatálya alól, amelyek e rendelet alkalmazásában pénzügyi szervezetnek minősülnek. Az említett irányelv 2. és 3. cikkében említett személyek és szervezetek e rendelet hatálya alóli kizárása nem terjedhet ki az említett központi értéktárakra, kollektív befektetési vállalkozásokra, vagy biztosítókra és viszontbiztosítókra.

(42) Az ágazatspecifikus uniós jogszabályok értelmében egyes pénzügyi szervezetekre – a méretükkel vagy az általuk nyújtott szolgáltatásokkal összefüggő okokból – enyhébb követelmények vagy mentességek vonatkoznak. A pénzügyi szervezetek említett kategóriája magában foglalja a kis méretű és össze nem kapcsolt befektetési vállalkozásokat, az olyan, kis méretű foglalkoztatói nyugellátást szolgáltató intézményeket, amelyeket az érintett tagállam az (EU) 2016/2341 irányelv 5. cikkében meghatározott feltételek mellett kizárhat az említett irányelv hatálya alól, és amelyek összesen legfeljebb 100 taggal rendelkező nyugdíjrendszereket működtetnek, továbbá a 2013/36/EU irányelv szerint mentesített intézményeket. Ezért az arányosság elvével összhangban és az ágazatspecifikus uniós jogszabályok szellemének megőrzése érdekében helyénvaló az említett pénzügyi szervezeteket is az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá vonni. Az EFH-k által kidolgozandó szabályozástechnikai standardok nem módosíthatják az említett pénzügyi szervezetekre vonatkozó IKT-kockázatkezelési keretrendszer arányos jellegét. Ezenkívül, az arányosság elvével összhangban helyénvaló az (EU) 2015/2366 irányelv 32. cikkének (1) bekezdésében említett azon pénzforgalmi intézményeket és a 2009/110/EK irányelv 9. cikkében említett azon elektronikuspénz-kibocsátó intézményeket, amelyeket az említett uniós jogi aktusokat átültető nemzeti joggal összhangban mentesítettek, ugyancsak az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá vonni, míg azon pénzforgalmi intézményeknek és elektronikuspénz-kibocsátó intézményeknek, amelyekre az ágazati uniós jogot átültető nemzeti joggal összhangban nem vonatkozik mentesség, az e rendeletben meghatározott általános keretnek kell megfelelniük.

(43) Hasonlóképpen, a mikrovállalkozásnak minősülő, vagy az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezetektől nem követelhető meg, hogy létrehozzanak egy feladatkört a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételéről kötött megállapodásaik nyomon követésére; vagy hogy kinevezzék a felső vezetés egy tagját a kapcsolódó kockázati kitettség és a releváns dokumentáció felvigyázásáért felelős személyként; hogy az IKT-kockázat kezelésére és felvigyázására vonatkozó felelősséget egy kontrollfunkcióra ruházzák, és az összeférhetetlenségek elkerülése érdekében biztosítsák az ilyen kontrollfunkció megfelelő függetlenségét; hogy dokumentálják és legalább évente egyszer felülvizsgálják az IKT-kockázatkezelési keretrendszert; hogy rendszeresen belső auditnak vessék alá az IKT-kockázatkezelési keretrendszert; hogy a hálózati és információsrendszer-infrastruktúrájában és folyamataiban bekövetkezett jelentős változásokat követően beható értékeléseket végezzenek; hogy rendszeresen elvégezzék az elavult IKT-rendszerek kockázatelemzését; hogy az IKT-reagálási és -helyreállítási tervek végrehajtását független belső audit felülvizsgálatoknak vessék alá; hogy válságkezelési funkcióval rendelkezzenek; hogy kiterjesszék az üzletmenet-folytonossági, reagálási és helyreállítási tervek tesztelését az elsődleges IKT-infrastruktúra és a tartalékeszközök közötti átállási forgatókönyvekre; hogy beszámoljanak az illetékes hatóságoknak – azok kérésére – a jelentős IKT-vonatkozású

([18]) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).

eseményekből eredő összesített becsült éves költségekről és veszteségekről; hogy fenntartsák az IKT-tartalékkapacitásokat; hogy tájékoztassák az illetékes nemzeti hatóságokat az IKT-vonatkozású események utólagos felülvizsgálatát követően végrehajtott változtatásokról; hogy folyamatosan nyomon kövessék a releváns technológiai fejlesztéseket; hogy átfogó programot alakítsanak ki a digitális működési reziliencia tesztelésére az e rendeletben előírt IKT-kockázatkezelési keretrendszer integráns részeként; vagy hogy fogadjanak el a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát, és azt rendszeresen vizsgálják felül.Ezenkívül a mikrovállalkozásoknak a kockázati profiljukat alapul véve csak azt kell mérlegelniük, hogy szükséges-e ilyen IKT-tartalékkapacitásokat fenntartaniuk. A mikrovállalkozások számára a digitális működési reziliencia tesztelését szolgáló programok tekintetében rugalmasabb rendszert kell biztosítani. Amikor mérlegelik az elvégzendő tesztelés típusát és gyakoriságát, a mikrovállalkozásoknak megfelelő egyensúlyra kell törekedniük a magas szintű digitális működési reziliencia fenntartására irányuló célkitűzés, a rendelkezésre álló erőforrások és az általános kockázati profiljuk között. A mikrovállalkozásokat és az e rendelet szerinti egyszerűsített IKT-kockázatkezelési keretrendszer hatálya alá tartozó pénzügyi szervezeteket mentesíteni kell azon követelmény alól, hogy elvégezzék az IKT-eszközök, -rendszerek és -folyamatok olyan fejlett tesztelését, amely fenyegetés alapú behatolási tesztelésen (TLPT, threat-led penetration testing) alapul, mivel az ilyen tesztelés elvégzése csak az e rendeletben meghatározott kritériumoknak megfelelő pénzügyi szervezetek számára írható elő. Korlátozott képességeikre tekintettel, a mikrovállalkozások számára lehetővé kell tenni, hogy a harmadik fél IKT-szolgáltatóval megállapodjanak arról, hogy a pénzügyi szervezet hozzáférési, ellenőrzési és audit jogát átruházzák egy, a harmadik fél IKT-szolgáltató által kinevezendő független harmadik félre, feltéve, hogy a pénzügyi szervezet bármikor tájékoztatást és bizonyosságot kérhet a vonatkozó független harmadik féltől a harmadik fél IKT-szolgáltató teljesítményéről.

(44) mivel a fenyegetés alapú behatolási tesztelést csak a digitális működési reziliencia fejlett tesztelése céljából azonosított pénzügyi szervezetek számára kell előírni, az ilyen tesztek lefolytatásával járó igazgatási folyamatok és pénzügyi költségek terhét a pénzügyi szervezetek kis hányada kell, hogy viselje.

(45) A pénzügyi szervezeteknél egyfelől az üzleti stratégiák, és másfelől az IKT-kockázatkezelés teljeskörű összehangolása és általános összhangja érdekében a pénzügyi szervezetek vezető testületei számára elő kell írni, hogy vállaljanak lényeges és tevékeny szerepet az IKT-kockázatkezelési keretrendszer, valamint a digitális működési rezilienciára vonatkozó általános stratégia irányításában és alakításában. A vezető testületek által alkalmazandó megközelítésnek nem elegendő az IKT-rendszerek rezilienciáját biztosító eszközökre összpontosítania, hanem ki kell terjednie a személyekre és a folyamatokra is olyan szabályzatok útján, amelyek a vállalati struktúra minden rétegében, a személyzet valamennyi tagjára vonatkozóan hangsúlyozzák a kiberkockázatok erőteljes tudatosítását és a szigorú kiberhigiéniás normák betartása melletti elkötelezettséget. A pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testületet terhelő végső felelősségnek egy olyan, az említett átfogó megközelítés részét képező általános elvnek kell lennie, amelynek az IKT-kockázatkezelés nyomon követésének kontrolljában való folyamatos vezető testületi részvétel formájában kell megnyilvánulnia.

(46) Ezenfelül a pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testület által vállalt teljeskörű és végső felelősség elve együtt jár azzal, hogy olyan szinten kell biztosítani az IKT-vonatkozású beruházások és az általános költségvetés szintjét, amely képessé tenné a pénzügyi szervezetet a magas szintű digitális működési reziliencia megvalósítására.

(47) A releváns nemzetközi, nemzeti és ágazati legjobb gyakorlatokra, iránymutatásokra, ajánlásokra, valamint kiberkockázat-kezelési megközelítésekre építő rendelet olyan elveket mozdít elő, amelyek megkönnyítik az IKT-kockázatkezelés általános strukturálását. Következésképpen, mindaddig, amíg a pénzügyi szervezetek által bevezetett fő képességek kezelik az IKT-kockázatkezelés e rendeletben meghatározott különböző funkcióit (azonosítás, védelem és megelőzés, felderítés, reagálás és helyreállítás, tanulás és alkalmazkodás, valamint kommunikáció), a pénzügyi szervezeteknek szabadon kell tudniuk alkalmazni az eltérő keretek között vagy kategóriák mentén kidolgozott IKT-kockázatkezelési modelleket.

(48) Ahhoz, hogy lépést tarthassanak a kiberfenyegetettségi helyzet alakulásával, a pénzügyi szervezeteknek naprakész IKT-rendszereket kell fenntartaniuk, amelyek megbízhatóak, és képesek nemcsak garantálni a szolgáltatásaikhoz szükséges adatfeldolgozást, hanem biztosítani elegendő technológiai rezilienciát is, hogy lehetővé váljon számukra a piaci stresszhelyzet vagy egyéb kedvezőtlen helyzetek miatti további adatfeldolgozási igények megfelelő kezelése.

(49) Hatékony üzletmenet-folytonossági és helyreállítási tervekre van szükség ahhoz, hogy a pénzügyi szervezetek – összhangban biztonsági mentési szabályzatukkal – az IKT-vonatkozású eseményeket, különösen a kibertámadásokat haladéktalanul és gyorsan, a kár mérséklésével, a tevékenység újraindítását és a helyreállítási intézkedéseket előtérbe helyezve oldhassák meg. Azonban a tevékenység ilyen újraindítása semmilyen módon nem veszélyeztetheti a hálózati és információs rendszerek integritását és biztonságát, vagy az adatok rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét.

(50) Míg e rendelet lehetővé teszi a pénzügyi szervezetek számára, hogy a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzéseiket rugalmasan határozzák meg, és így az ilyen célkitűzéseket a releváns funkciók jellegének és kritikusságának, valamint a vonatkozó üzleti igényeknek a maradéktalan figyelembevételével határozzák meg, mindazonáltal elő kell írni számukra, hogy az ilyen célkitűzések meghatározásakor végezzék el a piaci hatékonyságra gyakorolt potenciális általános hatás értékelését.

(51) A kibertámadások terjesztői hajlamosak arra, hogy közvetlenül a forrásnál próbáljanak anyagi haszonra szert tenni, jelentős következményeknek téve így ki a pénzügyi szervezeteket. Annak megelőzése érdekében, hogy az IKT-rendszerek elveszítsék integritásukat, vagy elérhetetlenné váljanak, és így az adatvédelmi incidensek vagy a fizikai IKT-infrastruktúrában keletkező kár elkerülése érdekében számottevő mértékben javítani és észszerűsíteni kell a jelentős IKT-vonatkozású események pénzügyi szervezetek általi bejelentését. Az IKT-vonatkozású események bejelentését harmonizálni kell egy olyan kötelezettség bevezetése révén, amelynek értelmében minden pénzügyi szervezetnek közvetlenül a releváns illetékes hatósága felé kell bejelentést tennie. Amennyiben egy pénzügyi szervezet egynél több illetékes nemzeti hatóság felügyelete alá tartozik, a tagállamoknak egyetlen illetékes hatóságot kell megjelölniük az említett bejelentés címzettjeként. Az 1024/2013/EU tanácsi rendelet ([19]) 6. cikkének (4) bekezdése szerint jelentősnek minősített hitelintézeteknek az említett bejelentést az illetékes nemzeti hatóságok felé kell megtenniük, amelyeknek ezt követően továbbítaniuk kell a bejelentést az Európai Központi Banknak (EKB).

(52) A közvetlen bejelentés várhatóan lehetővé teszi a pénzügyi felügyeletek számára, hogy azonnal hozzáférjenek a jelentős IKT-vonatkozású eseményekkel kapcsolatos információkhoz. A pénzügyi felügyeleteknek viszont továbbítaniuk kell a jelentős IKT-vonatkozású események részleteit a nem pénzügyi állami hatóságok (így például az (EU) 2022/2555 irányelv szerinti illetékes hatóságok és egyedüli kapcsolattartó pontok, a nemzeti adatvédelmi hatóságok, valamint a bűncselekmény jellegű jelentős IKT-vonatkozású események kapcsán a bűnüldöző hatóságok) részére annak érdekében, hogy fokozzák az ilyen hatóságoknak az ilyen biztonsági eseményekkel kapcsolatos ismereteit, és a CSIRT-ek esetében megkönnyítsék az azonnali segítségnyújtást, amely adott esetben a pénzügyi szervezetek számára adható. Ezenfelül a tagállamok számára lehetővé kell tenni, hogy úgy határozzanak, hogy a pénzügyi szervezeteknek maguknak kelljen ilyen információkat a pénzügyi szolgáltatások területén kívül működő hatóságok rendelkezésére bocsátani. Az említett információáramlásoknak lehetővé kell tenniük a pénzügyi szervezetek számára, hogy gyorsan profitáljanak bármely releváns technikai inputból, a korrekciós intézkedésekre vonatkozó tanácsadásból, és az ilyen hatóságok későbbi utókövetéséből. A jelentős IKT-vonatkozású eseményekkel kapcsolatos információk áramlásának kétirányúnak kell lennie: a pénzügyi felügyeleteknek meg kell adniuk a szükséges visszajelzést és iránymutatást a pénzügyi szervezet részére, ugyanakkor az EFH-knak – a szélesebb körű kollektív védelem érdekében – meg kell osztaniuk a valamely eseményhez kapcsolódó kiberfenyegetésekre és sérülékenységekre vonatkozó anonimizált adatokat.

(53) Miközben az események bejelentését valamennyi pénzügyi szervezet számára elő kell írni, az említett követelmény várhatóan nem érinti valamennyit azonos módon. Valóban, a releváns lényegességi küszöbértékeket és a bejelentés ütemezését az EFH-k által kidolgozandó szabályozástechnikai standardokon alapuló, felhatalmazáson alapuló jogi aktusok keretében megfelelően ki kell igazítani annak érdekében, hogy azok csak a jelentős IKT-vonatkozású eseményekre vonatkozzanak. Emellett a bejelentési kötelezettségek ütemezésének meghatározásakor a pénzügyi szervezetek sajátosságait is figyelembe kell venni.

(54) E rendeletnek elő kell írnia a hitelintézetek, a pénzforgalmi intézmények, a számlainformációkat összesítő szolgáltatók és az elektronikuspénz-kibocsátó intézmények számára, hogy valamennyi – korábban az (EU) 2015/2366 irányelv alapján bejelentett – pénzforgalmi vonatkozású működési vagy biztonsági eseményt bejelentsék, függetlenül a zavar vagy az esemény IKT-jellegétől.

([19]) A Tanács 1024/2013/EU rendelete (2013. október 15.) az Európai Központi Banknak a hitelintézetek prudenciális felügyeletére vonatkozó politikákkal kapcsolatos külön feladatokkal történő megbízásáról (HL L 287., 2013.10.29., 63. o.).

(55) Az EFH-kat meg kell bízni azzal, hogy értékeljék az IKT-vonatkozású események bejelentése uniós szintű lehetséges központosításának megvalósíthatóságát és feltételeit. Az ilyen központosítás jelentheti egy olyan, a jelentős IKT-vonatkozású események bejelentésére szolgáló egységes uniós adatbázis létrehozását, amely vagy közvetlenül fogadná a vonatkozó bejelentéseket és automatikusan értesítené az illetékes nemzeti hatóságokat, vagy mindössze az illetékes nemzeti hatóságok által továbbított releváns bejelentéseket fogná össze, és ezáltal koordinációs szerepet látna el. Az EFH-kat meg kell bízni azzal, hogy – az EKB-val és az ENISA-val egyeztetve – készítsenek közös jelentést, amelyben megvizsgálják egy egységes európai uniós adatbázis létrehozásának megvalósíthatóságát.

(56) A magas szintű digitális működési reziliencia megvalósításához, valamint összhangban mind a releváns nemzetközi szabványokkal (pl. G7: A fenyegetés alapú behatolási tesztelés alapelemei), mind az Unióban alkalmazott olyan keretekkel, mint a TIBER-EU, a pénzügyi szervezeteknek rendszeresen tesztelniük kell az IKT-rendszereik és az IKT-vonatkozású feladatokat ellátó munkatársaik megelőzési, felderítési, reagálási és helyreállítási képességeinek hatékonyságát, hogy feltárhassák és kezelhessék a potenciális IKT-sérülékenységeket. Ahhoz, hogy figyelembe lehessen venni a különböző pénzügyi szolgáltatási alágazatok között és azokon belül az egyes pénzügyi szervezetek kiberbiztonsági felkészültsége tekintetében fennálló különbségeket, a tesztelésnek az eszközök és műveletek széles skáláját kell felölelnie, az alapvető követelmények felmérésétől kezdve (pl. sérülékenységi értékelések és vizsgálatok, nyílt forrású elemzések, hálózatbiztonsági értékelések, hiányelemzések, fizikai biztonsági felülvizsgálatok, kérdőívek és szoftveres megoldások vizsgálata, lehetőség szerint forráskódvizsgálatok, forgatókönyv-alapú tesztek, kompatibilitás-vizsgálat, teljesítmény-vizsgálat vagy végpontok közötti tesztek) egészen a TLPT útján végzett fejlettebb tesztelésig. Az ilyen fejlett tesztelést csak azon pénzügyi szervezetek esetében kell előírni, amelyek IKT-szempontból kellően érettek ahhoz, hogy képesek legyen megfelelően elvégezni azokat. A digitális működési reziliencia e rendelettel előírt tesztelésének tehát azon pénzügyi szervezetek esetében, amelyek teljesítik az e rendeletben meghatározott kritériumokat (például nagy rendszerszintű jelentőséggel bíró és IKT-érett hitelintézetek, értéktőzsdék, központi értéktárak és központi szerződő felek), más pénzügyi szervezetekhez képest szigorúbbnak kell lennie. Ugyanakkor, a digitális működési reziliencia TLPT útján történő tesztelésének az alapvető pénzügyi szolgáltatási alágazatokban (például pénzforgalom, banki tevékenység, elszámolás és kiegyenlítés) működő és rendszerszintű szerepet betöltő pénzügyi szervezetek esetében nagyobb, és más alágazatok (például eszközkezelők és hitelminősítő intézetek) esetében kisebb relevanciával kell bírnia.

(57) A határokon átnyúló tevékenységet végző és az Unióban a letelepedés vagy a szolgáltatásnyújtás szabadságát gyakorló pénzügyi szervezeteknek a székhelyük szerinti tagállamban egy egységes, fejlett tesztelési követelményrendszernek (azaz TLPT) kell megfelelniük, amelynek magában kell foglalnia az IKT-infrastruktúrákat valamennyi olyan joghatóságban, ahol a határokon átnyúló tevékenységet végző pénzügyi csoport működik az Unión belül, ily módon lehetővé téve az ilyen pénzügyi csoportok számára, hogy csak egy joghatóságban keletkezzenek kapcsolódó IKT-tesztköltségeik.

(58) Annak érdekében, hogy az egyes illetékes hatóságok korábban – mindenekelőtt a TIBER-EU keret végrehajtása tekintetében – megszerzett szakértelmét fel lehessen használni, e rendeletnek lehetővé kell tennie a tagállamok számára, hogy egyetlen hatóságot jelöljenek ki, amely nemzeti szinten a pénzügyi ágazatban valamennyi TLPT-vonatkozású ügyért felel, vagy – ilyen kijelölés hiányában – az illetékes hatóságok számára lehetővé kell tenni, hogy a TLPT-vonatkozású feladatok ellátását egy másik, pénzügyi területen működő illetékes nemzeti hatóságra ruházzák át.

(59) mivel e rendelet nem írja elő a pénzügyi szervezetek számára, hogy egyetlen fenyegetés alapú behatolási tesztelés minden kritikus vagy fontos funkcióra kiterjedjen, a pénzügyi szervezetek szabadon határozhatják meg, hogy mely és mennyi kritikus vagy fontos funkcióra terjedjen ki az ilyen teszt hatálya.

(60) Az e rendelet értelmében vett csoportos tesztelés – amely egy TLPT-ben több pénzügyi szervezet részvételét jelenti, és amelyre vonatkozóan egy harmadik fél IKT-szolgáltató közvetlenül szerződéses megállapodást köthet egy külső tesztelővel – csak akkor engedélyezhető, amennyiben a harmadik fél IKT-szolgáltató által az olyan ügyfelek, amelyek az e rendelet hatályán kívül eső szervezetek, részére nyújtott szolgáltatások minőségét vagy biztonságát, vagy az ilyen szolgáltatásokhoz kapcsolódó adatok bizalmas jellegét észszerűen várható módon káros hatás éri. A csoportos tesztelésre biztosítékoknak is kell vonatkozniuk (egyetlen kijelölt pénzügyi szervezet általi irányítás, a részt vevő pénzügyi szervezetek számának kalibrálása) annak érdekében, hogy – a TLPT e rendelet szerinti célkitűzéseinek megfelelő – szigorú tesztelési gyakorlatot biztosítsanak a részt vevő pénzügyi szervezetek számára.

(61) A vállalati szinten rendelkezésre álló belső erőforrások kihasználása érdekében e rendeletnek lehetővé kell tennie belső tesztelők igénybevételét a TLPT lefolytatása céljából, feltéve, hogy van felügyeleti jóváhagyás, nincsenek összeférhetetlenségek, és fennáll a belső és külső tesztelők rendszeres időközönkénti váltakozása (minden harmadik tesztet követően), előírva ugyanakkor azt is, hogy a TLPT során a fenyegetettséggel kapcsolatos hírszerzés szolgáltatójának minden esetben a pénzügyi szervezeten kívüli vállalkozásnak kell lennie. A TLPT elvégzésével kapcsolatos felelősségnek teljes mértékben a pénzügyi szervezetnél kell maradnia. A hatóságok által kiállított tanúsítványoknak kizárólag a kölcsönös elismerés célját kell szolgálniuk, továbbá azok nem zárhatnak ki semmi olyan IKT-kockázat kezeléséhez szükséges utókövetési intézkedést, amelynek a pénzügyi szervezet ki van téve, és nem tekinthetők a pénzügyi szervezet IKT-kockázatkezelési és -mérséklési képességei felügyeleti jóváhagyásának sem.

(62) Ahhoz, hogy biztosított legyen a pénzügyi ágazatban a harmadik féltől eredő IKT-kockázat megbízható nyomon követése, olyan elvalapú szabályok meghatározására van szükség, amelyek iránymutatásul szolgálnak a pénzügyi szervezetek számára azon kockázatok nyomon követése során, amelyek a harmadik fél IKT-szolgáltatókhoz kiszervezett funkciókkal, különösen a harmadik fél IKT-szolgáltatók által ellátott kritikus vagy fontos funkciókkal, valamint általánosabban a harmadik féltől való valamennyi IKT-függőséggel összefüggésben felmerülnek.

(63) Figyelembe véve az IKT-kockázat különböző forrásainak összetettségét, ugyanakkor a pénzügyi szolgáltatások zökkenőmentes nyújtását lehetővé tevő technológiai megoldások szolgáltatóinak nagy számát és sokféleségét is, e rendeletnek a harmadik fél IKT-szolgáltatók széles körére – köztük a felhőalapú számítástechnikai szolgáltatásokat, szoftvereket, adatelemzési szolgáltatásokat kínáló szolgáltatókra és az adatközpont-szolgáltatásokat nyújtó szolgáltatókra – kell vonatkoznia. Hasonlóképpen, mivel a pénzügyi szervezeteknek hatékonyan és koherens módon kell azonosítaniuk és kezelniük valamennyi kockázattípust, többek között a pénzügyi csoporton belül beszerzett IKT-szolgáltatásokkal összefüggésben, egyértelművé kell tenni, hogy azon vállalkozások, amelyek egy pénzügyi csoport részét képezik, és elsősorban az anyavállalatuk vagy az anyavállalatuk leányvállalatai vagy fióktelepei számára nyújtanak IKT-szolgáltatásokat, valamint azon pénzügyi szervezetek, amelyek egyéb pénzügyi szervezetek számára nyújtanak IKT-szolgáltatásokat, e rendelet értelmében szintén harmadik fél IKT-szolgáltatóknak tekintendők. Végül, tekintettel arra, hogy a pénzforgalmi szolgáltatások fejlődő piaca egyre nagyobb mértékben függ az összetett technikai megoldásoktól, valamint tekintettel a pénzforgalmi szolgáltatások és a pénzforgalmi vonatkozású megoldások újonnan megjelenő típusaira, a pénzforgalmi szolgáltatások ökoszisztémájának azon résztvevőit, amelyek fizetésfeldolgozási tevékenységet végeznek vagy fizetési infrastruktúrákat üzemeltetnek, e rendelet értelmében ugyancsak harmadik fél IKT-szolgáltatóknak kell tekinteni, kivéve a fizetési vagy értékpapír-kiegyenlítési rendszereket működtető központi bankokat, valamint az állami feladatok ellátása keretében IKT-vonatkozású szolgáltatásokat nyújtó hatóságokat.

(64) A pénzügyi szervezeteknek továbbra is mindenkor teljes felelősséggel kell tartozniuk az e rendeletben meghatározott kötelezettségeikért. A pénzügyi szervezeteknek arányos megközelítést kell alkalmazniuk a harmadik fél IKT-szolgáltatók szintjén felmerülő kockázatok arányos nyomon követésére, az IKT-vonatkozású függőségeik nagyságrendjének, összetettségének és fontosságának, továbbá a szerződéses megállapodás tárgyát képező szolgáltatások, folyamatok vagy funkciók kritikusságának vagy fontosságának kellő figyelembevételével, és végső soron a pénzügyi szolgáltatások folytonosságára és minőségére egyedi és csoportszinten gyakorolt bármely potenciális hatás körültekintő értékelése alapján.

(65) Az ilyen nyomon követés elvégzéséhez a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiai megközelítést kell alkalmazni, amelyet a pénzügyi szervezet vezető testülete a harmadik féltől eredő IKT-kockázatra vonatkozó célzott stratégia elfogadásával tesz hivatalossá, és amely a harmadik féltől való IKT-függőségek folyamatos és teljeskörű szűrésén alapul. Ahhoz, hogy a felügyeleti hatóságok fokozottabban tudatában legyenek a harmadik féltől való IKT-függőségeknek, valamint az e rendelettel létrehozott felvigyázási keretrendszerrel összefüggésben végzett munka további támogatása érdekében, valamennyi pénzügyi szervezet számára elő kell írni, hogy vezessen nyilvántartást a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételére vonatkozó valamennyi szerződéses megállapodásról. A pénzügyi felügyeletek számára lehetővé kell tenni, hogy bekérjék a teljes nyilvántartást, vagy annak egyes részeit, és így alapvető információkat szerezzenek a pénzügyi szervezetek IKT-függőségeinek szélesebb körű megértéséhez.

(66) A szerződéses megállapodások formális megkötését beható elemzésnek kell megelőznie és megalapoznia, különösen az olyan elemekre összpontosítva, mint a tervezett IKT-szerződés által támogatott szolgáltatások kritikussága vagy fontossága, a szükséges felügyeleti jóváhagyások és egyéb feltételek, az esetlegesen felmerülő koncentrációs kockázat, valamint a harmadik fél IKT-szolgáltatók kiválasztási és értékelési folyamata során a kellő gondosság alkalmazása, továbbá az esetleges összeférhetetlenségek értékelése. A kritikus vagy fontos funkciókra vonatkozó szerződéses megállapodások kapcsán a pénzügyi szervezeteknek figyelembe kell venniük, hogy a harmadik fél IKT-szolgáltatók a legfrissebb és legszigorúbb információbiztonsági szabványokat alkalmazzák-e. A szerződéses

megállapodások felmondását legalább egy sor olyan körülmény előidézheti, amely hiányosságokra enged következtetni a harmadik fél IKT-szolgáltató szintjén, így különösen a jogszabályok vagy a szerződéses feltételek jelentős megsértése, a szerződéses megállapodásokban meghatározott funkciók teljesítésének a lehetséges megváltozására utaló körülmények, a harmadik fél IKT-szolgáltató általános IKT-kockázatkezelésében mutatkozó gyengeségek jelei, vagy olyan körülmények, amelyek arra utalnak, hogy a releváns illetékes hatóság nem képes hatékonyan felügyelni a pénzügyi szervezetet.

(67) A harmadik fél IKT-szolgáltatók koncentrációs kockázata rendszerszintű hatásának kezelése érdekében e rendelet kiegyensúlyozott megoldást ösztönöz az ilyen koncentrációs kockázatra vonatkozó rugalmas és fokozatos megközelítés alkalmazásával, mivel bármely merev felső határ vagy szigorú korlátozás megállapítása akadályozhatja az üzletvitelt, és korlátozhatja a szerződési szabadságot. Azt, hogy mekkora valószínűséggel merülhet fel ilyen kockázat, a pénzügyi szervezeteknek a tervezett szerződéses megállapodásaik alapos vizsgálatával kell meg határozniuk, többek között az alvállalkozási megállapodások beható elemzésével, különösen akkor, ha azokat harmadik országban letelepedett, harmadik fél IKT-szolgáltatóval kötik. Ebben a szakaszban, a szerződési szabadság megőrzése és a pénzügyi stabilitás biztosítása közötti megfelelő egyensúly érdekében nem célszerű a harmadik féllel szembeni IKT-kockázati kitettségre vonatkozó szigorú felső határokkal és limitekkel kapcsolatos szabályokat meghatározni. A kritikus harmadik fél IKT-szolgáltatók tekintetében az e rendelet szerint kinevezett vezető felvigyázónak a felvigyázási keretrendszerrel összefüggésben különös figyelmet kell fordítania a kölcsönös függőségek mértékének megértésére, az olyan konkrét esetek feltárására, ahol a kritikus harmadik fél IKT-szolgáltatók Unión belüli magas koncentrációja valószínűleg megterheli az uniós pénzügyi rendszer stabilitását és integritását, valamint az említett konkrét kockázat azonosítása esetén párbeszédet kell folytatnia a kritikus harmadik fél IKT-szolgáltatókkal.

(68) Annak érdekében, hogy rendszeresen értékeljék és nyomon kövessék egy harmadik fél IKT-szolgáltató képességét arra, hogy a pénzügyi szervezet részére annak digitális működési rezilienciáját érő káros hatások nélkül, biztonságosan nyújtson szolgáltatásokat, a harmadik fél IKT-szolgáltatókkal kötött szerződések több kulcselemét a teljesítés egészére kiterjedően harmonizálni szükséges. Az ilyen harmonizációnak ki kell terjednie legalább azon területekre, amelyek elengedhetetlenek ahhoz, hogy a pénzügyi szervezet teljeskörűen nyomon követhesse a harmadik fél IKT-szolgáltatótól esetlegesen eredő kockázatokat a pénzügyi szervezet azon szükségletének szempontjából, hogy biztosítsa digitális rezilienciáját, mivel nagymértékben függ az igénybe vett IKT-szolgáltatások stabilitásától, funkciójától, rendelkezésre állásától és biztonságától.

(69) A szerződéses megállapodásoknak az e rendelet követelményeivel való összehangolást célzó újratárgyalása során a pénzügyi szervezeteknek és a harmadik fél IKT-szolgáltatóknak biztosítaniuk kell, hogy a megállapodások hatálya kiterjedjen az e rendeletben meghatározott főbb szerződéses rendelkezésekre.

(70) A „kritikus vagy fontos funkció” e rendeletben szereplő fogalommeghatározása magában foglalja a 2014/59/EU európai parlamenti és tanácsi irányelv ([20]) 2. cikke (1) bekezdésének 35. pontjában meghatározott „kritikus funkciókat”. Ennek megfelelően a 2014/59/EU irányelv alapján kritikusnak tekintett funkciók beletartoznak az e rendelet értelmében vett kritikus funkciók fogalommeghatározásába.

(71) A szerződéses megállapodásokban – függetlenül az IKT-szolgáltatások által támogatott funkció kritikusságától vagy fontosságától – pontosan meg kell határozni különösen a funkciók és szolgáltatások teljeskörű leírását, a funkciók teljesítésének és az adatkezelésnek a helyszíneit, valamint a szolgáltatási szintek teljeskörű leírását. Egyéb lényeges elemek annak lehetővé tételéhez, hogy a pénzügyi szervezet nyomon kövesse a harmadik féltől származó IKT-kockázatot, a következők: szerződéses rendelkezések, amelyek meghatározzák, hogy a harmadik fél IKT-szolgáltató hogyan biztosítja a személyes adatok hozzáférhetőségét, rendelkezésre állását, integritását, biztonságát és védelmét; rendelkezések, amelyek meghatározzák a harmadik fél IKT-szolgáltató fizetésképtelensége, szanálása vagy üzleti tevékenységének megszűnése esetén az adatokhoz való hozzáférést, azok behajtását és visszaszolgáltatását lehetővé tevő releváns garanciákat; rendelkezések, amelyek előírják a harmadik fél IKT-szolgáltató számára a nyújtott

([20]) Az Európai Parlament és a Tanács 2014/59/EU irányelve (2014. május 15.) a hitelintézetek és befektetési vállalkozások helyreállítását és szanálását célzó keretrendszer létrehozásáról és a 82/891/EGK tanácsi irányelv, a 2001/24/EK, 2002/47/EK, 2004/25/EK, 2005/56/EK, 2007/36/EK, 2011/35/EU, 2012/30/EU és 2013/36/EU irányelv, valamint az 1093/2010/EU és a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról (HL L 173., 2014.6.12., 190. o.).

szolgáltatásokkal kapcsolatos IKT-biztonsági események esetén a többletköltség nélkül vagy előzetesen meghatározott költség mellett történő segítségnyújtást; a harmadik fél IKT-szolgáltató azon kötelezettségére vonatkozó rendelkezések, hogy maradéktalanul együttműködjön a pénzügyi szervezet illetékes hatóságaival és szanálási hatóságaival; valamint a szerződéses megállapodások megszüntetésére vonatkozó felmondási jogokra és a kapcsolódó minimális felmondási időre vonatkozó rendelkezések, összhangban az illetékes hatóságok és a szanálási hatóságok elvárásaival.

(72) Az ilyen szerződéses rendelkezéseken túlmenően, és annak biztosítása érdekében, hogy a pénzügyi szervezetek megőrizzék a teljes kontrollt a harmadik felek szintjén bekövetkező, az IKT-biztonságukra nézve potenciálisan ártalmas valamennyi fejlemény felett, a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtására vonatkozó szerződéseknek a következőkről is rendelkezniük kell: a szolgáltatási szint teljeskörű leírásának pontos meghatározása pontos mennyiségi és minőségi teljesítménycélokkal együtt, hogy indokolatlan késedelem nélkül meg lehessen hozni a megfelelő korrekciós intézkedéseket, amennyiben az elfogadott szolgáltatási szintek nem teljesülnek; a harmadik fél IKT-szolgáltatóra vonatkozó releváns felmondási idők és a pénzügyi szervezettel szembeni adatszolgáltatási kötelezettségeik az olyan fejlemények esetén, amelyek lényeges hatást gyakorolhatnak a harmadik fél IKT-szolgáltató azon képességére, hogy eredményesen nyújtsa a vonatkozó IKT-szolgáltatásait; a harmadik fél IKT-szolgáltatóra vonatkozó azon követelmény, hogy vészhelyzeti terveket vezessen be és teszteljen, továbbá rendelkezzen olyan IKT-biztonsági intézkedésekkel, eszközökkel és szabályzatokkal, amelyek lehetővé teszik a biztonságos szolgáltatásnyújtást, valamint hogy részt vegyen és teljes mértékben együttműködjön a pénzügyi szervezet által végzett TLPT során.

(73) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtására vonatkozó szerződéseknek olyan rendelkezéseket is tartalmazniuk kell, amelyek biztosítják a pénzügyi szervezet vagy egy kinevezett harmadik fél általi hozzáférési, ellenőrzési és audit jogokat, valamint a másolatkészítés jogát, mint elengedhetetlen eszközeit annak, hogy a pénzügyi szervezet folyamatosan nyomon követhesse a harmadik fél IKT-szolgáltató teljesítését, ami egyúttal feltételezi a szolgáltató teljes mértékű együttműködését az ellenőrzések során. Hasonlóképpen, a pénzügyi szervezet illetékes hatóságának is jogosultsággal kell rendelkeznie arra, hogy értesítés alapján – a bizalmas jellegű adatok védelmére is figyelemmel – ellenőrzést és auditot végezzen a harmadik fél IKT-szolgáltatónál.

(74) Az említett szerződéses megállapodásoknak célzott kilépési stratégiákat is meg kell határozniuk, ez utóbbiakkal lehetővé téve különösen a kötelező átállási időszakokat, amelyek során a harmadik fél IKT-szolgáltatóknak folyamatosan biztosítaniuk kell a releváns szolgáltatásokat annak érdekében, hogy a zavarok pénzügyi szervezet szintjén való fellépésének a kockázata mérséklődjön, vagy a szervezet eredményesen átválthasson más harmadik fél IKT-szolgáltatók igénybevételére, vagy ehelyett saját, házon belüli megoldásokhoz folyamodhasson, a nyújtott IKT-szolgáltatás összetettségének megfelelően. A 2014/59/EU irányelv hatálya alá tartozó pénzügyi szervezeteknek továbbá biztosítaniuk kell, hogy az IKT-szolgáltatásokra vonatkozó releváns szerződések robusztus kialakításúak és az említett pénzügyi szervezetek szanálása esetén maradéktalanul érvényesíthetőek legyenek. Ezért az említett pénzügyi szervezeteknek a szanálási hatóságok elvárásaival összhangban biztosítaniuk kell, hogy az IKT-szolgáltatásokra vonatkozó releváns szerződések szanálás esetén reziliensek. Az említett pénzügyi szervezeteknek mindaddig, amíg továbbra is teljesítik fizetési kötelezettségeiket, egyéb követelmények mellett biztosítaniuk kell, hogy az IKT-szolgáltatásokra vonatkozó szerződések rendelkezéseket tartalmazzanak arra vonatkozóan, hogy szerkezetátalakítás vagy szanálás indokával a szerződés nem szüntethető meg, nem függeszthető fel, és nem módosítható.

(75) Ezenkívül, a felhőszolgáltatásokra vonatkozóan a hatóságok vagy az uniós intézmények által kidolgozott általános szerződéses rendelkezések – így különösen a Bizottság által kidolgozott szerződéses rendelkezések – önkéntes alkalmazása további garanciát nyújthat a pénzügyi szervezetek és a harmadik fél IKT-szolgáltatók számára azáltal, hogy – a pénzügyi szolgáltatásokra vonatkozó uniós jogban meghatározott követelményekkel és elvárásokkal teljes összhangban – fokozza a jogbiztonság-szintjüket a pénzügyi ágazatban igénybe vett felhőszolgáltatások tekintetében. Az általános szerződéses rendelkezések kidolgozásának alapját az azon 2018. évi pénzügyi technológiai cselekvési tervben már előirányzott intézkedések képezik, amelyben a Bizottság bejelentette a szándékát, hogy ösztönözze és elősegítse a pénzügyi szervezetek által igénybe vett kiszervezett felhőszolgáltatásokra vonatkozó általános szerződéses rendelkezések kidolgozását, támaszkodva a felhőszolgáltatásban érdekeltek azon ágazatközi erőfeszítéseire, amelyeket a pénzügyi ágazat segítségével a Bizottság elősegített.

(76) Annak érdekében, hogy előmozdítsák a pénzügyi ágazatban a harmadik féltől eredő IKT-kockázat kezelésekor alkalmazott felügyeleti megközelítések konvergenciáját és hatékonyságát, valamint megerősítsék az olyan pénzügyi szervezetek digitális működési rezilienciáját, amelyek a pénzügyi szolgáltatások nyújtását támogató IKT-szolgáltatásokat kritikus harmadik fél IKT-szolgáltatóktól veszik igénybe, és ezáltal hozzájáruljanak az uniós pénzügyi rendszer stabilitásának, valamint a pénzügyi szolgáltatások belső piaca integritásának megőrzéséhez, a kritikus harmadik fél IKT-szolgáltatóknak uniós felvigyázási keretrendszer hatálya alá kell tartozniuk. Míg a felvigyázási keretrendszer létrehozását indokolttá teszik az uniós szintű fellépés hozzáadott értéke, továbbá az IKT-

szolgáltatások pénzügyi szolgáltatásnyújtás terén történő igénybevételének velejáró szerepe és sajátosságai, emlékeztetni kell ugyanakkor arra, hogy ez a megoldás csak ezzel, a kifejezetten a pénzügyi ágazat digitális működési rezilienciájával foglalkozó rendelettel összefüggésben tűnik alkalmasnak. Egy ilyen felvigyázási keretrendszer azonban nem tekinthető új modellnek az uniós felügyelet számára a pénzügyi szolgáltatások és tevékenységek egyéb területein.

(77) A felvigyázási keretrendszer hatályának kizárólag a kritikus harmadik fél IKT-szolgáltatókra célszerű kiterjednie. Ezért be kell vezetni egy kijelölési mechanizmust, amely figyelembe veszi azt, hogy a pénzügyi ágazat milyen mértékben és jelleggel támaszkodik ilyen harmadik fél IKT-szolgáltatókra. Az említett mechanizmusnak tartalmaznia kell egy sor mennyiségi és minőségi kritériumot azon kritikussá minősítési paraméterek meghatározása céljából, amelyeken a felvigyázási keretrendszerbe foglalás alapul. Annak biztosítása érdekében, hogy ez az értékelés pontos legyen, és függetlenül a harmadik fél IKT-szolgáltató szervezeti felépítésétől, e kritériumoknak az olyan harmadik fél IKT-szolgáltatók esetében, amelyek egy nagyobb csoporthoz tartoznak, a harmadik fél teljes IKT-szolgáltatói csoport felépítését figyelembe kell venniük. Egyrészről az említett kritériumok alkalmazásával automatikusan nem kijelölt, kritikus harmadik fél IKT-szolgáltatók számára lehetővé kell tenni a felvigyázási keretrendszerben történő önkéntes részvételt, másrészről mentesíteni kell azon harmadik fél IKT-szolgáltatókat, amelyek már olyan felvigyázási mechanizmust alkotó keretek hatálya alá tartoznak, amelyek támogatják a Központi Bankok Európai Rendszerének az EUMSZ 127. cikkének (2) bekezdésében említett feladatai ellátását.

(78) Hasonlóképpen, az olyan pénzügyi szervezetek számára, amelyek más pénzügyi szervezeteknek nyújtanak IKT-szolgáltatásokat, miközben az e rendelet szerinti harmadik fél IKT-szolgáltatók kategóriájába tartoznak, szintén mentességet kell biztosítani a felvigyázási keretrendszer alól, mivel már a releváns uniós pénzügyi szolgáltatási jogszabályok által létrehozott felügyeleti mechanizmusok hatálya alá tartoznak. Az illetékes hatóságoknak a felügyeleti tevékenységeikkel összefüggésben adott esetben figyelembe kell venniük azon IKT-kockázatot, amelyet az IKT-szolgáltatásokat nyújtó pénzügyi szervezetek jelentenek a pénzügyi szervezetek számára. Hasonlóképpen, a kockázatfigyelési mechanizmusok csoportszintű meglétéből fakadóan ugyanilyen mentességet kell bevezetni az olyan harmadik fél IKT-szolgáltatók számára, amelyek túlnyomóan a saját csoportjukba tartozó szervezetek számára nyújtanak szolgáltatásokat. Az olyan harmadik fél IKT-szolgáltatókat, amelyek csak egy tagállamban nyújtanak IKT-szolgáltatásokat olyan pénzügyi szervezeteknek, amelyek tevékenységüket csak az említett tagállamban folytatják, tevékenységeik korlátozottsága és a határokon átnyúló hatás hiánya miatt szintén mentesíteni kell a kijelölési mechanizmus alól.

(79) A pénzügyi szolgáltatások területén tapasztalható digitális átalakulás következtében soha nem látott mértékűvé vált az IKT-szolgáltatások igénybevétele és az azoktól való függés. Mivel mára elképzelhetetlenné vált a felhőszolgáltatások, szoftveres megoldások és adatokkal kapcsolatos szolgáltatások igénybevétele nélküli pénzügyi szolgáltatásnyújtás, az Unió pénzügyi ökoszisztémája és bizonyos, IKT-szolgáltatók által nyújtott IKT-szolgáltatások között mostanra mély kölcsönös függőségi viszony alakult ki. Az említett szolgáltatók közül néhányan az IKT-alapú technológiák kifejlesztése és alkalmazása terén folytatott innovatori tevékenységüknél fogva jelentős szerepet töltenek be a pénzügyi szolgáltatások nyújtásában, vagy szervesen beépültek a pénzügyi szolgáltatási értékláncba. Így kritikussá váltak az uniós pénzügyi rendszer stabilitása és integritása szempontjából. Ez a kritikus harmadik fél IKT-szolgáltatók által nyújtott szolgáltatásoktól való széles körű függés – a különböző piaci szereplők információs rendszerei közötti kölcsönös függőséggel kombinálva – közvetlen és potenciálisan súlyos kockázatot jelent az Unió pénzügyi szolgáltatási rendszerére és a pénzügyi szolgáltatások nyújtásának folytonosságára nézve, ha a kritikus harmadik fél IKT-szolgáltatókat működési zavarok vagy jelentős kiberbiztonsági események érintenék. A kiberbiztonsági események egyik feltűnő képessége az, hogy a pénzügyi ágazatban figyelemmel kísért egyéb típusú kockázatoknál lényegesen gyorsabb ütemben sokszorozódhatnak és terjedhetnek a pénzügyi rendszerben, valamint átnyúlhatnak más ágazatokba és a földrajzi határokon túl is. Az ilyen események potenciálisan rendszerszintű válsággá szélesedhetnek, amennyiben megkopik a pénzügyi rendszerbe vetett bizalom a reálgazdaságot támogató funkciók zavara vagy jelentős pénzügyi veszteségek miatt, és ez olyan szintet ér el, amelyet a pénzügyi rendszer már nem bír el, vagy amely erőteljes sokkhatás-elnyelő intézkedéseket tesz szükségessé. Annak érdekében, hogy ilyen helyzetek ne következhessenek be – veszélyeztetve az Unió pénzügyi stabilitását és integritását –, alapvető fontosságú biztosítani a pénzügyi területen fennálló, harmadik féltől eredő IKT-kockázattal kapcsolatos felügyeleti gyakorlatok közötti konvergenciát, így különösen olyan új szabályok révén, amelyek lehetővé teszik a kritikus harmadik fél IKT-szolgáltatók feletti uniós szintű felvigyázást.

(80) A felvigyázási keretrendszer jelentős részben függ attól, hogy milyen mértékű az együttműködés a vezető felvigyázó és a pénzügyi szervezetek számára a pénzügyi szolgáltatások nyújtását befolyásoló szolgáltatásokat nyújtó, kritikus harmadik fél IKT-szolgáltató között. A felvigyázás sikere többek között a vezető felvigyázó azon képességén múlik, hogy hatékonyan el tudja-e végezni a kritikus harmadik fél IKT-szolgáltatók által alkalmazott szabályok, kontrollok és folyamatok értékelését célzó nyomonkövetési missziókat és ellenőrzéseket, továbbá fel tudja-e mérni az e szolgáltatók tevékenységei által a pénzügyi stabilitásra és a pénzügyi rendszer integritására gyakorolt potenciális kumulatív hatást. Kritikus jelentőségű ugyanakkor, hogy a kritikus harmadik fél IKT-szolgáltatók kövessék a vezető felvigyázó által megfogalmazott ajánlásokat, és megoldást találjanak az általa felvetett aggályokra. Mivel az együttműködés hiánya – így például a telephelyeire való belépés vagy az információszolgáltatás megtagadása – valamely, olyan szolgáltatásokat nyújtó, kritikus harmadik fél IKT-szolgáltató részéről, amelyek befolyásolják a pénzügyi szolgáltatások nyújtását, végső soron megfosztaná a vezető felvigyázót a harmadik féltől eredő IKT-kockázat felmérését lehetővé tevő alapvető eszközeitől, és káros hatásokkal járhatna a pénzügyi stabilitásra és a pénzügyi rendszer integritására nézve, szükséges rendelkezni egy arányos szankciórendszerről is.

(81) Mindezt szem előtt tartva, azon igényt, hogy a vezető felvigyázó a kritikus harmadik fél IKT-szolgáltatókat az e rendeletben meghatározott átláthatósági és hozzáféréssel kapcsolatos kötelezettségek teljesítésére kötelező büntető bírságokat szabhasson ki, nem veszélyeztethetik olyan nehézségek, amelyek az említett bírságoknak a harmadik országbeli székhellyel rendelkező, kritikus harmadik fél IKT-szolgáltatókkal szembeni végrehajtásából fakadnak. Az említett bírságok végrehajthatóságának biztosítása érdekében, valamint hogy gyorsan foganatosítani lehessen a kijelölési mechanizmussal és az ajánlások kibocsátásával összefüggésben a kritikus harmadik fél IKT-szolgáltatók védelemhez való jogának érvényesítését szolgáló eljárásokat, azon kritikus harmadik fél IKT-szolgáltatókat, amelyek pénzügyi szervezetek számára a pénzügyi szolgáltatások nyújtását befolyásoló szolgáltatásokat nyújtanak, kötelezni kell arra, hogy megfelelő üzleti jelenléttel rendelkezzenek az Unióban. A felvigyázás jellegéből és abból fakadóan, hogy más joghatóságokban nincs ezzel összehasonlítható szabályozás, nem állnak rendelkezésre olyan alternatív mechanizmusok, amelyek alkalmasak arra, hogy e célkitűzés elérését a harmadik országbeli pénzügyi felügyeletekkel történő hatékony együttműködés útján biztosítsák az olyan rendszerszintű jelentőséggel bíró harmadik fél IKT-szolgáltatók által képviselt digitális működési kockázatok hatásának figyelemmel kísérése vonatkozásában, amelyek harmadik országban letelepedett kritikus harmadik fél IKT-szolgáltatóknak minősülnek. Ezért egy olyan, harmadik országban letelepedett, harmadik fél IKT-szolgáltatónak, amelyet e rendelet értelmében kritikusnak jelöltek ki, ahhoz, hogy az Unióban továbbra is nyújthasson IKT-szolgáltatásokat pénzügyi szervezeteknek, az ekként való kijelölése időpontjától számított 12 hónapon belül minden szükséges lépést meg kell tennie – az uniós vívmányokban mindenütt alkalmazott, nevezetesen a 2013/34/EU európai parlamenti és tanácsi irányelvben ([21]) foglalt fogalommeghatározás szerinti leányvállalat létrehozása révén – az Unióban történő bejegyeztetése céljából.

(82) A leányvállalat Unióban való létrehozásának követelménye nem jelenti azt, hogy a kritikus harmadik fél IKT-szolgáltató nem nyújthat IKT-szolgáltatásokat és azokhoz kapcsolódó technikai támogatást az Unión kívül található létesítményekből és infrastruktúra révén. E rendelet nem ír elő adatlokalizálási kötelezettséget, mivel nem teszi kötelezővé, hogy az adattárolást- vagy kezelést az Unióban kell végezni.

(83) A kritikus harmadik fél IKT-szolgáltatók számára lehetővé kell tenni, hogy a világon bárhonnan tudjanak IKT-szolgáltatásokat nyújtani, vagyis nem szükségszerűen vagy nem csak az Unióban található telephelyekről. A felvigyázási tevékenységeket először az Unióban található telephelyeken, az Unióban található gazdasági szereplőkkel való kapcsolatfelvétel útján kell elvégezni – ideértve a kritikus harmadik fél IKT-szolgáltatók által az e rendelet szerint létrehozott leányvállalatokat is. Az ilyen, Unión belüli intézkedések azonban kevésnek bizonyulhatnak ahhoz, hogy a vezető felvigyázó maradéktalanul és hatékonyan el tudja látni az e rendelet szerinti feladatait. A vezető felvigyázónak ezért jogosultnak kell lennie a megfelelő felvigyázási hatáskörei harmadik országokban való gyakorlására is. Az említett hatáskörök harmadik országokban való gyakorlása keretében a vezető felvigyázónak meg kell tudnia vizsgálni azon létesítményeket, amelyekből a kritikus harmadik fél IKT-szolgáltató az IKT-szolgáltatásokat vagy a technikai támogató szolgáltatásokat ténylegesen nyújtja vagy irányítja, továbbá átfogó és operatív szintű átlátásra kell tudnia szert tenni a kritikus harmadik fél IKT-szolgáltató IKT-kockázatkezeléséről. A vezető felvigyázó uniós hivatalként történő, az Unió területén kívüli hatáskörgyakorlásának a lehetőségét megfelelően feltételekhez kell kötni – mindenekelőtt az érintett kritikus harmadik fél IKT-szolgáltató

([21]) Az Európai Parlament és a Tanács 2013/34/EU irányelve (2013. június 26.) a meghatározott típusú vállalkozások éves pénzügyi kimutatásairól, összevont (konszolidált) éves pénzügyi kimutatásairól és a kapcsolódó beszámolókról, a 2006/43/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 78/660/EGK és a 83/349/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 182., 2013.6.29., 19. o.).

hozzájárulásához. Hasonlóképpen feltétel, hogy a harmadik ország releváns hatóságait tájékoztassák a vezető felvigyázó tevékenységeinek a területükön történő gyakorlásáról, és hogy azok ne emeljenek kifogást. A hatékony végrehajtás biztosítása érdekében azonban – valamint az uniós intézmények és a tagállamok vonatkozó hatásköreinek sérelme nélkül – az ilyen hatásköröket az érintett harmadik ország releváns hatóságaival igazgatási együttműködési megállapodások megkötése révén teljeskörűen rögzíteni is kell. E rendeletben ezért lehetővé kell tenni az EFH-k számára, hogy a megfelelő harmadik országbeli hatóságokkal igazgatási együttműködési megállapodásokat kössenek, amelyek egyébként nem keletkeztethetnek az Unió és tagállamai vonatkozásában jogi kötelezettségeket.

(84) A vezető felvigyázóval való kommunikáció megkönnyítése és a megfelelő képviselet biztosítása érdekében azon kritikus harmadik fél IKT-szolgáltatóknak, amelyek valamely csoport tagjai, ki kell jelölniük egy jogi személyt a koordinációs pontjuk szerepének betöltésére.

(85) A felvigyázási keretrendszer nem sértheti a tagállamok azon hatáskörét, hogy lefolytassák saját felvigyázási vagy nyomonkövetési misszióikat azon harmadik fél IKT-szolgáltatók tekintetében, amelyeket e rendelet alapján nem jelöltek ki kritikusként, de amelyeket nemzeti szinten jelentősnek tekintenek.

(86) A pénzügyi szolgáltatások területét jellemző többrétegű intézményi struktúra kihasználása érdekében az EFH-k vegyes bizottságának – a kiberbiztonsággal kapcsolatos feladataival összhangban – továbbra is biztosítania kell az általános ágazatközi koordinációt az IKT-kockázatot érintő valamennyi kérdésben. Ennek során a vegyes bizottságot egy új albizottságnak kell támogatnia (a továbbiakban: a felvigyázási fórum), amely ellátja mind a kritikus harmadik fél IKT-szolgáltatókat érintő egyedi döntésekhez, mind a kollektív ajánlások kibocsátásához szükséges előkészítő munkát, különösen a kritikus harmadik fél IKT-szolgáltatókra vonatkozó felvigyázási programok összehasonlító teljesítményértékelése és az IKT-koncentrációs kockázattal kapcsolatos kérdéseket kezelő legjobb gyakorlatok azonosítása kapcsán.

(87) Annak biztosítása céljából, hogy a kritikus harmadik fél IKT-szolgáltatókra vonatkozóan megfelelő és hatékony uniós szintű felvigyázás érvényesüljön, e rendelet úgy rendelkezik, hogy a három EFH bármelyike kijelölhető vezető felvigyázóként. Az egyes konkrét kritikus harmadik fél IKT-szolgáltatókat annak értékelése alapján kell hozzárendelni a három EFH valamelyikéhez, hogy túlnyomóan milyen pénzügyi szervezetek működnek az említett EFH felelősségi körébe tartozó pénzügyi ágazatokban. E megközelítésnek a feladatoknak és a felelősségi köröknek a három EFH közötti kiegyensúlyozott elosztását kell eredményeznie a felvigyázási funkciók ellátása tekintetében, valamint biztosítania kell a három hatóságnál rendelkezésre álló emberi erőforrások és technikai szakértelem lehető legjobb kihasználását.

(88) A vezető felvigyázók számára biztosítani kell a vizsgálatok lefolytatásához, a kritikus harmadik fél IKT-szolgáltatók telephelyein és helyszínein a helyszíni és a helyszínen kívüli ellenőrzések elvégzéséhez, valamint a hiánytalan és naprakész információk beszerzéséhez szükséges hatásköröket. Az említett hatásköröknek képessé kell tenniük a vezető felvigyázót arra, hogy tényleges betekintést nyerjen a pénzügyi szervezeteket – és végső soron az Unió pénzügyi rendszerét – érintő, harmadik felektől eredő IKT-kockázat típusába, dimenziójába és hatásába. Az EFH-k vezető felvigyázási szereppel való felruházása szükséges előfeltétele az IKT-kockázat rendszerszintű dimenziója megértésének és kezelésének pénzügyi téren. A kritikus harmadik fél IKT-szolgáltatók által az uniós pénzügyi ágazatra gyakorolt hatás és az ezzel járó IKT-koncentrációs kockázat által okozott potenciális problémák miatt uniós szintű kollektív megközelítés alkalmazására van szükség. Ha számos illetékes hatóság párhuzamosan gyakorol többféle ellenőrzési és hozzáférési jogot egymástól elkülönülten, kismértékű egymás közötti koordináció mellett vagy annak teljes hiányában, az megakadályozná, hogy a pénzügyi felügyeletek teljes és átfogó áttekintésre tegyenek szert az Unióban meglévő, harmadik felektől eredő IKT-kockázatot illetően, ugyanakkor a kritikus harmadik fél IKT-szolgáltatók számára redundanciát, megterhelést és bonyolultságot is jelentene, ha számos nyomonkövetési és ellenőrzési kérés vonatkozna rájuk.

(89) Tekintettel arra, hogy a kritikusként való kijelölés jelentős hatásokkal jár, e rendelettel biztosítani kell a kritikus harmadik fél IKT-szolgáltatók jogainak a felvigyázási keretrendszer végrehajtása során történő tiszteletben tartását. Az ilyen szolgáltatóknak a kritikusként való kijelölésüket megelőzően például joguk kell, hogy legyen ahhoz, hogy a vezető felvigyázóhoz indokolással ellátott nyilatkozatot nyújtsanak be, amely tartalmaz minden, a kijelölésükkel kapcsolatos értékelés céljából releváns információt. Mivel a vezető felvigyázónak felhatalmazással kell rendelkeznie az IKT-kockázatot érintő kérdésekről és azok megfelelő korrekciós intézkedéseiről szóló ajánlások benyújtására, ami magában foglalja azon jogkört is, hogy kifogást emeljen bizonyos olyan szerződéses megállapodásokkal szemben, amelyek végső soron hátrányosan érintik valamely pénzügyi szervezet vagy a pénzügyi rendszer stabilitását, a kritikus harmadik fél IKT-szolgáltatók számára is biztosítani kell a lehetőséget, hogy az említett ajánlások véglegesítését megelőzően magyarázatot adjanak az ajánlásokban előirányzott megoldások várható hatásait illetően

az olyan ügyfelekre nézve, amelyek az e rendelet hatályán kívül eső szervezetek, és megoldásokat fogalmazzanak meg a kockázatok csökkentése érdekében. Az ajánlásokkal egyet nem értő, kritikus harmadik fél IKT-szolgáltatóknak indokolással ellátott magyarázatot kell benyújtaniuk az ajánlás jóvá nem hagyására irányuló szándékukról. Amennyiben nem nyújtanak be ilyen, indokolással ellátott magyarázatot, vagy az elégtelennek bizonyul, a vezető felvigyázónak nyilvános hirdetményt kell kiadnia, amelyben összefoglalva ismerteti a meg nem felelési ügyet.

(90) Az illetékes hatóságoknak a vezető felvigyázó által kibocsátott ajánlásoknak való érdemi megfelelés ellenőrzési feladatát megfelelően bele kell foglalniuk a pénzügyi szervezetek prudenciális felügyeletével kapcsolatos feladatkörükbe. Az illetékes hatóságoknak hatáskörrel kell rendelkezniük arra, hogy a vezető felvigyázó ajánlásaiban megjelölt kockázatok kezelése céljából további intézkedések megtételére kötelezzék a pénzügyi szervezeteket, és az illetékes hatóságoknak kellő időben ki kell adniuk erre irányuló értesítéseiket. Amikor a vezető felvigyázó olyan, kritikus harmadik fél IKT-szolgáltatóknak címzett ajánlásokat ad ki, amelyek az (EU) 2022/2555 irányelv szerinti felügyelet alá tartoznak, az illetékes hatóságoknak hatáskörrel kell rendelkezniük arra, hogy a további intézkedések megtétele előtt önkéntes alapon konzultáljanak az említett irányelv szerinti illetékes hatóságokkal annak érdekében, hogy elősegítsék a szóban forgó, kritikus harmadik fél IKT-szolgáltatókkal kapcsolatban a koordinált megközelítés mentén való ügyintézést.

(91) A felvigyázás gyakorlása során három operatív elvnek kell érvényesülnie, törekedve a következők biztosítására: a) szoros koordináció az EFH-k között vezető felvigyázási szerepük ellátásával összefüggésben, egy közös felvigyázási hálózaton (KFH) keresztül; b) összhang az (EU) 2022/2555 irányelv által létrehozott kerettel (az említett irányelv szerinti szervek közötti önkéntes konzultáció révén, a kritikus harmadik fél IKT-szolgáltatókra irányuló intézkedések közötti átfedések elkerülése érdekében); és c) gondosság alkalmazása a kritikus harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások zavaraival kapcsolatos, olyan ügyfeleket érintő potenciális kockázatok minimalizálása érdekében, amelyek nem tartoznak e rendelet hatálya alá.

(92) A felvigyázási keretrendszer nem válthatja ki, vagy semmilyen módon és semmilyen részben nem helyettesítheti a pénzügyi szervezetekkel szembeni azon követelményt, hogy a harmadik fél IKT-szolgáltatók igénybevételével járó kockázatok kezeléséről maguk gondoskodjanak, ideértve azon kötelezettségüket, hogy fenntartsák a kritikus harmadik fél IKT-szolgáltatókkal létrejött szerződéses megállapodásaik folyamatos monitorozását. Hasonlóképpen, a felvigyázási keretrendszer nem érintheti a pénzügyi szervezetek azon teljes felelősségét, hogy megfeleljenek az e rendeletben és a pénzügyi szolgáltatásokra vonatkozó releváns jogszabályokban megállapított valamennyi jogi kötelezettségnek, és teljesítsék azokat.

(93) A párhuzamosságok és átfedések elkerülése érdekében az illetékes hatóságoknak tartózkodniuk kell olyan intézkedések egyenkénti meghozatalától, amelyek a kritikus harmadik fél IKT-szolgáltatók kockázatainak nyomon követésére irányulnak, és e tekintetben a vezető felvigyázó releváns értékelésére kell támaszkodniuk. A felvigyázási keretrendszerbe tartozó feladatok ellátásával összefüggésben minden intézkedést minden esetben egyeztetni kell a vezető felvigyázóval, és vele azokról előzetesen meg kell állapodni.

(94) A harmadik fél IKT-szolgáltatók digitáliskockázat-kezelésének felülvizsgálatával és nyomon követésével kapcsolatos bevált módszerek alkalmazása terén a nemzetközi konvergencia előmozdítása érdekében az EFH-kat arra kell ösztönözni, hogy kössenek együttműködési megállapodásokat a releváns, felügyeletet és szabályozást ellátó harmadik országbeli hatóságokkal.

(95) Az illetékes hatóságoknál, a három EFH-nál és – önkéntességi alapon – az (EU) 2022/2555 irányelv szerinti illetékes hatóságoknál működési és IKT-kockázatra szakosodott személyzet konkrét kompetenciáinak, technikai készségeinek és szakértelmének hasznosítása céljából a vezető felvigyázónak a nemzeti felügyeletek képességeire és tudására kell támaszkodnia, és célzott vizsgálócsoportokat kell létrehoznia minden egyes, kritikus harmadik fél IKT-szolgáltató tekintetében, multidiszciplináris csoportokat alkotva a felvigyázási tevékenységek előkészítésének és végrehajtásának a támogatására, ideértve az általános vizsgálatokat és a kritikus harmadik fél IKT-szolgáltatóknál végzett ellenőrzéseket is, valamint annak bármely szükséges utókövetése céljából.

(96) Míg a felvigyázási feladatokhoz kapcsolódó költségeket teljes mértékben a kritikus harmadik fél IKT-szolgáltatóknak felszámított díjak fedeznék, valószínű azonban, hogy az EFH-knál még a felvigyázási keretrendszer beindítása előtt felmerülnek olyan költségek, amelyek a jövőbeli felvigyázási tevékenységet támogató célzott IKT-rendszerek bevezetésével kapcsolatosak, mivel először ki kell alakítani és telepíteni kell célzott IKT-rendszereket. E rendelet ezért hibrid finanszírozási modell alkalmazását írja elő, ahol a felvigyázási keretrendszert magát teljes egészében díjakból kellene finanszírozni, míg az EFH-k IKT-rendszereinek kialakítását az Unió és az illetékes nemzeti hatóságok hozzájárulásaiból finanszíroznák.

(97) Az illetékes hatóságoknak rendelkezniük kell minden olyan felügyeleti, vizsgálati és szankcionálási hatáskörrel, amely az e rendelet szerinti feladataik ellátásához szükséges. Az általuk kiszabott közigazgatási szankciókról alapszabályként értesítést kell közzétenniük. Mivel a pénzügyi szervezetek és a harmadik fél IKT-szolgáltatók székhelye különböző tagállamokban is lehet, és azok különböző illetékes hatóságok felügyelete alá tartozhatnak, e rendelet alkalmazását meg kell könnyíteni egyfelől azáltal, hogy a releváns illetékes hatóságok szorosan együttműködnek egymással – ideértve az 1024/2013/EU tanácsi rendelettel ráruházott külön feladatok tekintetében az EKB-t is –, és másfelől azáltal, hogy konzultálnak az EFH-kkal a kölcsönös információcsere és a releváns felügyeleti tevékenységekkel összefüggésben történő segítségnyújtás révén.

(98) A kritikus harmadik fél IKT-szolgáltatókként való kijelöléséhez alapul szolgáló kritériumok mennyiségi és minőségi szempontjainak részletesebb meghatározása, valamint a felvigyázási díjak harmonizálása céljából a Bizottságot az EUMSZ 290. cikkével összhangban fel kell hatalmazni jogi aktusok elfogadására abból a célból, hogy e rendeletet kiegészítse a következők részletes meghatározása érdekében: egy harmadik fél IKT-szolgáltató meghibásodása vagy működési kiesése milyen rendszerszintű hatással jár azon pénzügyi szervezetekre nézve, amelyeknek IKT-szolgáltatásait nyújtja; azon globális rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények száma, amelyek a szóban forgó harmadik fél IKT-szolgáltatóra támaszkodnak; az adott piacon aktív harmadik fél IKT-szolgáltatók száma; mekkora költségekkel jár az adatok és az IKT-feladatok egy harmadik fél másik IKT-szolgáltatóhoz való átvitele; valamint a felvigyázási díjak összege, és a megfizetésük előírt módja. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban ([22]) megállapított elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlamentnek és a Tanácsnak a tagállamok szakértőivel egyidejűleg kell kézhez kapnia minden dokumentumot, és szakértőik számára lehetővé kell tenni a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein való rendszeres részvételt.

(99) A szabályozástechnikai standardoknak biztosítaniuk kell az e rendeletben megállapított követelmények következetes harmonizálását. Jelentős szakértelemmel rendelkező szervként betöltött szerepkörük részeként az EFH-knak kell kidolgozniuk azon Bizottság részére benyújtandó szabályozástechnikai standardtervezeteket, amelyek nem járnak szakpolitikai döntéshozatallal. Szabályozástechnikai standardokat kell kidolgozni az IKT-kockázatkezelés, a jelentős IKT-vonatkozású események bejelentése, tesztelése terén, valamint a harmadik féltől eredő IKT-kockázat megbízható nyomon követésére vonatkozó alapkövetelményekkel kapcsolatban. A Bizottságnak és az EFH-knak biztosítaniuk kell, hogy az említett standardokat és követelményeket valamennyi pénzügyi szervezet olyan módon tudja alkalmazni, amely arányban áll a méretével és általános kockázati profiljával, valamint szolgáltatásai, tevékenységei és műveletei jellegével, nagyságrendjével és összetettségével. A Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikke szerinti felhatalmazáson alapuló jogi aktusok útján, valamint az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban elfogadja az említett szabályozás-technikai standardokat.

(100) A jelentős IKT-vonatkozású eseményekkel és a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekkel kapcsolatos bejelentések összehasonlíthatóságának megkönnyítése érdekében, valamint a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokkal kapcsolatos átláthatóság biztosítása céljából az EFH-knak végrehajtás-technikai standardtervezeteket kell kidolgozniuk a jelentős IKT-vonatkozású eseményeknek és a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményeknek a pénzügyi szervezetek általi bejelentésére szolgáló egységes mintadokumentumok, űrlapok és eljárások, továbbá az információk nyilvántartásához szükséges egységes mintadokumentumok létrehozása céljából. Az említett standardok kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint a szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét. A Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 291. cikke szerinti végrehajtási jogi aktusok útján, valamint az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az említett végrehajtás-technikai standardokat.

([22]) HL L 123., 2016.5.12., 1. o.

(101) mivel korábban már sor került további követelmények felhatalmazáson alapuló és végrehajtási jogi aktusok útján történő meghatározására az 1060/2009/EK ([23]), a 648/2012/EU ([24]), a 600/2014/EU ([25]) és a 909/2014/EU ([26]) európai parlamenti és tanácsi rendeletben foglalt szabályozás-technikai és végrehajtás-technikai standardok alapján, helyénvaló felhatalmazni az EFH-kat, hogy akár önállóan, akár a vegyes bizottság keretében együttesen szabályozás-technikai és végrehajtás-technikai standardokat terjesszenek a Bizottság elé azon felhatalmazáson alapuló és végrehajtási jogi aktusok elfogadása céljából, amelyek továbbviszik és aktualizálják a meglévő IKT-kockázatkezelési szabályokat.

(102) mivel ez a rendelet az (EU) 2022/2556 európai parlamenti és tanácsi irányelvvel ([27]) együtt maga után vonja a pénzügyi szolgáltatásokra vonatkozó uniós vívmányok számos rendeletében és irányelvében, többek között az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU és a 909/2014/EU rendeletben, valamint az (EU) 2016/1011 ([28]) európai parlamenti és tanácsi rendeletben foglalt, az IKT-kockázatkezelésre vonatkozó rendelkezések egységes szerkezetbe foglalását, a teljes következetesség biztosítása érdekében az említett rendeleteket módosítani kell annak egyértelművé tétele céljából, hogy az alkalmazandó, IKT-kockázatkezeléssel kapcsolatos rendelkezéseket e rendelet állapítja meg.

(103) Következésképpen az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendeletben a működési kockázattal kapcsolatos azon releváns cikkek hatályát, amelyek a felhatalmazáson alapuló és a végrehajtási jogi aktusok elfogadására vonatkozó felhatalmazást tartalmazták, le kell szűkíteni annak érdekében, hogy e rendeletbe kerüljenek át mindazon rendelkezések, amelyek jelenleg az említett rendeletek részét képező, a digitális működési rezilienciával kapcsolatos aspektusokat szabályozzák.

(104) A fizetési rendszerek működtetését és a fizetésfeldolgozási tevékenységek ellátását lehetővé tevő IKT-infrastruktúrák használatával kapcsolatos potenciális rendszerszintű kiberkockázatokat uniós szinten megfelelően kezelni kell a digitális működési rezilienciára vonatkozó harmonizált szabályok útján. E célból a Bizottságnak mielőbb fel kell mérnie, hogy szükség van-e e rendelet hatályának felülvizsgálatára – amely felülvizsgálat egyúttal összehangolandó az (EU) 2015/2366 irányelvben előirányzott átfogó felülvizsgálat eredményével. Az elmúlt évtizedben elkövetett számos nagyszabású támadás mutatja, hogyan váltak a fizetési rendszerek a kiberfenyegetéseknek kitetté. Mivel központi helyzetben vannak a pénzforgalmi szolgáltatási láncban, és erőteljesen összekapcsolódnak az általános pénzügyi rendszerrel, a fizetési rendszerek és a fizetésfeldolgozási tevékenységek kritikus jelentőségre tettek szert az uniós pénzügyi piacok működése szempontjából. Az ilyen rendszerek elleni kibertámadások súlyos működési zavarokat okozhatnak az üzletmenetben, amelyek közvetlenül kihathatnak a legfőbb gazdasági funkciókra – így például a fizetések megkönnyítésére –, és a kapcsolódó gazdasági folyamatokra közvetett hatást gyakorolhatnak. Amíg létre nem jön egy harmonizált rendszer, és meg nem valósul a fizetésirendszer-üzemeltetők és a fizetésfeldolgozó szervezetek feletti uniós szintű felügyelet, a tagállamok – hasonló piaci gyakorlatok alkalmazása céljából – a saját joghatóságuk alatt felügyelt fizetésirendszer-üzemeltetőkre és fizetésfeldolgozó szervezetekre vonatkozó szabályok alkalmazásakor inspirációt nyerhetnek az e rendelettel meghatározott, a digitális működési rezilienciára vonatkozó követelményekből.

([23]) Az Európai Parlament és a Tanács 1060/2009/EK rendelete (2009. szeptember 16.) a hitelminősítő intézetekről (HL L 302., 2009.11.17., 1. o.).

([24]) 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.).

([25]) 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.).

([26]) 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 a 98/26/EK és a 2014/65/EU irányelv, valamint a 236/2012/EU rendelet módosításáról (HL L 257., 2014.8.28., 1. o.).

([27]) Az Európai Parlament és a Tanács (EU) 2022/2556 irányelve (2022. december 14.) a 2009/65/EK, 2009/138/EK, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 és (EU) 2016/2341 irányelvnek a pénzügyi ágazat digitális működési rezilienciája tekintetében történő módosításáról (lásd e Hivatalos Lap 153. oldalát).

([28]) Az Európai Parlament és a Tanács (EU) 2016/1011 rendelete (2016. június 8.) a pénzügyi eszközökben és pénzügyi ügyletekben referenciamutatóként vagy a befektetési alapok teljesítményének méréséhez felhasznált indexekről, valamint a 2008/48/EK és a 2014/17/EU irányelv, továbbá az 596/2014/EU rendelet módosításáról (HL L 171., 2016.6.29., 1. o.).

(105) mivel e rendelet célját – nevezetesen a szabályozott pénzügyi szervezetek számára magas szintű digitális működési reziliencia megvalósítását – a tagállamok nem tudják kielégítően megvalósítani, mert az számos különböző uniós és nemzeti jogszabály harmonizálását követeli meg, az Unió szintjén azonban e cél nagyságrendje és hatása miatt jobban megvalósítható, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.

(106) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([29]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2021. május 10-én véleményt nyilvánított ([30]),

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

Általános rendelkezések

1. cikk

Tárgy

(1) Az egységesen magas szintű digitális működési reziliencia elérése érdekében e rendelet egységes követelményeket állapít meg a pénzügyi szervezetek üzleti folyamatait támogató hálózati és információs rendszerek biztonságára vonatkozóan, a következők szerint:

a) a pénzügyi szervezetekre a következőkkel kapcsolatban alkalmazandó követelmények:

   i. az információs és kommunikációs technológiák (IKT) kockázatkezelése;

   ii. a jelentős IKT-vonatkozású események bejelentése és a jelentős kiberfenyegetésekre vonatkozó – önkéntes alapon történő – értesítés az illetékes hatóságok felé;

   iii. a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményeknek a 2. cikk (1) bekezdésének a)–d) pontjában említett pénzügyi szervezetek általi bejelentése az illetékes hatóságoknál;

   iv. a digitális működési reziliencia tesztelése;

   v. a kiberfenyegetésekkel és sérülékenységekkel kapcsolatos információk és hírszerzés megosztása;

   vi. a harmadik féltől eredő IKT-kockázat megbízható kezelését célzó intézkedések;

b) a harmadik fél IKT-szolgáltatók és a pénzügyi szervezetek között létrejött szerződéses megállapodásokkal kapcsolatos követelmények;

c) a pénzügyi szervezetek részére szolgáltatást nyújtó, kritikus harmadik fél IKT-szolgáltatók tekintetében a felvigyázási keretrendszer létrehozására és végzésére vonatkozó szabályok;

d) az illetékes hatóságok közötti együttműködés szabályai, valamint az illetékes hatóságok felügyeleti és végrehajtási tevékenységére vonatkozó szabályok az e rendeletben szabályozott kérdésekben.

(2) Az (EU) 2022/2555 irányelv 3. cikkét átültető nemzeti szabályok értelmében alapvető vagy fontos szervezetként azonosított pénzügyi szervezetek tekintetében ez a rendelet az említett irányelv 4. cikkének alkalmazásában ágazatspecifikus uniós jogi aktusnak minősül.

(3) E rendelet nem érinti a tagállamoknak a közbiztonságra, védelemre és nemzetbiztonságra vonatkozó alapvető állami funkciók tekintetében az uniós joggal összhangban fennálló felelősségét.

([29]) 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.).

([30]) HL C 229., 2021.6.15., 16. o.

2. cikk

Hatály

(1) A (3) és a (4) bekezdés sérelme nélkül, e rendelet a következő jogalanyokra alkalmazandó:

a) hitelintézetek;

b) pénzforgalmi intézmények, ideértve az (EU) 2015/2366 irányelv alapján mentességet élvező pénzforgalmi intézményeket is;

c) számlainformációkat összesítő szolgáltatók;

d) elektronikuspénz-kibocsátó intézmények, ideértve a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézményeket is;

e) befektetési vállalkozások;

f) a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról szóló európai parlamenti és tanácsi rendelet (a továbbiakban: a kriptoeszközök piacairól szóló rendelet) alapján engedélyezett kriptoeszköz-szolgáltatók, valamint az eszközalapú tokenek kibocsátói;

g) központi értéktárak;

h) központi szerződő felek;

i) kereskedési helyszínek;

j) kereskedési adattárak;

k) alternatívbefektetésialap-kezelők;

l) alapkezelő társaságok;

m) adatszolgáltatók;

n) biztosítók és viszontbiztosítók;

o) biztosításközvetítők, viszontbiztosítás-közvetítők és a kiegészítő biztosításközvetítői tevékenységet végző személyek;

p) foglalkoztatói nyugellátást szolgáltató intézmények;

q) hitelminősítő intézetek;

r) kritikus referenciamutatók kezelői;

s) közösségi finanszírozási szolgáltatók;

t) értékpapírosítási adattárak;

u) harmadik fél IKT-szolgáltatók.

(2) E rendelet alkalmazásában az (1) bekezdés a)–t) pontjában említett szervezetek együttes megnevezése: „pénzügyi szervezetek”.

(3) Ez a rendelet nem alkalmazandó a következőkre:

a) a 2011/61/EU irányelv 3. cikkének (2) bekezdésében említett alternatívbefektetésialap-kezelők;

b) a 2009/138/EK irányelv 4. cikkében említett biztosítók és viszontbiztosítók;

c) olyan nyugdíjkonstrukciókat működtető foglalkoztatói nyugellátást szolgáltató intézmények, amely nyugdíjkonstrukciók összesen nem rendelkeznek tizenötnél több taggal;

d) a 2014/65/EU irányelv 2. és 3. cikke alapján mentességet élvező természetes vagy jogi személyek;

e) mikrovállalkozásnak vagy kis- vagy középvállalkozásnak minősülő biztosításközvetítők, viszontbiztosítás-közvetítők és kiegészítő biztosításközvetítői tevékenységet végző személyek;

f) a 2013/36/EU irányelv 2. cikke (5) bekezdésének 3. pontjában említett postai elszámolóközpontok.

(4) A tagállamok kizárhatják e rendelet hatálya alól a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett, saját területükön található jogalanyokat. Amennyiben valamely tagállam él az ilyen lehetőséggel, arról – valamint az ezzel kapcsolatos minden későbbi változásról is – tájékoztatja a Bizottságot. A Bizottság honlapján vagy egyéb könnyű hozzáférést biztosító úton nyilvánosságra hozza az említett információkat.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „digitális működési reziliencia”: a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja működési integritását és megbízhatóságát azáltal, hogy harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások igénybevételével közvetlenül vagy közvetetten biztosítja azon hálózati és információs rendszerek biztonságának kezeléséhez szükséges IKT-vonatkozású képességek teljes körét, amelyeket a pénzügyi szervezet használ, és amelyek a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogatják, többek között zavarok fennállásakor is;

2. „hálózati és információs rendszer”: az (EU) 2022/2555 irányelv 6. cikkének 1. pontjában meghatározott hálózati és információs rendszer;

3. „elavult IKT-rendszer”: olyan IKT-rendszer, amely elérte életciklusának végét (kifutási szakaszban van), amely technológiai vagy kereskedelmi okokból már nem alkalmas frissítésre vagy javításra, vagy amelyhez értékesítője vagy harmadik fél IKT-szolgáltató már nem nyújt támogatást, amely azonban még használatban van, és támogatja a pénzügyi szervezet funkcióit;

4. „hálózati és információs rendszerek biztonsága”: az (EU) 2022/2555 irányelv 6. cikkének 2. pontjában meghatározott hálózati és információs rendszerek biztonsága;

5. „IKT-kockázat”: minden olyan, a hálózati és információs rendszerek használata kapcsán észszerűen azonosítható körülmény, amely, ha bekövetkezik, veszélyeztetheti a hálózati és információs rendszerek, valamely technológiafüggő eszköz vagy folyamat, vagy egyéb műveletek és folyamatok vagy a szolgáltatásnyújtás biztonságát azáltal, hogy káros hatásokkal jár a digitális vagy a fizikai környezetre nézve;

6. „információs vagyonelem”: információk olyan tárgyi vagy immateriális gyűjteménye, amely védelemre érdemes;

7. „IKT-eszköz”: a pénzügyi szervezet által használt hálózati és információs rendszerek részét képező szoftver- vagy hardvereszköz;

8. „IKT-vonatkozású esemény”: olyan, a pénzügyi szervezet által nem tervezett egyedi esemény vagy egymással összefüggő események sorozata, amely veszélyezteti a hálózati és információs rendszerek biztonságát, és káros hatása van az adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére, vagy a pénzügyi szervezet által nyújtott szolgáltatásokra;

9. „pénzforgalmi vonatkozású működési vagy biztonsági esemény”: olyan, a 2. cikk (1) bekezdésének a) d) pontjában említett pénzügyi szervezetek által nem tervezett, akár IKT-vonatkozású, akár egyéb egyedi esemény vagy egymással összefüggő események sorozata, amelynek káros hatása van a pénzforgalmi vonatkozású adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére, vagy a pénzügyi szervezet által nyújtott pénzforgalmi vonatkozású szolgáltatásokra;

10. „jelentős IKT-vonatkozású esemény”: olyan IKT-vonatkozású esemény, amelynek jelentős káros hatása van a pénzügyi szervezet kritikus vagy fontos funkcióit támogató hálózati és információs rendszerekre;

11. „jelentős pénzforgalmi vonatkozású működési vagy biztonsági esemény”: olyan pénzforgalmi vonatkozású működési vagy biztonsági esemény, amelynek jelentős káros hatása van a pénzügyi szervezetek által nyújtott pénzforgalmi vonatkozású szolgáltatásokra;

12. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

13. „jelentős kiberfenyegetés”: olyan kiberfenyegetés, amelynek technikai sajátosságai azt jelzik, hogy potenciálisan jelentős IKT-vonatkozású eseményt vagy jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményt eredményezhet;

14. „kibertámadás”: rosszindulatú IKT-vonatkozású esemény, amelynek során valamely fenyegető szereplő valamely eszköz megsemmisítésére, felfedésére, módosítására, használhatatlanná tételére, eltulajdonítására, az eszközhöz való illetéktelen hozzáférésre, vagy annak illetéktelen felhasználására tesz kísérletet;

15. „fenyegetettséggel kapcsolatos hírszerzés”: azzal a céllal összesített, átalakított, elemzett, értelmezett vagy tovább gazdagított információk, hogy biztosítsák a döntéshozatalhoz szükséges kontextust, és lehetővé tegyék a valamely IKT-vonatkozású esemény vagy kiberfenyegetés hatásainak enyhítéséhez szükséges releváns és elégséges szintű megértést, ideértve valamely kibertámadás technikai részleteit, a támadásért felelősök kilétét, valamint az elkövetés módját és indítékait;

16. „sérülékenység”: valamely vagyonelem, rendszer, folyamat vagy kontroll kihasználható gyengesége, érzékenysége vagy hibája;

17. „fenyegetés alapú behatolási tesztelés (threat led penetration testing, TLPT)”: olyan keret, amely utánozza egy tényleges kiberfenyegetés forrásának tekintett, valós fenyegetést jelentő szereplők taktikáját, módszereit és eljárásait, és amely elvégzi a pénzügyi szervezet kritikus éles rendszereinek kontrollált, testreszabott, hírszerzésen alapuló (red team) tesztelését;

18. „harmadik féltől eredő IKT-kockázat”: a pénzügyi szervezetnél azzal összefüggésben felmerülő esetleges IKT-kockázat, hogy harmadik fél IKT-szolgáltatók vagy azok alvállalkozói által nyújtott szolgáltatásokat vesz igénybe, ideértve a kiszervezés útján igénybe vett IKT-szolgáltatásokat is;

19. „harmadik fél IKT-szolgáltató”: IKT-szolgáltatásokat nyújtó vállalkozás;

20. „csoporton belüli IKT-szolgáltató”: olyan vállalkozás, amely egy pénzügyi csoport részét képezi, és főként az ugyanazon csoportba vagy ugyanazon intézményvédelmi rendszerhez tartozó pénzügyi szervezeteknek – többek között az anyavállalatának, leányvállalatainak és fióktelepeinek, vagy más, közös tulajdonban vagy közös ellenőrzés alatt álló szervezeteknek – történő IKT-szolgáltatásnyújtással foglalkozik;

21. „IKT-szolgáltatások”: IKT-rendszerek útján egy vagy több belső vagy külső felhasználó részére folyamatos jelleggel nyújtott digitális és adatszolgáltatások, ideértve a hardvert mint szolgáltatást és a hardverszolgáltatásokat, ami magában foglalja a hardverszolgáltató általi szoftver- vagy belsőrendszervezérlőprogram-(firmware-)frissítéseket is, ide nem értve a hagyományos analóg telefonszolgáltatásokat;

22. „kritikus vagy fontos funkció”: olyan funkció, amelynek zavara lényegesen rontaná a pénzügyi szervezet pénzügyi teljesítményét, vagy szolgáltatásai és tevékenységei megbízhatóságát vagy folytonosságát, vagy az említett funkció kiesése, hibás vagy meghiúsult működése lényegesen rontaná a pénzügyi szervezet képességét az engedélyében foglalt feltételek és kötelezettségek, valamint a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt egyéb kötelezettségei folyamatos teljesítésére;

23. „kritikus harmadik fél IKT-szolgáltató”: a 31. cikkel összhangban kritikusként kijelölt, harmadik fél IKT-szolgáltató;

24. „harmadik országban letelepedett, harmadik fél IKT-szolgáltató”: harmadik országban letelepedett, jogi személyiséggel rendelkező, harmadik fél IKT-szolgáltató, amely egy pénzügyi szervezettel IKT-szolgáltatások nyújtásáról szóló szerződéses megállapodást kötött;

25. „leányvállalat”: a 2013/34/EU irányelv 2. cikke 10. pontjának és 22. cikkének értelmében vett leányvállalkozás;

26. „csoport”: a 2013/34/EU irányelv 2. cikkének 11. pontjában meghatározott csoport;

27. „anyavállalat”: a 2013/34/EU irányelv 2. cikkének 9. pontja és 22. cikke értelmében vett anyavállalat;

28. „harmadik országban letelepedett IKT-alvállalkozó”: harmadik országban letelepedett, jogi személyiséggel rendelkező IKT-alvállalkozó, amely harmadik fél IKT-szolgáltatóval vagy harmadik országban letelepedett, harmadik fél IKT-szolgáltatóval szerződéses megállapodást kötött;

29. „IKT-koncentrációs kockázat”: egyetlen vagy több kapcsolódó kritikus harmadik fél IKT-szolgáltatóval szembeni kitettség, amely az ilyen szolgáltatóktól való olyan mértékű függőséget teremt, hogy egy ilyen szolgáltató rendelkezésre nem állása, meghibásodása vagy egyéb típusú hiányossága potenciálisan veszélyeztetheti a pénzügyi szervezet kritikus vagy fontos funkciók ellátására való képességét, vagy számára más típusú káros hatásokat – többek között nagy veszteségeket – okozhat, vagy veszélyeztetheti az Unió egészének pénzügyi stabilitását;

30. „vezető testület”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 36. pontjában, a 2013/36/EU irányelv 3. cikke (1) bekezdésének 7. pontjában, a 2009/65/EK európai parlamenti és tanácsi irányelv ([31]) 2. cikke (1) bekezdésének s. pontjában, a 909/2014/EU rendelet 2. cikke (1) bekezdésének 45. pontjában, az (EU) 2016/1011 rendelet 3. cikke (1) bekezdésének 20. pontjában és a kriptoeszközök piacairól szóló rendelet releváns rendelkezéseiben meghatározott vezető testület, vagy annak tagjaival egyenértékű személyek csoportja, akik ténylegesen működtetik a szervezetet, vagy a releváns uniós vagy nemzeti jogszabályokkal összhangban kulcsfontosságú funkciókat látnak el;

31. „hitelintézet”: az 575/2013/EU európai parlamenti és tanácsi rendelet ([32]) 4. cikke (1) bekezdésének 1. pontjában meghatározott hitelintézet;

32. „a 2013/36/EU irányelv alapján mentesített intézmény”: valamely, a 2013/36/EU irányelv 2. cikke (5) bekezdésének 4–23. pontjában említett jogalany;

33. „befektetési vállalkozás”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 1. pontjában meghatározott befektetési vállalkozás;

34. „kis méretű és össze nem kapcsolt befektetési vállalkozás”: olyan befektetési vállalkozás, amely megfelel az (EU) 2019/2033 európai parlamenti és tanácsi rendelet ([33]) 12. cikkének (1) bekezdésében megállapított feltételeknek;

35. „pénzforgalmi intézmény”: az (EU) 2015/2366 irányelv 4. cikkének 4. pontjában meghatározott pénzforgalmi intézmény;

36. „az (EU) 2015/2366 irányelv alapján mentesített pénzforgalmi intézmény”: az (EU) 2015/2366 irányelv 32. cikkének (1) bekezdése értelmében mentességet élvező pénzforgalmi intézmény;

37. „számlainformációkat összesítő szolgáltató”: az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett számlainformációkat összesítő szolgáltató;

38. „elektronikuspénz-kibocsátó intézmény”: a 2009/110/EK európai parlamenti és tanácsi irányelv 2. cikkének 1. pontjában meghatározott elektronikuspénz-kibocsátó intézmény;

39. „a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmény”: a 2009/110/EK irányelv 9. cikkének (1) bekezdésében foglaltak szerinti, mentességet élvező elektronikuspénz-kibocsátó intézmény;

40. „központi szerződő fél”: a 648/2012/EU rendelet 2. cikkének 1. pontjában meghatározott központi szerződő fél;

41. „kereskedési adattár”: a 648/2012/EU rendelet 2. cikkének 2. pontjában meghatározott kereskedési adattár;

42. „központi értéktár”: a 909/2014/EU rendelet 2. cikke (1) bekezdésének 1. pontjában meghatározott központi értéktár;

43. „kereskedési helyszín”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 24. pontjában meghatározott kereskedési helyszín;

44. „alternatívbefektetésialap-kezelő”: a 2011/61/EU irányelv 4. cikke (1) bekezdésének b) pontjában meghatározott alternatívbefektetésialap-kezelő;

45. „alapkezelő társaság”: a 2009/65/EK irányelv 2. cikke (1) bekezdésének b) pontjában meghatározott alapkezelő társaság;

46. „adatszolgáltató”: a 600/2014/EU rendelet értelmében vett, annak 2. cikk (1) bekezdésének 34–36. pontjában említett adatszolgáltató;

47. „biztosító”: a 2009/138/EK irányelv 13. cikkének 1. pontjában meghatározott biztosító;

48. „viszontbiztosító”: a 2009/138/EK irányelv 13. cikkének 4. pontjában meghatározott viszontbiztosító;

([31]) Az Európai Parlament és a Tanács 2009/65/EK irányelve (2009. július 13.) az átruházható értékpapírokkal foglalkozó kollektív befektetési vállalkozásokra (ÁÉKBV) vonatkozó törvényi, rendeleti és közigazgatási rendelkezések összehangolásáról (HL L 302., 2009.11.17., 32. o.).

([32]) Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26.) a hitelintézetekre vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.).

([33]) Az Európai Parlament és a Tanács (EU) 2019/2033 rendelete (2019. november 27.) a befektetési vállalkozásokra vonatkozó prudenciális követelményekről, valamint az 1093/2010/EU, az 575/2013/EU, a 600/2014/EU és a 806/2014/EU rendelet módosításáról (HL L 314., 2019.12.5., 1. o.).

49. „biztosításközvetítő”: az (EU) 2016/97 európai parlamenti és tanácsi irányelv ([34]) 2. cikke (1) bekezdésének 3. pontjában meghatározott biztosításközvetítő;

50. „kiegészítő biztosításközvetítői tevékenységet végző személy”: az (EU) 2016/97 irányelv 2. cikke (1) bekezdésének 4. pontjában meghatározott kiegészítő biztosításközvetítői tevékenységet végző személy;

51. „viszontbiztosítás-közvetítő”: az (EU) 2016/97 irányelv 2. cikke (1) bekezdésének 5. pontjában meghatározott viszontbiztosítás-közvetítő;

52. „foglalkoztatói nyugellátást szolgáltató intézmény”: az (EU) 2016/2341 irányelv 6. cikkének 1. pontjában meghatározott foglalkoztatói nyugellátást szolgáltató intézmény;

53. „kis méretű foglalkoztatói nyugellátást szolgáltató intézmény”: olyan nyugdíjkonstrukciókat működtető foglalkoztatói nyugellátást szolgáltató intézmény, amely nyugdíjkonstrukciók összesen nem rendelkeznek száznál több taggal;

54. „hitelminősítő intézet”: az 1060/2009/EK rendelet 3. cikke (1) bekezdésének b) pontjában meghatározott hitelminősítő intézet;

55. „kriptoeszköz-szolgáltató”: a kriptoeszközök piacairól szóló rendelet releváns rendelkezéseiben meghatározott kriptoeszköz-szolgáltató;

56. „eszközalapú tokenek kibocsátója”: a kriptoeszközök piacairól szóló rendelet releváns rendelkezéseiben meghatározott eszközalapú tokenek kibocsátója;

57. „kritikus referenciamutatók kezelője”: az (EU) 2016/1011 rendelet 3. cikke (1) bekezdésének 25. pontjában meghatározott »kritikus referenciamutatók« kezelője;

58. „közösségi finanszírozási szolgáltató”: az (EU) 2020/1503 európai parlamenti és tanácsi rendelet ([35]) 2. cikke (1) bekezdésének e) pontjában meghatározott közösségi finanszírozási szolgáltató;

59. „értékpapírosítási adattár”: az (EU) 2017/2402 európai parlamenti és tanácsi rendelet ([36]) 2. cikkének 23. pontjában meghatározott értékpapírosítási adattár;

60. „mikrovállalkozás”: a kereskedési helyszínektől, a központi szerződő felektől, a kereskedési adattáraktól és a központi értéktáraktól eltérő olyan pénzügyi szervezet, amely kevesebb mint 10 főt foglalkoztat, és éves árbevétele és/vagy éves mérlegfőösszege nem haladja meg a 2 millió EUR-t;

61. „vezető felvigyázó”: az e rendelet 31. cikke (1) bekezdésének b) pontjával összhangban kinevezett európai felügyeleti hatóság;

62. „vegyes bizottság”: az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 54. cikkében említett bizottság;

63. „kisvállalkozás”: olyan pénzügyi szervezet, amely 10 vagy több főt, de kevesebb mint 50 főt foglalkoztat, és 2 millió EUR-t meghaladó, de 10 millió EUR-t meg nem haladó éves árbevétellel és/vagy éves mérlegfőösszeggel rendelkezik;

64. „középvállalkozás”: olyan pénzügyi szervezet, amely nem kisvállalkozás, kevesebb mint 250 főt foglalkoztat, és 50 millió EUR-t meg nem haladó éves árbevétellel és/vagy 43 millió EUR-t meg nem haladó éves mérlegfőösszeggel rendelkezik;

65. „hatóság”: bármely kormányzati vagy egyéb közigazgatási szerv, ideértve a nemzeti központi bankokat is.

([34]) Az Európai Parlament és a Tanács (EU) 2016/97 irányelve (2016. január 20.) a biztosítási értékesítésről (HL L 26., 2016.2.2., 19. o.).

([35]) Az Európai Parlament és a Tanács (EU) 2020/1503 rendelete (2020. október 7.) az európai közösségi finanszírozási üzleti szolgáltatókról, valamint az (EU) 2017/1129 rendelet és az (EU) 2019/1937 irányelv módosításáról (HL L 347., 2020.10.20., 1. o.).

([36]) Az Európai Parlament és a Tanács (EU) 2017/2402 rendelete (2017. december 12.) az értékpapírosítás általános keretrendszerének meghatározásáról, az egyszerű, átlátható és egységesített értékpapírosítás egyedi keretrendszerének létrehozásáról, valamint a 2009/65/EK, a 2009/138/EK és a 2011/61/EU irányelv és az 1060/2009/EK és a 648/2012/EU rendelet módosításáról (HL L 347., 2017.12.28., 35. o.).

4. cikk

Arányossági elv

(1) A pénzügyi szervezetek a II. fejezetben megállapított szabályokat az arányosság elvével összhangban hajtják végre, figyelembe véve méretüket és általános kockázati profiljukat, valamint szolgáltatásaik, tevékenységeik és működésük jellegét, nagyságrendjét és összetettségét.

(2) Ezenkívül, a III. és a IV. fejezet, valamint az V. fejezeten belüli I. szakasz pénzügyi szervezetek általi alkalmazásának arányban kell állnia méretükkel és általános kockázati profiljukkal, valamint szolgáltatásaik, tevékenységeik és működésük jellegével, nagyságrendjével és összetettségével, amint azt az említett fejezetek releváns szabályai konkrétan előírják.

(3) Az illetékes hatóságoknak figyelembe kell venniük az arányossági elv pénzügyi szervezetek általi alkalmazását, amikor felülvizsgálják az IKT-kockázatkezelési keretrendszer következetességét az illetékes hatóságok kérésére a 6. cikk (5) bekezdésének és a 16. cikk (2) bekezdésének alapján benyújtott jelentések alapján.

II. FEJEZET

IKT-kockázatkezelés

I. szakasz

5. cikk

Irányítás és szervezés

(1) A pénzügyi szervezeteknek rendelkezniük kell egy olyan belső irányítási és kontrollkerettel, amely biztosítja az IKT-kockázat eredményes és prudens kezelését a 6. cikk (4) bekezdésével összhangban, a digitális működési reziliencia magas szintjének elérése érdekében.

(2) A pénzügyi szervezet vezető testületének kell meghatároznia, jóváhagynia és felvigyáznia a 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszerrel összefüggő valamennyi intézkedést, és viselnie a felelősséget azok végrehajtásáért.

Az első albekezdés alkalmazásában a vezető testület:

a) viseli a végső felelősséget a pénzügyi szervezet IKT-kockázatainak kezeléséért;

b) bevezet az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normák fenntartását biztosítani célzó politikákat;

c) egyértelmű feladat- és felelősségi köröket jelöl ki valamennyi IKT-vonatkozású funkcióval összefüggésben, és létrehozza az említett funkciók közötti hatékony és jól időzített kommunikációt, együttműködést és koordinációt biztosító, megfelelő irányítási rendszert;

d) viseli a 6. cikk (8) bekezdésében említett, digitális működési rezilienciára vonatkozó stratégia létrehozásával és jóváhagyásával kapcsolatos általános felelősséget, ideértve a pénzügyi szervezet megfelelő IKT-kockázati tolerancia-szintjének a 6. cikk (8) bekezdésének b) pontjában említett megállapítását is;

e) jóváhagyja, felvigyázza és időszakonként felülvizsgálja a pénzügyi szervezetnek a 11. cikk (1), illetve (3) bekezdésében említett IKT-üzletmenetfolytonossági politikáját, illetve IKT-reagálási és -helyreállítási tervét, amelyeknek elfogadására sor kerülhet a pénzügyi szervezet átfogó üzletmenet-folytonossági politikájának, valamint reagálási és helyreállítási tervének integráns részét képező célzott egyedi szabályzat formájában is;

f) jóváhagyja és időszakonként felülvizsgálja a pénzügyi szervezet IKT-vonatkozású belső ellenőrzési terveit, IKT-ellenőrzéseit és azok lényeges módosításait;

g) megállapítja és időszakonként felülvizsgálja a pénzügyi szervezet digitális működési rezilienciával kapcsolatos szükségleteinek kielégítését biztosító költségvetést minden erőforrástípus tekintetében, ideértve a személyzet valamennyi tagja számára biztosítandó, a 13. cikk (6) bekezdésében említett releváns, IKT-biztonsági tudatosságot elősegítő programokat és digitális működési rezilienciával kapcsolatos képzéseket, valamint IKT-készségeket;

h) jóváhagyja és időszakonként felülvizsgálja a pénzügyi szervezetnek a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló megállapodásokkal kapcsolatos szabályait;

i) vállalati szinten létrehozza a következőkkel kapcsolatos megfelelő tájékozódást lehetővé tevő bejelentési csatornákat:

   i. a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételére vonatkozóan kötött megállapodások;

   ii. bármely releváns, a harmadik fél IKT-szolgáltatókra vonatkozó tervezett lényeges változtatás;

   iii. az ilyen változtatások potenciális hatása az említett megállapodásokkal érintett kritikus vagy fontos funkciókra, ideértve az említett változtatások hatását értékelő kockázatelemzés-összefoglalót, továbbá legalább a jelentős IKT-vonatkozású események és azok hatásai, valamint reagálási, helyreállítási és korrekciós intézkedések.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek létre kell hozniuk egy feladatkört a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások alkalmazásáról kötött megállapodások nyomon követése érdekében, vagy ki kell jelölniük a felső vezetés egy tagját a kapcsolódó kockázati kitettség és a releváns dokumentáció feletti felvigyázásért felelős személyként.

(4) A pénzügyi szervezet vezető testülete tagjainak aktívan tájékozódniuk kell az aktuális információkról annak érdekében, hogy rendelkezésükre álljanak az ahhoz szükséges megfelelő ismeretek és készségek, hogy át tudják látni és értékelni tudják az IKT-kockázatot és annak a pénzügyi szervezet működésére gyakorolt hatását, többek között a kezelés alatt álló IKT-kockázattal arányos, célirányos képzés rendszeres végzése révén.

II. szakasz

6. cikk

IKT-kockázatkezelési keretrendszer

(1) A pénzügyi szervezeteknek általános kockázatkezelési rendszerük részeként megbízható, átfogó és jól dokumentált IKT-kockázatkezelési keretrendszerrel kell rendelkezniük, amely lehetővé teszi számukra az IKT-kockázat gyors, hatékony és átfogó kezelését, továbbá a digitális működési reziliencia magas szintjének biztosítását.

(2) Az IKT-kockázatkezelési keretrendszer magában foglalja legalább azon stratégiákat, szabályzatokat, eljárásokat, IKT-protokollokat és -eszközöket, amelyek szükségesek valamennyi információs vagyonelem és IKT-eszköz – többek között a számítógépes szoftverek, hardvereszközök és szerverek – kellő és adekvát védelméhez, valamint valamennyi releváns fizikai rendszerelem és infrastruktúra – így például a telephelyek, az adatközpontok és kijelölt érzékeny területek – védelméhez annak biztosítására, hogy valamennyi információs vagyonelem és IKT-eszköz megfelelő védelmet kapjon a kockázatokkal – köztük a káreseménnyel, valamint az illetéktelen hozzáféréssel és használattal – szemben.

(3) A pénzügyi szervezeteknek az IKT-kockázatkezelési keretrendszerükkel összhangban, megfelelő stratégiák, szabályzatok, eljárások, protokollok és eszközök bevezetésével minimalizálniuk kell az IKT-kockázat hatását. Az IKT-kockázatról és az IKT-kockázatkezelési keretrendszerükről teljeskörű és naprakész tájékoztatást kell nyújtaniuk az illetékes hatóságok számára, azok kérésére.

(4) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek az IKT-kockázat kezelésére és felvigyázására vonatkozó felelősséget egy kontrollfunkcióhoz rendelik hozzá, és az összeférhetetlenségek elkerülése érdekében biztosítják az ilyen kontrollfunkció megfelelő szintű függetlenségét. A pénzügyi szervezetek biztosítják az IKT-kockázatkezelési funkciók, kontrollfunkciók és belső ellenőrzési funkciók megfelelő elkülönítését és függetlenségét a három védelmi vonalra épülő modellnek vagy egy belső kockázatkezelési és kontrollmodellnek megfelelően.

(5) Az IKT-kockázatkezelési keretrendszert dokumentálni kell, és legalább évente egyszer – vagy mikrovállalkozások esetében időszakonként – felül kell vizsgálni, továbbá jelentős IKT-vonatkozású események bekövetkezésekor, valamint a digitális működési reziliencia tesztelésére vagy ellenőrzésére irányuló releváns folyamatokból származó felügyeleti utasításokat és következtetéseket követően. A keretet folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján. Az illetékes hatóság kérésére jelentést kell benyújtani számára az IKT-kockázatkezelési keretrendszer felülvizsgálatáról.

(6) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek IKT-kockázatkezelési keretrendszerére ellenőrök általi, rendszeres, a pénzügyi szervezetek ellenőrzési tervével összhangban végzendő belső ellenőrzési kötelezettség vonatkozik. Az említett ellenőröknek elegendő ismerettel, készségekkel és szakértelemmel kell rendelkezniük az IKT-kockázat terén, valamint megfelelő függetlenséggel. Az IKT-ellenőrzések gyakoriságának és fókuszpontjának arányban kell állnia a pénzügyi szervezet IKT-kockázatával.

(7) A pénzügyi szervezetnek a belső ellenőrzési felülvizsgálat következtetései alapján formális utókövetési folyamatot kell kialakítania, beleértve a kritikus IKT-audit megállapítások kellő időben történő igazolására és a hiányosságok korrekciójára vonatkozó szabályokat.

(8) Az IKT-kockázatkezelési keretrendszernek magában kell foglalnia egy digitális működési rezilienciára vonatkozó stratégiát is, amely meghatározza, hogy hogyan hajtandó végre a keret. E célból a digitális működési rezilienciára vonatkozó stratégiának magában kell foglalnia az IKT-kockázat kezelésére és a konkrét IKT-célkitűzések megvalósítására irányuló módszereket, a következők révén:

a) ki kell fejteni, hogy az IKT-kockázatkezelési keretrendszer hogyan támogatja a pénzügyi szervezet üzleti stratégiáját és célkitűzéseit;

b) meg kell határozni az IKT-kockázati toleranciaszintet a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban, továbbá elemezni kell az IKT-zavarok hatásaival kapcsolatos toleranciát;

c) egyértelmű információbiztonsági célokat kell kitűzni, megállapítva a fő teljesítménymutatókat és kockázati mérőszámokat is;

d) ismertetni kell az IKT-referenciaarchitektúrát az egyes konkrét üzleti célkitűzések eléréséhez szükséges változtatásokkal együtt;

e) fel kell vázolni azon különböző mechanizmusokat, amelyeket az IKT-vonatkozású események észlelése, hatásaik megelőzése és az azzal szembeni védelem céljából vezettek be;

f) a bejelentett jelentős IKT-vonatkozású események számát és a megelőző intézkedések eredményességét alapul véve, bizonyítékokkal alá kell támasztani a digitális működési reziliencia aktuális helyzetét;

g) e rendelet IV. fejezetével összhangban el kell végezni a digitális működési reziliencia tesztelését;

h) fel kell vázolni az IKT-vonatkozású események esetén alkalmazandó kommunikációs stratégiát, amelynek közzététele a 14. cikkel összhangban kötelező.

(9) A pénzügyi szervezetek a (8) bekezdésben említett, digitális működési rezilienciára vonatkozó stratégia keretében meghatározhatnak egy több szolgáltatóra épülő, holisztikus IKT-stratégiát is – akár csoport-, akár szervezeti szinten –, amely bemutatja a harmadik fél IKT-szolgáltatóktól való főbb függőségeket, és kifejti a harmadik fél IKT-szolgáltatóknál alkalmazott beszerzési mix indokait.

(10) A pénzügyi szervezetek az uniós és a nemzeti ágazati jogszabályokkal összhangban kiszervezhetik az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzésének feladatait csoporton belüli vagy külső vállalkozásokhoz. Kiszervezés esetén a pénzügyi szervezet továbbra is teljes felelősséggel tartozik az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzéséért.

7. cikk

IKT-rendszerek, -protokollok és -eszközök

A pénzügyi szervezetek az IKT-kockázat kezelése érdekében olyan naprakész IKT-rendszereket, -protokollokat és -eszközöket alkalmaznak és tartanak fenn, amelyek:

a) az arányosságnak a 4. cikkben említett elvével összhangban megfelelnek a tevékenységeik folytatását támogató műveletek nagyságrendjének;

b) megbízhatóak;

c) elegendő kapacitással rendelkeznek a tevékenységek elvégzéséhez és a szolgáltatások időben történő nyújtásához szükséges adatok pontos feldolgozására, továbbá szükség szerint a kiugróan magas megbízások, üzenetküldési vagy ügyleti volumenek kezelésére, többek között amennyiben új technológia bevezetésére kerül sor;

d) technológiai szempontból reziliensek annak érdekében, hogy szükség szerint, piaci stresszhelyzetben vagy egyéb kedvezőtlen helyzetekben megfelelően kezeljék a további információs feldolgozási igényeket.

8. cikk

Azonosítás

(1) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek azonosítaniuk, osztályozniuk és megfelelően dokumentálniuk kell valamennyi, az IKT-ra támaszkodó üzleti funkciót, feladat- és felelősségi kört, az említett funkciókat támogató információs vagyonelemeket és IKT-eszközöket, valamint azok IKT-kockázattal kapcsolatos feladatkörét és függőségeit. A pénzügyi szervezeteknek szükség szerint, de legalább évente felül kell vizsgálniuk ezen osztályozás és minden releváns dokumentáció megfelelőségét.

(2) A pénzügyi szervezeteknek folyamatosan azonosítaniuk kell az IKT-kockázat valamennyi forrását, különösen a más pénzügyi szervezetekkel szembeni és azoktól eredő kockázati kitettséget, továbbá értékelniük kell az IKT-ra támaszkodó üzleti funkcióik, információs vagyonelemeik és IKT-eszközeik szempontjából releváns kiberfenyegetéseket és IKT-sérülékenységeket. A pénzügyi szervezeteknek rendszeresen, de legalább évente felül kell vizsgálniuk az őket érintő kockázati forgatókönyveket.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek a hálózati és információsrendszer-infrastruktúrában, az IKT-ra támaszkodó üzleti funkcióikat, információs vagyonelemeiket és IKT-eszközeiket érintő folyamatokban és eljárásokban bekövetkezett minden jelentős változást követően kockázatértékelést kell végezniük.

(4) A pénzügyi szervezeteknek azonosítaniuk kell valamennyi információs vagyonelemet és IKT-eszközt, ideértve a távoli helyeken találhatókat is, továbbá a hálózati erőforrásokat és a hardvereszközöket, és fel kell térképezniük, hogy melyek tekinthetők kritikusnak. Fel kell térképezniük az információs vagyonelemek és IKT-eszközök konfigurációját, valamint a különböző információs vagyonelemek és IKT-eszközök közötti kapcsolatokat és kölcsönös függőségeket.

(5) A pénzügyi szervezeteknek azonosítaniuk és dokumentálniuk kell a harmadik fél IKT-szolgáltatóktól függő valamennyi folyamatot, valamint azonosítaniuk kell a kritikus vagy fontos funkciókat támogató szolgáltatást nyújtó, harmadik fél IKT-szolgáltatókkal meglévő összeköttetéseket.

(6) Az (1), (4) és (5) bekezdés alkalmazásában a pénzügyi szervezeteknek releváns nyilvántartásokat kell vezetniük, valamint azokat időszakonként és minden alkalommal, amikor a (3) bekezdésben említett jelentős változás következik be, frissíteniük kell.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek rendszeresen, de legalább évente, továbbá a technológiák, alkalmazások vagy rendszerek összekapcsolása előtt és után minden esetben célzottan értékelniük kell valamennyi elavult IKT-rendszer IKT-kockázatait.

9. cikk

Védelem és megelőzés

(1) Az IKT-rendszerek megfelelő védelme céljából és a válaszintézkedések megszervezése érdekében a pénzügyi szervezetek folyamatosan nyomon követik és ellenőrzik az IKT-rendszerek és -eszközök biztonságát és működését, és minimalizálják az IKT-rendszereket érintő IKT-kockázat hatását megfelelő IKT-biztonsági eszközök, szabályzatok és eljárások bevezetésével.

(2) A pénzügyi szervezetek megtervezik, beszerzik és bevezetik azon IKT-biztonsági stratégiákat, szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek célja biztosítani az IKT-rendszerek rezilienciáját, folytonosságát és rendelkezésre állását – különös tekintettel azokra, amelyek kritikus vagy fontos funkciókat támogatnak –, továbbá fenntartani az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normákat, legyen szó használaton kívüli, használatban lévő vagy továbbítás alatt álló adatokról.

(3) A (2) bekezdésben említett célkitűzések elérése érdekében a pénzügyi szervezetek olyan IKT-megoldásokat és -folyamatokat alkalmaznak, amelyek a 4. cikkel összhangban megfelelőek. Az említett IKT-megoldásoknak és -folyamatoknak:

a) garantálniuk kell az adattovábbítási eszközök biztonságát;

b) minimalizálniuk kell az adatsérülés és -vesztés, a jogosulatlan hozzáférés, valamint az üzleti tevékenységet akadályozható technikai hibák kockázatát;

c) meg kell akadályozniuk az adatok rendelkezésre állásának hiányát, hitelességének és integritásának sérülését, bizalmas kezelésének megsértését és az adatvesztést;

d) biztosítaniuk kell az adatoknak az adatgazdálkodás során felmerülő kockázatokkal szembeni védelmét, ideértve a nem megfelelő kezelést, a feldolgozással kapcsolatos kockázatokat és az emberi hibát is.

(4) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek:

a) információs biztonsági szabályzatot dolgoznak ki és dokumentálnak, amely meghatározza az adatok, az információs vagyonelemek és az IKT-eszközök – ideértve adott esetben az ügyfeleikét is – rendelkezésre állását, hitelességét, integritását és bizalmas kezelését védeni célzó szabályokat;

b) kockázatalapú megközelítést követve, létrehoznak egy megbízható hálózati és infrastruktúra-menedzsment struktúrát, megfelelő technikákat, módszereket és protokollokat alkalmazva, amelyek magukban foglalhatják automatizált mechanizmusok végrehajtását is, az érintett információs vagyonelemek kibertámadás esetén történő elszigetelése érdekében;

c) olyan szabályzatokat hajtanak végre, amelyek az információs vagyonelemekhez és az IKT-eszközökhöz való fizikai vagy logikai hozzáférést kizárólag a jogszerű és jóváhagyott funkciókhoz és tevékenységekhez szükséges mértékűre korlátozzák, és e célból olyan szabályzatokat, eljárásokat és kontrollokat határoznak meg, amelyek szabályozzák a hozzáférés-kezelési jogosultságokat, és biztosítják azok megbízható adminisztrációját;

d) erős hitelesítési mechanizmusokat szolgáló szabályzatokat és protokollokat vezetnek be releváns normák és célzott kontrollrendszerek alapján, valamint a kriptográfiai kulcsokhoz kapcsolódó védelmi intézkedéseket hajtanak végre, ahol az adatok jóváhagyott adatminősítési és IKT-kockázatértékelési folyamatok eredményei alapján kerülnek titkosításra;

e) az IKT-változás többek között a szoftver-, hardver- és belsővezérlőprogram-összetevőket, -rendszert vagy -biztonságot érintő változások kezelését szolgáló, olyan dokumentált szabályzatokat, eljárásokat és kontrollokat vezetnek be, amelyek kockázatértékelési megközelítésen alapulnak, és integráns részét képezik a pénzügyi szervezet általános változásmenedzsment-folyamatának, annak biztosítása érdekében, hogy az IKT-rendszerekben bekövetkező valamennyi változást kontrollált módon rögzítsék, teszteljék, értékeljék, hagyják jóvá, hajtsák végre és ellenőrizzék;

f) megfelelő és átfogó, dokumentált szabályzatokkal rendelkeznek a hibajavító csomagokra és frissítésekre vonatkozóan.

A b) pont első albekezdésének alkalmazásában a pénzügyi szervezetek a hálózati kapcsolati infrastruktúrát azonnali megszakításra vagy szakaszokra bontásra alkalmas módon alakítják ki annak érdekében, hogy minimalizálják és megelőzzék az átterjedést, különösen az összekapcsolt pénzügyi folyamatok esetében.

Az e) pont első albekezdésének alkalmazásában az IKT-vonatkozású változásmenedzsment-folyamatot a megfelelő vezetői szintnek kell jóváhagynia, és annak konkrét protokollokkal kell rendelkeznie.

10. cikk

Észlelés

(1) A pénzügyi szervezeteknek rendelkezniük kell azt lehetővé tevő mechanizmusokkal, hogy a 17. cikknek megfelelően azonnal észleljék a rendellenes tevékenységeket – beleértve az IKT-hálózatok teljesítményproblémáit és az IKT-vonatkozású eseményeket is –, továbbá hogy azonosítsák a potenciális lényeges egyedi meghibásodási pontokat.

Az első albekezdésben említett valamennyi észlelési mechanizmust a 25. cikkel összhangban rendszeresen tesztelnie kell.

(2) Az (1) bekezdésben említett észlelési mechanizmusoknak lehetővé kell tenniük a többszintű kontrollt, valamint meg kell határozniuk az IKT-vonatkozású események válaszfolyamatait kiváltó és elindító riasztási értékhatárokat és kritériumokat, ideértve az automatikus riasztási mechanizmusokat az IKT-vonatkozású eseményekre való reagálásért felelős, releváns személyzet számára.

(3) A pénzügyi szervezeteknek elegendő erőforrásokat és képességeket kell biztosítaniuk a felhasználói tevékenységek, valamint az IKT-vonatkozású rendellenességek és biztonsági események, különösen a kibertámadások előfordulásának nyomon követéséhez.

(4) Az adatszolgáltatóknak ezenkívül rendelkezniük kell olyan rendszerekkel, amelyek eredményesen ellenőrizhetik a kereskedési jelentéseket azok teljeskörűsége szempontjából, azonosíthatják a kihagyásokat és a nyilvánvaló hibákat, és kérhetik az említett jelentések újraküldését.

11. cikk

Reagálás és helyreállítás

(1) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként, a 8. cikkben említett azonosítási követelmények alapján a pénzügyi szervezeteknek átfogó IKT-üzletmenetfolytonossági politikát kell bevezetniük, amelyet a pénzügyi szervezet átfogó üzletmenet-folytonossági politikájának integráns részét képező célzott egyedi szabályzatként is elfogadhatnak.

(2) A pénzügyi szervezeteknek az IKT-üzletmenetfolytonossági politikát célzott, megfelelő és dokumentált intézkedések, tervek, eljárások és mechanizmusok útján kell végrehajtaniuk, a következők céljából:

a) a folytonosság biztosítása a pénzügyi szervezet kritikus vagy fontos funkcióinak ellátásában;

b) valamennyi IKT-vonatkozású eseményre gyors, megfelelő és eredményes reagálás és annak megoldása a kár mérséklésével, a tevékenység újraindítását és a helyreállítási intézkedéseket előtérbe helyezve;

c) célzott tervek haladéktalan aktiválása, amelyek lehetővé teszik az IKT-vonatkozású események egyes típusainak megfelelő, elszigetelésre irányuló intézkedések, folyamatok és technológiák alkalmazását, a további károk megelőzését, valamint a 12. cikkel összhangban kialakított célzott reagálási és helyreállítási intézkedéseket;

d) előzetes hatások, károk és veszteségek felmérése;

e) olyan kommunikációs és válságkezelési intézkedések meghatározása, amelyek biztosítják a naprakész információk eljuttatását a releváns belső személyzet valamennyi tagja és valamennyi külső érdekelt fél részére a 14. cikk, valamint az illetékes hatóságok részére a 19. cikk szerint.

(3) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek kapcsolódó IKT-vonatkozású reagálási és helyreállítási terveket kell bevezetniük, amelyeket a mikrovállalkozásnak nem minősülő pénzügyi szervezetek esetében független belső felülvizsgálatnak kell alávetni.

(4) A pénzügyi szervezeteknek – különösen a harmadik fél IKT-szolgáltatókkal kötött megállapodások keretében kiszervezett vagy megbízásba adott kritikus vagy lényeges funkciókra vonatkozóan – megfelelő IKT-üzletmenetfolytonossági terveket kell bevezetniük és fenntartaniuk, amelyeket időszakonként tesztelniük kell.

(5) Az átfogó üzletmenet-folytonossági politika részeként a pénzügyi szervezeteknek üzleti hatáselemzést (BIA) kell végezniük az üzletmenetben okozott súlyos zavaroknak való kitettségükről. Az üzleti hatáselemzés keretében a pénzügyi szervezeteknek mennyiségi és minőségi kritériumok alapján értékelniük kell az üzletmenetben okozott súlyos zavarok lehetséges hatását, adott esetben belső és külső adatok és forgatókönyv-elemzés felhasználásával. Az üzleti hatáselemzésnek tekintetbe kell vennie az azonosított és felvázolt üzleti funkcióknak, támogatási folyamatoknak, harmadik felektől való függőségeknek és információs vagyonelemeknek, valamint azok kölcsönös függőségeinek a kritikusságát. A pénzügyi szervezeteknek biztosítaniuk kell, hogy az IKT-eszközöket és IKT-szolgáltatásokat az üzleti hatáselemzéssel teljes összhangban alakítsák ki és használják, különösen valamennyi kritikus összetevő redundanciájának megfelelő biztosítása tekintetében.

(6) Átfogó IKT-kockázatkezelésük keretében a pénzügyi szervezeteknek:

a) tesztelniük kell az IKT-üzletmenetfolytonossági terveket és az IKT-reagálási és -helyreállítási terveket a valamennyi funkciót támogató IKT-rendszerekhez kapcsolódóan legalább évente, valamint a kritikus vagy fontos funkciókat támogató IKT-rendszereket érintő bármely jelentős változás bekövetkezése esetén;

b) tesztelniük kell a 14. cikknek megfelelően kialakított válsághelyzeti kommunikációs terveket.

Az első albekezdés a) pontjának alkalmazásában a mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek a tesztelési terveikben szerepeltetniük kell a kibertámadásokra, továbbá az elsődleges IKT-infrastruktúrájuk és a 12. cikkben meghatározott kötelezettségek teljesítéséhez szükséges tartalékkapacitás, biztonsági mentések és tartalékeszközök közötti átállásokra vonatkozó forgatókönyveket.

A pénzügyi szervezeteknek rendszeresen felül kell vizsgálniuk az IKT-üzletmenetfolytonossági politikájukat, valamint az IKT-reagálási és -helyreállítási terveiket, figyelembe véve az első albekezdés szerint elvégzett tesztek eredményeit, valamint az ellenőrzések és felügyeleti felülvizsgálatok alapján megfogalmazott ajánlásokat.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek olyan válságkezelési funkcióval kell rendelkezniük, amely az IKT-üzletmenet-folytonossági terveik vagy az IKT-reagálási és helyreállítási terveik aktiválása esetén a 14. cikkel összhangban többek között egyértelmű eljárásokat határoz meg a belső és külső válsághelyzeti kommunikáció kezelésére vonatkozóan.

(8) A pénzügyi szervezeteknek az olyan, zavart okozó eseményeket megelőzően és azok időtartama alatt végzett tevékenységekről, amikor az IKT-üzletmenetfolytonossági terveik és az IKT-reagálási és -helyreállítási terveik aktiválására kerül sor, könnyen hozzáférhető nyilvántartást kell vezetniük.

(9) A központi értéktáraknak az illetékes hatóságok rendelkezésére kell bocsátaniuk az IKT-vonatkozású üzletmenet-folytonossági tesztek vagy hasonló műveletek eredményeinek másolatát.

(10) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek az illetékes hatóságok kérésére jelentést kell tenniük a jelentős IKT-vonatkozású események által okozott költségek és veszteségek összesített éves becsléséről.

(11) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 16. cikkével összhangban az EFH-knak a vegyes bizottság keretében 2024. július 17-ig közös iránymutatásokat kell kidolgozniuk a (10) bekezdésben említett költségek és veszteségek összesített éves becslésére vonatkozóan.

12. cikk

Biztonsági mentési szabályzatok és eljárások, visszaállítási és helyreállítási eljárások és módszerek

(1) Annak biztosítása céljából, hogy IKT-rendszereiket és adataikat minimális leállási időt, valamint korlátozott mértékű zavart és veszteséget követően állíthassák helyre, a pénzügyi szervezeteknek – IKT-kockázatkezelési keretrendszerük részeként – ki kell dolgozniuk és dokumentálniuk kell a következőket:

a) olyan biztonsági mentési szabályzatok és eljárások, amelyek az információk kritikussága vagy az adatok bizalmassági szintje alapján meghatározzák a biztonsági mentéssel érintett adatok körét és a biztonsági mentés minimális gyakoriságát;

b) visszaállítási és helyreállítási eljárások és módszerek.

(2) A pénzügyi szervezeteknek létre kell hozniuk biztonsági mentési rendszereket, amelyek aktiválhatók a biztonsági mentési szabályzatoknak és eljárásoknak megfelelően, valamint a visszaállítási és helyreállítási eljárásokat és módszereket. A biztonsági mentési rendszerek aktiválása nem veszélyeztetheti a hálózati és információs rendszerek biztonságát, vagy az adatok rendelkezésre állását, hitelességét, integritását vagy bizalmas kezelését. A biztonsági mentési eljárásokat, valamint a visszaállítási és helyreállítási eljárásokat és módszereket időszakonként tesztelni kell.

(3) Az adatok biztonsági mentés alapján, saját rendszerekkel végzett helyreállításához a pénzügyi szervezeteknek olyan IKT-rendszereket kell használniuk, amelyek fizikailag és logikailag elkülönülnek a forrásoldali IKT-rendszertől. Az IKT-rendszereket védeni kell minden illetéktelen hozzáféréssel vagy IKT-sérüléssel szemben, és lehetővé kell tenni a szolgáltatások időben történő visszaállítását az adatok és a rendszer biztonsági mentéseinek szükség szerinti felhasználásával.

A központi szerződő felek esetében a helyreállítási terveknek lehetővé kell tenniük a zavar bekövetkezésekor folyamatban lévő valamennyi tranzakció helyreállítását, hogy a központi szerződő fél biztonsággal folytatni tudja működését, és a tervezett időben le tudja zárni az ügyleteket.

Az adatszolgáltatóknak emellett megfelelő erőforrásokat kell fenntartaniuk, valamint biztonsági mentési és helyreállítási eszközökkel kell rendelkezniük annak érdekében, hogy mindenkor kínálhassák és fenntarthassák szolgáltatásaikat.

(4) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek olyan IKT-tartalékkapacitásokat kell fenntartaniuk, amelyek biztosítják az üzleti igények ellátásához elégséges és megfelelő erőforrásokat, képességeket és funkciókat. A mikrovállalkozásoknak kockázati profiljukat alapul véve, mérlegelniük kell, hogy szükséges-e ilyen IKT-tartalékkapacitásokat fenntartaniuk.

(5) A központi értéktáraknak fenn kell tartaniuk legalább egy másodlagos adatfeldolgozó helyszínt, amely rendelkezik az üzleti igényeik ellátásához szükséges megfelelő erőforrásokkal, képességekkel, funkciókkal és személyi feltételekkel.

A másodlagos adatfeldolgozási helyszínnek:

a) olyan földrajzi távolságra kell elhelyezkednie az elsődleges adatfeldolgozási helyszíntől, amely biztosítja, hogy attól elkülönülő kockázati profillal rendelkezzen, és ne érintsék az elsődleges helyszínt érintő esemény hatásai;

b) képesnek kell lennie arra, hogy biztosítsa a kritikus vagy fontos funkcióknak az elsődleges helyszínnel azonos folytonosságát, vagy az ahhoz szükséges szolgáltatási szintet, hogy a pénzügyi szervezet működési folyamatai teljesítsék a helyreállítási célkitűzéseket;

c) azonnal elérhetőnek kell lennie a pénzügyi szervezet személyzete számára, biztosítandó a kritikus vagy fontos funkciók folytonosságát abban az esetben, ha az elsődleges adatfeldolgozási helyszín elérhetetlenné vált.

(6) Az egyes funkciókhoz kapcsolódó helyreállítási időre és helyreállítási pontra vonatkozó célkitűzések megállapításakor a pénzügyi szervezeteknek figyelembe kell venniük, hogy kritikus vagy fontos funkcióról van-e szó, valamint a piaci hatékonyságra potenciálisan gyakorolt általános hatást. Az ilyen, időre vonatkozó célkitűzéseknek biztosítaniuk kell a megállapodás szerinti szolgáltatási szintek teljesítését rendkívüli helyzetekben.

(7) IKT-vonatkozású eseményt követő helyreállítás során a pénzügyi szervezeteknek el kell végezniük a szükséges ellenőrzéseket – ideértve az esetleges többszörös ellenőrzést és adategyeztetést –, hogy fenntartsák az adatok legmagasabb szintű integritását. A szervezeteknek az adatok külső érdekelti forrásból való rekonstruálása esetén is el kell végezniük ezen ellenőrzéseket, hogy biztosítsák valamennyi adat rendszerek közötti következetességét.

13. cikk

Tanulás és alkalmazkodás

(1) A pénzügyi szervezeteknek rendelkezniük kell képességekkel és személyzettel ahhoz, hogy információkat gyűjtsenek a sérülékenységekről és kiberfenyegetésekről, valamint az IKT-vonatkozású eseményekről – különösen a kibertámadásokról –, és elemezzék azok valószínű hatását a szervezet digitális működési rezilienciájára.

(2) A pénzügyi szervezetek az alaptevékenységeiket megzavaró, jelentős IKT-vonatkozású eseményeket követően elvégzik az IKT-vonatkozású események utólagos felülvizsgálatát, elemezve a zavar okait, és azonosítva az IKT-műveletekben vagy a 11. cikkben említett IKT-üzletmenetfolytonossági politikában teendő szükséges javításokat.

A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek kérésre tájékoztatniuk kell az illetékes hatóságokat az IKT-vonatkozású események első albekezdésben említett utólagos felülvizsgálatát követően végrehajtott változásokról.

Az IKT-vonatkozású események első albekezdésben említett utólagos felülvizsgálata keretében meg kell állapítani, hogy a kialakított eljárásokat követték-e, és a megtett intézkedések eredményesek voltak-e többek között a következők vonatkozásában:

a) a biztonsági riasztásokra való reagálásnak, valamint az IKT-vonatkozású események hatása és súlyossága megállapításának a gyorsasága;

b) adott esetben az igazságügyi szakértői elemzés elvégzésének minősége és sebessége;

c) a biztonsági események pénzügyi szervezeten belüli eszkalációjának eredményessége;

d) a belső és külső kommunikáció eredményessége.

(3) A digitális működési reziliencia 26. és 27. cikkel összhangban végzett tesztéséből, a valós IKT-vonatkozású eseményekből, ezen belül különösen a kibertámadásokból, továbbá az IKT-üzletmenetfolytonossági tervek és az IKT-reagálási és -helyreállítási tervek aktiválása során felmerült kihívásokból, valamint a partnerekkel kicserélt és a felügyeleti felülvizsgálatok során értékelt információkból származó tapasztalatokat a szervezetnek megfelelően és folyamatosan be kell építenie az IKT-kockázatértékelés folyamatába. Az említett megállapítások képezik a 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer releváns összetevői megfelelő felülvizsgálatának alapját.

(4) A pénzügyi szervezetek nyomon követik a 6. cikk (8) bekezdésében meghatározott, a digitális működési rezilienciára vonatkozó stratégiájuk végrehajtásának eredményességét. Felvázolják az IKT-kockázat időbeli alakulását, elemzik az IKT-vonatkozású események – így különösen a kibertámadások és mintázataik – gyakoriságát, típusait, nagyságát és alakulását, abból a célból, hogy megértsék az IKT-kockázati kitettség szintjét – különösen a kritikus vagy fontos funkciókkal kapcsolatban –, és javítsák a pénzügyi szervezet kiberbiztonsági érettségét és felkészültségét.

(5) A vezető IKT-munkatársaknak legalább évente be kell számolniuk a vezető testületnek a (3) bekezdésben említett megállapításokról, és javaslatokat kell előterjeszteniük.

(6) A pénzügyi szervezeteknek a személyzetük képzési rendszerének részét képező kötelező modulokként IKT-biztonsági tudatosságot elősegítő programokat és a digitális működési rezilienciával kapcsolatos képzéseket kell kidolgozniuk. Az említett programok és képzések valamennyi munkavállalóra és a felső vezetés valamennyi tagjára alkalmazandók, és azok összetettségi szintjét a munkavállalók feladatköreihez kell igazítani. Adott esetben a pénzügyi szervezeteknek harmadik fél IKT-szolgáltatókat is be kell vonniuk a releváns képzési programjaikba a 30. cikk (2) bekezdésének i) pontjával összhangban.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek folyamatosan nyomon kell követniük a releváns technológiai fejleményeket többek között annak megértése céljából, hogy az új technológiák bevezetésének milyen hatása lehet az IKT-biztonsági követelményekre és a digitális működési rezilienciára. Lépést kell tartaniuk a legkorszerűbb IKT-kockázatkezelési folyamatokkal, hogy eredményesen léphessenek fel a kibertámadások meglévő és új formáival szemben.

14. cikk

Kommunikáció

(1) A 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek válsághelyzeti kommunikációs tervvel kell rendelkezniük, amely legalább a jelentős IKT-vonatkozású eseményekről és sérülékenységekről lehetővé teszi az ügyfelek, partnerek, valamint adott esetben a nyilvánosság felelős tájékoztatását.

(2) Az IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezeteknek a saját személyzetükre és a külső érdekeltekre vonatkozó kommunikációs szabályzatot kell bevezetniük. A személyzetre vonatkozó kommunikációs szabályzatban figyelembe kell venni annak szükségességét, hogy különbséget tegyenek az IKT-kockázatkezelésért, különösen a reagálásért és helyreállításért felelős munkatársak, valamint a tájékoztatást igénylő munkatársak között.

(3) A pénzügyi szervezeten belül legalább egy személyt meg kell bízni az IKT-vonatkozású eseményekre vonatkozó kommunikációs stratégia végrehajtásával, akinek e célból a nyilvánossággal és a médiával kapcsolatos feladatot is el kell látnia.

15. cikk

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

Az EFH-knak a vegyes bizottság keretében, az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) egyeztetve. közös szabályozástechnikai standardtervezeteket kell kidolgozniuk annak érdekében, hogy:

a) meghatározzák azon további elemeket, amelyeket a 9. cikk (2) bekezdésében említett IKT-biztonsági szabályzatoknak, eljárásoknak, protokolloknak és eszközöknek tartalmazniuk kell a hálózatok biztonságának garantálása, a behatolások és az adatokkal való visszaélés elleni megfelelő biztosítékok lehetővé tétele, az adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének többek között kriptográfiai technikákkal történő megőrzése, továbbá a garantáltan pontos és gyors, jelentős zavaroktól és indokolatlan késedelemtől mentes adattovábbítás érdekében;

b) kidolgozzák a hozzáférés-kezelési jogosultságokra vonatkozó, a 9. cikk (4) bekezdésének c) pontjában említett kontrollok további összetevőit és a kapcsolódó humánerőforrás-politikát, amely meghatározza a hozzáférési jogosultságokat, a jogosultságok kiosztására és visszavonására, az IKT-kockázattal kapcsolatos rendellenes magatartásformák megfelelő többek között hálózathasználati mintákra, időbeosztásra, IT-tevékenységre és ismeretlen eszközökre vonatkozó mutatókon keresztül történő nyomon követésére vonatkozó eljárásokat;

c) részletesen kidolgozzák a 10. cikk (1) bekezdésében meghatározott, a rendellenes tevékenységek azonnali észlelésére szolgáló mechanizmusokat, valamint a 10. cikk (2) bekezdésében megállapított azon kritériumokat, amelyek alapján az IKT-vonatkozású események észlelési és válaszfolyamatainak beindítására sor kerül;

d) részletesen meghatározzák a 11. cikk (1) bekezdésében említett IKT-üzletmenetfolytonossági politika összetevőit;

e) részletesen meghatározzák az IKT-üzletmenetfolytonossági tervek 11. cikk (6) bekezdésében említett tesztelését annak biztosítására, hogy az ilyen tesztelés kellőképpen figyelembe vegyen olyan forgatókönyveket, amelyek szerint egy kritikus vagy lényeges funkció ellátása elfogadhatatlan színvonalúra csökken vagy meghiúsul, és kellőképpen tekintetbe vegye bármely releváns harmadik fél IKT-szolgáltató fizetésképtelenségének vagy egyéb hiányosságainak potenciális hatásait, valamint adott esetben a vonatkozó szolgáltatók joghatósági területén fennálló politikai kockázatokat;

f) részletesen meghatározzák a 11. cikk (3) bekezdésében említett IKT-reagálási és -helyreállítási tervek összetevőit;

g) részletesen meghatározzák a 6. cikk (5) bekezdésében említett, az IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés tartalmát és formátumát.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az európai felügyeleti hatóságoknak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásainak, tevékenységeinek és műveleteinek jellegét, nagyságrendjét és összetettségét, ugyanakkor kellően tekintetbe kell venniük a különböző pénzügyi szolgáltatási ágazatokban végzett tevékenységek eltérő jellegéből eredő sajátos jellemzőket.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

16. cikk

Egyszerűsített IKT-kockázatkezelési keretrendszer

(1) E rendelet 5–15. cikke nem alkalmazandó a következőkre: az (EU) 2015/2366 irányelv alapján mentesített kis méretű és össze nem kapcsolt befektetési vállalkozások, pénzforgalmi intézmények; a 2013/36/EU irányelv alapján mentesített azon intézmények, amelyek tekintetében a tagállamok úgy döntöttek, hogy nem alkalmazzák az e rendelet 2. cikkének (4) bekezdésében említett opciót; a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmények; és a kis méretű foglalkoztatói nyugellátást szolgáltató intézmények.

Az első albekezdés sérelme nélkül az első albekezdésben felsorolt szervezeteknek:

a) megbízható és dokumentált IKT-kockázatkezelési keretrendszert kell létrehozniuk és fenntartaniuk, amely részletezi az IKT-kockázat gyors, hatékony és átfogó kezelését célzó mechanizmusokat és intézkedéseket, többek között a releváns fizikai összetevők és infrastruktúrák védelme érdekében;

b) folyamatosan nyomon kell követniük valamennyi IKT-rendszer biztonságát és működését;

c) minimalizálniuk kell az IKT-kockázat hatását olyan megbízható, reziliens és naprakész IKT-rendszerek, -protokollok és -eszközök alkalmazásával, amelyek alkalmasak tevékenységeik végzésének és a szolgáltatások nyújtásának támogatására, valamint a hálózati és információs rendszerekben tárolt adatok rendelkezésre állásának, hitelességének, integritásának és bizalmas jellegének megfelelő fenntartására;

d) lehetővé kell tenniük a hálózati és információs rendszerekben jelentkező IKT-kockázat és -rendellenességek forrásainak azonnali azonosítását és felderítését, valamint az IKT-vonatkozású események gyors kezelését;

e) azonosítaniuk kell a harmadik fél IKT-szolgáltatóktól való főbb függőségeket;

f) biztosítaniuk kell a kritikus vagy lényeges funkciók folytonosságát olyan üzletmenet-folytonossági tervek, valamint reagálási és helyreállítási intézkedések révén, amelyek magukban foglalják legalább a biztonsági mentést és helyreállítást biztosító intézkedéseket;

g) rendszeresen tesztelniük kell az f) pontban említett terveket és intézkedéseket, valamint az a) és c) pontnak megfelelően végrehajtott kontrollok hatékonyságát;

h) adott esetben be kell építeniük az IKT-kockázatértékelési folyamatba a g) pontban említett tesztekből és a biztonsági események utólagos elemzéséből származó releváns operatív következtetéseket, és az igényeknek és az IKT-kockázati profilnak megfelelően IKT-biztonsági tudatosságnövelő programokat és digitális működési reziliencia-képzéseket kell kidolgozniuk a személyzet és a vezetés számára.

(2) Az (1) bekezdés második albekezdésének a) pontjában említett IKT-kockázatkezelési keretrendszert dokumentálni kell, és a felügyeleti utasításoknak megfelelően időszakonként és minden jelentős IKT-vonatkozású esemény bekövetkezésekor felül kell vizsgálni. A keretet folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján. Az illetékes hatóság számára – a kérésére – jelentést kell benyújtani az IKT-kockázatkezelési keretrendszer felülvizsgálatáról.

(3) Az EFH-knak a vegyes bizottság keretében, az ENISA-val egyeztetve, közös szabályozástechnikai standardtervezeteket kell kidolgozniuk annak érdekében, hogy:

a) részletesen meghatározzák az (1) bekezdés második albekezdésének a) pontjában említett IKT-kockázatkezelési keretrendszerbe foglalandó elemeket;

b) részletesen meghatározzák az (1) bekezdés második albekezdésének c) pontjában említett, az IKT-kockázat hatásának minimalizálását szolgáló rendszerekkel, protokollokkal és eszközökkel kapcsolatos elemeket a hálózatok biztonságának garantálása érdekében, lehetővé téve a behatolások és az adatokkal való visszaélés elleni megfelelő biztosítékokat, valamint megőrizve az adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét;

c) részletesen meghatározzák az (1) bekezdés második albekezdésének f) pontjában említett IKT-üzletmenetfolytonossági tervek összetevőit;

d) részletesen meghatározzák az üzletmenet-folytonossági tervek tesztelésére vonatkozó szabályokat, és biztosítsák az (1) bekezdés második albekezdésének g) pontjában említett kontrollok hatékonyságát, és biztosítsák, hogy az ilyen tesztelés során kellő figyelmet kapjanak az olyan helyzetek, amikor egy kritikus vagy fontos funkció ellátása elfogadhatatlan színvonalúra csökken vagy meghiúsul;

e) részletesen meghatározzák a (2) bekezdésben említett, az IKT-kockázatkezelési keretrendszer felülvizsgálatáról szóló jelentés tartalmát és formátumát.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

III. FEJEZET

Az IKT-vonatkozású események kezelése, osztályozása és bejelentése

17. cikk

Az IKT-vonatkozású események kezelési folyamata

(1) A pénzügyi szervezeteknek meg kell határozniuk, ki kell alakítaniuk és végre kell hajtaniuk az IKT-vonatkozású események észlelésére, kezelésére és bejelentésére szolgáló folyamatot.

(2) A pénzügyi szervezetek nyilvántartanak valamennyi IKT-vonatkozású eseményt és jelentős kiberfenyegetést. A pénzügyi szervezetek megfelelő eljárásokat és folyamatokat alakítanak ki, hogy biztosítsák az IKT-vonatkozású események következetes és integrált monitorozását, kezelését és utókövetését, biztosítsák a kiváltó okok azonosítását, dokumentálását és kezelését az ilyen események előfordulásának megelőzése érdekében.

(3) Az IKT-vonatkozású események (1) bekezdésben említett kezelési folyamata keretében:

a) korai előrejelző mutatókat kell bevezetni;

b) a 18. cikk (1) bekezdésében meghatározott kritériumok alapján meg kell határozni az IKT-vonatkozású események azonosítását, nyomon követését, naplózását, kategorizálását és osztályozását biztosító, az események prioritásának és súlyosságának és az érintett szolgáltatások kritikusságának megfelelő eljárásokat;

c) ki kell jelölni azon szerep- és felelősségi köröket, amelyeket az IKT-vonatkozású események egyes típusai és forgatókönyvei tekintetében aktiválni kell;

d) meg kell határozni a személyzettel, a külső érdekelt felekkel és a médiával a 14. cikkel összhangban folytatott kommunikációra, az ügyfelek értesítésére, a belső eszkalációs eljárásokra – ideértve az IKT-vonatkozású ügyfélpanaszok kezelését is –, továbbá adott esetben a partner pénzügyi szervezetek tájékoztatására vonatkozó terveket;

e) biztosítani kell, hogy legalább a jelentős IKT-vonatkozású eseményeket bejelentik a releváns felső vezetésnek, és tájékoztatni kell a vezető testületet legalább a jelentős IKT-vonatkozású eseményekről, ismertetve az ilyen IKT-vonatkozású események eredményeként megállapítandó hatást, reagálást és további kontrollokat;

f) meg kell határozni az IKT-vonatkozású eseményekre való reagálást célzó eljárásokat a hatások enyhítése, valamint annak biztosítása érdekében, hogy a szolgáltatások mielőbb működőképessé és biztonságossá váljanak.

18. cikk

Az IKT-vonatkozású események és a kiberfenyegetések osztályozása

(1) A pénzügyi szervezeteknek a következő kritériumok alapján kell osztályozniuk az IKT-vonatkozású eseményeket, és megállapítaniuk azok hatását:

a) az IKT-vonatkozású esemény által érintett ügyfelek vagy pénzügyi partnerek száma és/vagy relevanciája, és – adott esetben – az érintett tranzakciók mennyisége vagy száma, valamint az, hogy az IKT-vonatkozású eseménynek van-e a hírnevet érintő hatása;

b) az IKT-vonatkozású esemény időtartama, beleértve a leállási időt is;

c) az IKT-vonatkozású esemény földrajzi kiterjedése az érintett területek vonatkozásában, különösen, ha az esemény kettőnél több tagállamot érint;

d) az IKT-vonatkozású eseménnyel járó adatvesztések az adatok rendelkezésre állásához, hitelességéhez, integritásához vagy bizalmas jellegéhez kapcsolódóan;

e) az érintett szolgáltatások kritikussága, beleértve a pénzügyi szervezet ügyleteit és működését is;

f) az IKT-vonatkozású esemény gazdasági hatása – ideértve különösen a közvetlen és közvetett költségeket és veszteségeket – abszolút és relatív értelemben egyaránt.

(2) A pénzügyi szervezetek a kiberfenyegetéseket jelentősnek minősítik a kockázatnak kitett szolgáltatások kritikussága alapján, ideértve a pénzügyi szervezet ügyleteit és műveleteit, a megcélzott ügyfelek vagy pénzügyi partnerek számát és/vagy relevanciáját, valamint a kockázatnak kitett területek földrajzi eloszlását.

(3) Az EFH-knak a vegyes bizottság keretében, az EKB-val és az ENISA-val egyeztetve, közös szabályozástechnikai standardtervezeteket kell kidolgozniuk, amelyekben részletesen meghatározzák a következőket:

a) az (1) bekezdésben meghatározott kritériumok, ideértve azon lényegességi küszöbértékeket, amelyek alapján megállapíthatók azon jelentős IKT-vonatkozású események, vagy adott esetben jelentős pénzforgalmi vonatkozású működési vagy biztonsági események, amelyek a 19. cikk (1) bekezdésében előírt bejelentési kötelezettség alá tartoznak;

b) azon kritériumok, amelyek alapján az illetékes hatóságok értékelik a jelentős IKT-vonatkozású események vagy adott esetben a jelentős pénzforgalmi vonatkozású működési vagy biztonsági események relevanciáját más tagállamokban a releváns illetékes hatóságok szempontjából, továbbá a jelentős IKT-vonatkozású eseményekkel vagy adott esetben a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekkel kapcsolatos bejelentések azon részletei, amelyeket a 19. cikk (6) és (7) bekezdésének megfelelően meg kell osztaniuk más illetékes hatóságokkal;

c) az e cikk (2) bekezdésében meghatározott kritériumok, beleértve a jelentős kiberfenyegetések meghatározására vonatkozó, magasnak minősülő lényegességi küszöbértékeket.

(4) Az e cikk (3) bekezdésében említett közös szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a 4. cikk (2) bekezdésében meghatározott kritériumokat, valamint a nemzetközi szabványokat, az ENISA által kidolgozott és közzétett iránymutatásokat és specifikációkat, ideértve adott esetben a más gazdasági ágazatokra vonatkozó specifikációkat is. A 4. cikk (2) bekezdésében meghatározott kritériumok alkalmazása céljából az EFH-knak megfelelően figyelembe kell venniük a mikrovállalkozások és a kis- és középvállalkozások azon igényét, hogy elegendő erőforrást és kapacitást mozgósítsanak az IKT-vonatkozású események gyors kezelésének biztosítása érdekében.

Az EFH-knak az említett közös szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban a (3) bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

19. cikk

A jelentős IKT-vonatkozású események bejelentése és a jelentős kiberfenyegetésekről szóló önkéntes értesítés

(1) A pénzügyi szervezeteknek a jelentős IKT-vonatkozású eseményeket az e cikk (4) bekezdésével összhangban be kell jelenteniük a 46. cikkben említett releváns illetékes hatóságnak.

Amennyiben egy pénzügyi szervezet a 46. cikkben említett illetékes nemzeti hatóságok közül egynél több felügyelete alá tartozik, a tagállamok egyetlen illetékes hatóságot jelölnek ki az e cikkben előírt funkciók és kötelezettségek végrehajtásáért felelős releváns illetékes hatóságként.

Az 1024/2013/EU rendelet 6. cikkének (4) bekezdésével összhangban jelentősnek minősített hitelintézetek bejelentik a jelentős IKT-vonatkozású eseményeket a 2013/36/EU irányelv 4. cikkével összhangban kijelölt releváns illetékes nemzeti hatóságnak, amely haladéktalanul továbbítja az említett jelentést az EKB-nak.

Az első albekezdés alkalmazásában a pénzügyi szervezeteknek a releváns információk összegyűjtését és elemzését követően a 20. cikkben említett sablonok felhasználásával el kell készíteniük az e cikk (4) bekezdésében említett kezdeti értesítést és jelentéseket, és be kell nyújtaniuk azokat az illetékes hatóságnak. Abban az esetben, ha technikai okokból lehetetlen a kezdeti értesítés mintadokumentum használatával történő benyújtása, a pénzügyi szervezeteknek alternatív módon kell értesíteniük arról az illetékes hatóságot.

A (4) bekezdésben említett kezdeti értesítésnek és jelentéseknek tartalmazniuk kell minden olyan információt, amelyre az illetékes hatóságnak szüksége van a jelentős IKT-vonatkozású esemény jelentőségének megállapításához és esteleges határokon átnyúló hatásainak értékeléséhez.

A pénzügyi szervezet által a releváns illetékes hatóság felé történő, az első albekezdés alapján történő bejelentés sérelme nélkül a tagállamok megállapíthatják továbbá, hogy a pénzügyi szervezetek egy részének vagy mindegyikének az e cikk (4) bekezdésében említett kezdeti értesítést és minden egyes jelentést be kell nyújtaniuk a 20. cikkben említett sablonok felhasználásával az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságoknak vagy számítógép-biztonsági eseményekre reagáló csoportoknak (CSIRT-ek) is.

(2) A pénzügyi szervezetek önkéntes alapon értesíthetik a releváns illetékes hatóságot a jelentős kiberfenyegetésekről, amennyiben úgy ítélik meg, hogy a fenyegetés relevanciával bír a pénzügyi rendszer, a szolgáltatás igénybevevői vagy az ügyfelek számára. A releváns illetékes hatóság átadhatja az ilyen információkat a (6) bekezdésben említett egyéb releváns hatóságoknak.

Az 1024/2013/EU rendelet 6. cikkének (4) bekezdésével összhangban jelentősnek minősített hitelintézetek önkéntes alapon értesíthetik a jelentős kiberfenyegetésekről a 2013/36/EU irányelv 4. cikkével összhangban kijelölt, releváns illetékes nemzeti hatóságot, amelynek haladéktalanul továbbítania kell az értesítést az EKB-nak.

A tagállamok dönthetnek úgy, hogy azon pénzügyi szervezetek, amelyek az első albekezdéssel összhangban önkéntes alapon értesítést küldenek, az említett értesítést az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott CSIRT-eknek is továbbíthatják.

(3) Amennyiben jelentős IKT-vonatkozású esemény következik be, és hatással van az ügyfelek pénzügyi érdekeire, a pénzügyi szervezeteknek – amint az eseményt észlelik – indokolatlan késedelem nélkül tájékoztatniuk kell az ügyfeleiket a jelentős IKT-vonatkozású eseményről és az ilyen esemény káros hatásainak enyhítésére tett intézkedésekről.

Jelentős kiberfenyegetés esetén a pénzügyi szervezeteknek adott esetben tájékoztatniuk kell a potenciálisan érintett ügyfeleiket minden olyan megfelelő védelmi intézkedésről, amelyek meghozatalát az utóbbiak mérlegelhetik.

(4) A pénzügyi szervezeteknek a 20. cikk első bekezdése a) pontjának ii. alpontjával összhangban megállapítandó határidőkön belül be kell nyújtaniuk a releváns illetékes hatóságnak a következőket:

a) kezdeti értesítés;

b) időközi jelentés az a) pontban említett kezdeti értesítést követően, amint az eredeti biztonsági esemény állapota jelentősen megváltozik, vagy a jelentős IKT-vonatkozású esemény kezelése a rendelkezésre álló új információk alapján módosul, amelyet adott esetben aktualizált bejelentéseknek kell követniük minden olyan alkalommal, amikor releváns állapotfrissítés áll rendelkezésre, valamint az illetékes hatóság külön kérésére;

c) zárójelentés, amikor lezárult a kiváltó okok elemzése, függetlenül attól, hogy enyhítő intézkedések végrehajtására sor került-e már, és amikor rendelkezésre állnak a hatással kapcsolatban a becslések helyettesítésére alkalmas tényadatok.

(5) A pénzügyi szervezetek az uniós és nemzeti ágazati jogszabályokkal összhangban kiszervezhetik az e cikk szerinti bejelentési kötelezettségeket harmadik fél szolgáltatónak. Az ilyen kiszervezés esetén a pénzügyi szervezet továbbra is teljes felelősséggel tartozik a biztonsági eseményre vonatkozó bejelentési követelmények teljesítéséért.

(6) A (4) bekezdésben említett kezdeti értesítés és minden egyes jelentés átvételét követően az illetékes hatóságnak kellő időben részletes tájékoztatást kell nyújtania a jelentős IKT-vonatkozású eseményről a következő címzetteknek – adott esetben – a vonatkozó hatáskörük alapján:

a) az EBH, az ESMA vagy az EIOPA;

b) a 2. cikk (1) bekezdésének a), b) és d) pontjában említett pénzügyi szervezetek esetében az EKB;

c) az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságok, egyedüli kapcsolattartó pontok vagy CSIRT-ek;

d) a 2014/59/EU irányelv 3. cikkében említett szanálási hatóságok és az Egységes Szanálási Testület (ESZT) a 806/2014/EU európai parlamenti és tanácsi rendelet ([37]) 7. cikkének (2) bekezdésében említett szervezetek, valamint a 806/2014/EU rendelet 7. cikke (4) bekezdésének b) pontjában és (5) bekezdésében említett szervezetek és csoportok tekintetében, ha az ilyen adatok olyan eseményekre vonatkoznak, amelyek kockázatot jelentenek a 2014/59/EU irányelv 2. cikkének 35. pontja értelmében vett kritikus funkciók biztosítására nézve; és

e) a nemzeti jog szerinti egyéb releváns hatóságok.

(7) Az információk (6) bekezdés szerinti kézhezvételét követően az EBH, az ESMA vagy az EIOPA, valamint az EKB – az ENISA-val egyeztetve és a releváns illetékes hatósággal együttműködve – értékeli, hogy a jelentős IKT-vonatkozású esemény releváns-e más tagállamok illetékes hatóságai számára. Az említett értékelést követően az EBH, az ESMA vagy az EIOPA ennek megfelelően a lehető leghamarabb értesíti más tagállamokban a releváns illetékes hatóságokat. Az EKB értesítést küld a Központi Bankok Európai Rendszere tagjainak a fizetési rendszer szempontjából releváns kérdésekről. Az értesítés alapján az illetékes hatóságoknak adott esetben meg kell hozniuk minden szükséges intézkedést a pénzügyi rendszer közvetlen stabilitásának megóvása érdekében.

([37]) Az Európai Parlament és a Tanács 806/2014/EU rendelete (2014. július 15.) a hitelintézeteknek és bizonyos befektetési vállalkozásoknak az Egységes Szanálási Mechanizmus keretében történő szanálására vonatkozó egységes szabályok és egységes eljárás kialakításáról, valamint az Egységes Szanálási Alap létrehozásáról és az 1093/2010/EU rendelet módosításáról (HL L 225., 2014.7.30., 1. o.).

(8) Az ESMA által e cikk (7) bekezdése alapján küldendő értesítés nem érinti az illetékes hatóság azon felelősségét, hogy sürgősen továbbítsa a jelentős IKT-vonatkozású esemény részleteit a fogadó tagállambeli releváns hatóságnak, amennyiben valamely központi értéktár jelentős határokon átnyúló tevékenységet folytat a fogadó tagállamban, a jelentős IKT-vonatkozású esemény valószínűleg súlyos következményekkel jár a fogadó tagállam pénzügyi piacaira nézve, és amennyiben az illetékes hatóságok között együttműködési megállapodások vannak érvényben a pénzügyi szervezetek felügyeletéhez kapcsolódóan.

20. cikk

A bejelentések tartalmának és a sablonjainak harmonizációja

Az EFH-k a vegyes bizottság keretében, valamint az ENISA-val és az EKB-val konzultálva, kidolgozzák a következőket:

a) közös szabályozástechnikai standardtervezetek, amelyek:

   i. megállapítják a jelentős IKT-vonatkozású eseményekre vonatkozó jelentések tartalmát, hogy azok tükrözzék a 18. cikk (1) bekezdésében meghatározott kritériumokat, és további elemeket építenek be, így például a bejelentés más tagállamok számára való relevanciájának megállapítására vonatkozó részleteket, valamint azt, hogy az esemény jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseménynek minősül-e vagy sem;

   ii. meghatározzák a 19. cikk (4) bekezdésében említett kezdeti értesítésre és minden egyes jelentésre vonatkozó határidőket;

   iii. meghatározzák a jelentős kiberfenyegetésekről szóló értesítés tartalmát.

   Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint a szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét és különösen annak biztosítása céljából, hogy e bekezdés a) pontja ii. alpontjának alkalmazásában a különböző határidők adott esetben tükrözhessék a pénzügyi ágazatok sajátosságait az IKT-vonatkozású események e rendelet és az (EU) 2022/2555 irányelv alapján történő bejelentésére vonatkozó következetes megközelítés fenntartásának sérelme nélkül. Az EFH-knak adott esetben meg kell indokolniuk, amennyiben eltérnek az említett irányelvvel összefüggésben alkalmazott megközelítésektől.

b) közös végrehajtás-technikai standardtervezetek, amelyek a pénzügyi szervezetek számára rögzítik a jelentős IKT-vonatkozású esemény bejelentésére és a jelentős kiberfenyegetésről szóló értesítésre szolgáló szabványos űrlapokat, sablonokat és eljárásokat.

Az EFH-knak az első bekezdés a) pontjában említett közös szabályozástechnikai standardtervezeteket és az első bekezdés b) pontjában említett közös végrehajtás-technikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első bekezdés a) pontjában említett közös szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az első bekezdés b) pontjában említett közös végrehajtás-technikai standardokat.

21. cikk

A jelentős IKT-vonatkozású események központosított bejelentése

(1) Az EFH-knak a vegyes bizottság keretében, valamint az EKB-val és az ENISA-val konzultálva, közös jelentésben értékelniük kell annak lehetőségét, hogy az eseménybejelentést még nagyobb mértékben központosítsák azáltal, hogy egységes uniós központi adatbázist hoznak létre a jelentős IKT-vonatkozású események pénzügyi szervezetek általi bejelentése céljára. A közös jelentésben meg kell vizsgálni, hogy a felügyeleti konvergencia növelése érdekében milyen lehetőségek vannak az IKT-vonatkozású események bejelentésével kapcsolatos információáramlás megkönnyítésére, a járulékos költségek csökkentésére, valamint a tematikus elemzések megalapozására.

(2) Az (1) bekezdésben említett közös jelentésnek legalább a következő elemeket kell magában foglalnia:

a) az egységes európai uniós adatbázis létrehozásának előfeltételei;

b) az előnyök, a korlátok és a kockázatok, ideértve az érzékeny információk magas koncentrációjához kapcsolódó kockázatokat is;

c) az egyéb releváns bejelentési rendszerekkel kapcsolatos átjárhatóság biztosításához szükséges képesség;

d) az üzemeltetés elemei;

e) a tagság feltételei;

f) az egységes uniós adatbázishoz a pénzügyi szervezetek és az illetékes nemzeti hatóságok által való hozzáférés technikai feltételei;

g) az egységes uniós adatbázist támogató működési platform kialakításával felmerülő pénzügyi költségek előzetes értékelése, ideértve a szükséges szakértelmet is.

(3) Az EFH-knak az (1) bekezdésben említett jelentést 2025. január 17-ig be kell nyújtaniuk az Európai Parlamentnek, a Tanácsnak és a Bizottságnak.

22. cikk

Felügyeleti visszajelzés

(1) Az (EU) 2022/2555 irányelv szerinti CSIRT-ek által – adott esetben – a nemzeti joggal összhangban biztosítható technikai input, tanácsadás vagy korrekciós intézkedések, valamint későbbi utókövetés sérelme nélkül az illetékes hatóságnak a 19. cikk (4) bekezdésében említett kezdeti értesítés és minden egyes jelentés átvételekor vissza kell igazolnia azok kézhezvételét, és – amennyiben megvalósítható – kellő időben releváns és arányos visszajelzést vagy magas szintű iránymutatást nyújthat a pénzügyi szervezetnek, különösen a hasonló fenyegetésekkel kapcsolatos releváns anonimizált adatok és hírszerzés rendelkezésre bocsátásával, továbbá megvitathatja a pénzügyi szervezet szintjén alkalmazott korrekciós intézkedéseket, valamint a pénzügyi ágazat egészét érintő káros hatások minimalizálását és csökkentését célzó módokat. A pénzügyi szervezetek továbbra is teljes felelősséggel tartoznak a 19. cikk (1) bekezdése szerint bejelentett IKT-vonatkozású események kezeléséért és következményeiért, a kapott felügyeleti visszajelzések sérelme nélkül.

(2) Az EFH-knak a vegyes bizottság keretében anonimizált és összesített formában évente be kell számolniuk a jelentős IKT-vonatkozású eseményekről, amelyekről az illetékes hatóságoknak a 19. cikk (6) bekezdésével összhangban részletes tájékoztatást kell nyújtaniuk, meghatározva legalább a jelentős IKT-vonatkozású események számát, jellegét és a pénzügyi szervezetek vagy ügyfelek működésére gyakorolt hatását, a meghozott korrekciós intézkedéseket és a keletkezett költségeket.

Az EFH-knak figyelmeztetéseket kell kibocsátaniuk és magas szintű statisztikákat készíteniük, hogy támogassák az IKT-fenyegetési és -sérülékenységi értékeléseket.

23. cikk

Hitelintézeteket, pénzforgalmi intézményeket, számlainformációkat összesítő szolgáltatókat és elektronikuspénz-kibocsátó intézményeket érintő, pénzforgalmi vonatkozású működési vagy biztonsági események

Az e fejezetben megállapított követelmények alkalmazandók a pénzforgalmi vonatkozású működési vagy biztonsági eseményekre, valamint a jelentős pénzforgalmi vonatkozású működési vagy biztonsági eseményekre is, amennyiben azok hitelintézeteket, pénzforgalmi intézményeket, számlainformációkat összesítő szolgáltatókat és elektronikuspénz-kibocsátó intézményeket érintenek.

IV. FEJEZET

A digitális működési reziliencia tesztelése

24. cikk

A digitális működési reziliencia tesztelésének végrehajtására vonatkozó általános követelmények

(1) Az IKT-vonatkozású események kezelésére való felkészültség értékelése, a digitális működési reziliencia gyengeségeinek, hiányosságainak és lefedetlenségeinek azonosítása, valamint a korrekciós intézkedések gyors végrehajtása érdekében a mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek a 4. cikk (2) bekezdésében meghatározott kritériumok figyelembevételével a digitális működési reziliencia tesztelésére megbízható és átfogó programot kell kialakítaniuk, fenntartaniuk és felülvizsgálniuk, a 6. cikkben említett IKT-kockázatkezelési keretrendszer integráns részeként.

(2) A digitális működési reziliencia tesztelését szolgáló programnak magában kell foglalnia a 25. és 26. cikkel összhangban alkalmazandó értékeléseket, teszteket, módszertanokat, gyakorlatokat és eszközöket.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek az e cikk (1) bekezdésében említett, a digitális működési reziliencia tesztelését szolgáló program lefolytatása során – a 4. cikk (2) bekezdésében meghatározott kritériumokat figyelembe véve – kockázatalapú megközelítést kell követniük, kellően tekintetbe véve az IKT-kockázat változó környezetét, minden olyan konkrét kockázatot, amelynek az érintett pénzügyi szervezet ki van vagy ki lehet téve, az információs vagyonelemek és a nyújtott szolgáltatások kritikusságát, valamint a pénzügyi szervezet által megfelelőnek tartott bármely egyéb tényezőt.

(4) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek biztosítaniuk kell, hogy a teszteket független belső vagy külső fél hajtsa végre. Amennyiben a teszteket belső tesztelő végzi, a pénzügyi szervezeteknek elegendő erőforrást kell elkülöníteniük, és biztosítaniuk kell, hogy a teszt tervezési és végrehajtási szakaszában ne legyenek összeférhetetlenségek.

(5) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek eljárásokat és szabályzatokat kell kialakítaniuk a tesztek lefolytatása során feltárt valamennyi probléma rangsorolása, osztályozása és orvoslása céljából, továbbá ki kell alakítaniuk azon belső validálási módszertanokat, amelyekkel megerősíthető, hogy a szervezet maradéktalanul kezelte az azonosított gyengeségeket és hiányosságokat.

(6) A mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek legalább évente biztosítaniuk kell, hogy megfelelő teszteket végezzenek a kritikus vagy fontos funkciókat támogató valamennyi IKT-rendszeren és -alkalmazáson.

25. cikk

Az IKT-eszközök és -rendszerek tesztelése

(1) A 24. cikkben említett, a digitális működési reziliencia tesztelését szolgáló programnak – a 4. cikk (2) bekezdésében meghatározott kritériumokkal összhangban – biztosítania kell olyan megfelelő tesztek elvégzését, mint például sérülékenységi értékelések és ellenőrzések, nyílt forrású elemzések, hálózatbiztonsági értékelések, eltéréselemzések, fizikai biztonsági felülvizsgálatok, kérdőívek és szoftveres átvilágítási megoldások, lehetőség szerint forráskódvizsgálatok, forgatókönyv-alapú tesztek, kompatibilitás-tesztelés, teljesítmény-tesztelés, végpontok közötti tesztelés és behatolási tesztelés.

(2) A központi értéktáraknak és a központi szerződő feleknek sérülékenységi vizsgálatokat kell végezniük a pénzügyi szervezet kritikus vagy fontos funkcióit támogató új vagy meglévő alkalmazások és infrastrukturális összetevők, valamint IKT-szolgáltatások bevezetése vagy újbóli bevezetése előtt.

(3) A mikrovállalkozásoknak az (1) bekezdésben említett teszteket a kockázatalapú megközelítést az IKT-tesztelés stratégiai tervezésével kombinálva kell végrehajtaniuk, kellően figyelembe véve, hogy kiegyensúlyozott megközelítést kell fenntartani egyrészt az e cikkben előírt IKT-tesztelésre fordítandó erőforrás-nagyságrend és idő, másrészt a sürgősség, a kockázat típusa, az információs vagyonelemek és nyújtott szolgáltatások kritikussága, valamint bármely egyéb releváns tényező között, beleértve a pénzügyi szervezet számításba vett kockázatok vállalására való képességét is.

26. cikk

Az IKT-eszközök, -rendszerek és -folyamatok TLPT-n alapuló fejlett tesztelése

(1) A 16. cikk (1) bekezdésének első albekezdésében említett szervezetektől eltérő és mikrovállalkozásnak nem minősülő, az e cikk (8) bekezdésének harmadik albekezdésével összhangban azonosított pénzügyi szervezeteknek legalább 3 évente fejlett tesztelést kell végezniük a TLPT útján. Az illetékes hatóság a pénzügyi szervezet kockázati profilja alapján és a működési körülményeket figyelembe véve, szükség esetén felkérheti a pénzügyi szervezetet, hogy csökkentse vagy növelje a tesztelés gyakoriságát.

(2) Minden egyes fenyegetés alapú behatolási tesztelésnek ki kell terjednie a pénzügyi szervezet számos vagy valamennyi kritikus vagy fontos funkciójára, és azt az ilyen funkciókat támogató éles rendszereken kell lefolytatni.

A pénzügyi szervezeteknek azonosítaniuk kell a kritikus vagy fontos funkciókat támogató valamennyi releváns, alapul szolgáló IKT-rendszert, -folyamatot és -technológiát, továbbá valamennyi releváns IKT-szolgáltatást, beleértve azokat, amelyek a harmadik fél IKT-szolgáltatókhoz kiszervezett vagy azoknak megbízásba adott kritikus vagy fontos funkciókat támogatják.

A pénzügyi szervezeteknek értékelniük kell, hogy mely kritikus vagy fontos funkciókra szükséges kiterjednie a TLPT-nek. Ezen értékelés eredménye határozza meg a TLPT pontos terjedelmét, és azt az illetékes hatóságoknak validálniuk kell.

(3) Amennyiben a TLPT harmadik fél IKT-szolgáltatókra is kiterjed, a pénzügyi szervezetnek meg kell hoznia a szükséges intézkedéseket és biztosítékokat az ilyen harmadik fél IKT-szolgáltatók TLPT-ben való részvételének biztosítása érdekében, és mindenkor teljes felelősséget kell viselnie az e rendeletnek való megfelelés biztosításáért.

(4) A (2) bekezdés első és második albekezdésének sérelme nélkül, amennyiben egy harmadik fél IKT-szolgáltatónak a (3) bekezdésben említett, TLPT-ben való közreműködéséről észszerűen feltételezhető, hogy az káros hatást gyakorol a harmadik fél IKT-szolgáltató által az e rendelet hatályán kívül eső ügyfeleknek nyújtott szolgáltatások minőségére vagy biztonságára, vagy az ilyen szolgáltatásokhoz kapcsolódó adatok bizalmasságára, a pénzügyi szervezet és a harmadik fél IKT-szolgáltató írásban megállapodhat arról, hogy a harmadik fél IKT-szolgáltató közvetlenül szerződéses megállapodást köt egy külső tesztelővel abból a célból, hogy egyetlen kijelölt pénzügyi szervezet irányítása alatt csoportos TLPT-t végezzen el több olyan pénzügyi szervezet részvételével, amelyek részére a harmadik fél IKT-szolgáltató IKT-szolgáltatásokat nyújt.

Az említett csoportos tesztelés kiterjed a pénzügyi szervezetek által a vonatkozó harmadik fél IKT-szolgáltatónak megbízásba adott kritikus vagy fontos funkciókat támogató IKT-szolgáltatások releváns körére. A csoportos tesztelést a csoportos tesztelésben részt vevő pénzügyi szervezetek által végzett TLPT-nek kell tekinteni.

A csoportos tesztelésben részt vevő pénzügyi szervezetek számát megfelelően, az érintett szolgáltatások összetettségét és típusát figyelembe véve kell kalibrálni.

(5) A pénzügyi szervezeteknek harmadik fél IKT-szolgáltatók és más érintett felek – ideértve a tesztelőket, de kizárva az illetékes hatóságokat – közreműködésével eredményes kockázatkezelési kontrollok útján mérsékelniük kell az adatokat érő bármilyen hatás, az eszközökben keletkező kár és a kritikus vagy fontos funkciók, szolgáltatások vagy műveletek zavarának kockázatát magánál a pénzügyi szervezetnél, annak partnereinél, valamint a pénzügyi ágazat egészében.

(6) A teszt befejezésekor, a jelentések és korrekciós tervek jóváhagyását követően a pénzügyi szervezet és adott esetben a külső tesztelők a (9) vagy (10) bekezdéssel összhangban kijelölt hatóság rendelkezésére bocsátják a releváns megállapítások összefoglalását, a korrekciós terveket és azon dokumentációt, amely bemutatja, hogy a TLPT-t a követelményeknek megfelelően végezték el.

(7) A hatóságoknak igazolást kell kiadniuk a pénzügyi szervezetek részére, amely megerősíti, hogy a tesztet a dokumentációban igazoltak szerint a követelményeknek megfelelően hajtották végre, annak érdekében, hogy az illetékes hatóságok között lehetővé váljon a fenyegetés alapú behatolási tesztelés kölcsönös elismerése. A pénzügyi szervezet értesíti a releváns illetékes hatóságot az igazolásról, a releváns megállapítások összefoglalásáról és a korrekciós tervekről.

Az ilyen igazolást nem érintve, a pénzügyi szervezetek mindenkor teljes felelősséggel tartoznak a (4) bekezdésben említett tesztek hatásáért.

(8) A pénzügyi szervezeteknek a 27. cikkel összhangban szerződést kell kötniük a tesztelőkkel a TLPT elvégzése céljából. Amennyiben a pénzügyi szervezetek belső tesztelőket vesznek igénybe a TLPT elvégzésének céljából, három tesztenként külső tesztelőt kell megbízniuk.

Az 1024/2013/EU rendelet 6. cikke (4) bekezdésének megfelelően jelentősnek minősített hitelintézetek a 27. cikk (1) bekezdése a)–e) pontjának megfelelően csak külső tesztelőket alkalmazhatnak.

Az illetékes hatóságoknak a 4. cikk (2) bekezdésében meghatározott kritériumok figyelembevételével, a következők értékelése alapján kell kiválasztaniuk a TLPT elvégzésére kötelezett pénzügyi szervezeteket:

a) hatás-vonatkozású tényezők, így különösen az a mérték, amennyire a pénzügyi szervezet által nyújtott szolgáltatások és elvégzett tevékenységek hatnak a pénzügyi ágazatra;

b) esetleges pénzügyi stabilitási megfontolások, ideértve a pénzügyi szervezet uniós vagy nemzeti léptékű rendszerszintű jellegét, az esettől függően;

c) a pénzügyi szervezet vagy az érintett technológiai elemek egyedi IKT-kockázati profilja és IKT-érettségi szintje.

(9) A tagállamok kijelölhetnek egyetlen hatóságot a pénzügyi szektorban, hogy feleljen a pénzügyi szektorban nemzeti szinten a TLPT-vonatkozású ügyekért, és az e célból szükséges valamennyi hatáskörrel és feladattal megbízzák azt.

(10) Az e cikk (9) bekezdésének megfelelő kijelölés hiányában és a TLPT elvégzésére kötelezett pénzügyi szervezetek kiválasztására vonatkozó hatáskör sérelme nélkül, az illetékes hatóság az e cikkben és a 27. cikkben említett feladatok egy részének vagy mindegyikének ellátását átruházhatja egy másik nemzeti hatóságra a pénzügyi szektorban.

(11) Az EFH-knak az EKB-val egyetértésben közös szabályozástechnikai standardtervezeteket kell kidolgozniuk a TIBER–EU keretnek megfelelően, a következők részletes meghatározása érdekében:

a) a (8) bekezdés második albekezdésének alkalmazása céljából használt kritériumok;

b) a belső tesztelők igénybevételére vonatkozó követelmények és standardok;

c) a következőkre vonatkozó követelmények:

   i. a (2) bekezdésben említett TLPT hatóköre;

   ii. a tesztelési folyamat egyes szakaszaiban követendő tesztelési módszertan és megközelítés;

   iii. a tesztelés eredményei, lezárása és korrekciós szakaszai;

d) az egynél több tagállamban működő pénzügyi szervezetek körében elvégzendő TLPT végrehajtásához és e tesztelés kölcsönös elismerésének az elősegítéséhez szükséges felügyeleti és egyéb releváns együttműködés típusa a megfelelő szintű felügyeleti részvétel, valamint a pénzügyi alágazatok vagy a helyi pénzügyi piacok sajátos igényeihez igazodó, rugalmas végrehajtás biztosítása érdekében.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak kellő figyelmet kell fordítaniuk a különböző pénzügyi szolgáltatási ágazatok tevékenységeinek eltérő jellegéből eredő sajátosságokra.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

27. cikk

A TLPT lefolytatására vonatkozó, a tesztelőknek előírt követelmények

(1) A pénzügyi szervezetek a TLPT lefolytatására csak olyan tesztelőket vehetnek igénybe:

a) amelyek a legnagyobb fokú alkalmassággal és szakmai hírnévvel rendelkeznek;

b) amelyek rendelkeznek technikai és szervezeti képességekkel, valamint speciális szakértelmet mutatnak fel a fenyegetettséggel kapcsolatos hírszerzés, a behatolási tesztelés és a saját támadóerős (red team) tesztelés terén;

c) amelyeket egy tagállambeli akkreditációs testület tanúsított, vagy amelyek formális magatartási kódexek vagy etikai keretek szerint járnak el;

d) amelyek független bizonyosságot vagy audit jelentést biztosítanak a TLPT lefolytatásával összefüggő kockázatok megbízható kezelésével kapcsolatban, ideértve a pénzügyi szervezet bizalmas adatainak kellő védelmét és a pénzügyi szervezet üzleti kockázataival kapcsolatos jogorvoslatot is;

e) amelyek releváns szakmai felelősségbiztosítások révén megfelelően és teljeskörűen biztosítva vannak, többek között a szakmai kötelezettségmulasztás és a gondatlanság kockázataival szemben.

(2) A belső tesztelők igénybevétele során a pénzügyi szervezeteknek biztosítaniuk kell, hogy az (1) bekezdésben foglalt követelmények mellett, a következő feltételek is teljesüljenek:

a) az ilyen igénybevételt a releváns illetékes hatóság vagy a 26. cikk (9) és (10) bekezdésével összhangban kijelölt egyetlen hatóság jóváhagyta;

b) a releváns illetékes hatóság meggyőződött arról, hogy a pénzügyi szervezet elegendő célzott forrást különített el, és biztosította az összeférhetetlenség elkerülését a teszt tervezési és végrehajtási szakaszában; és

c) a fenyegetettséggel kapcsolatos hírszerzés nyújtója a pénzügyi szervezeten kívül működik.

(3) A pénzügyi szervezeteknek biztosítaniuk kell, hogy a külső tesztelőkkel kötött szerződések előírják a TLPT eredményeinek megbízható kezelését, továbbá azt, hogy az adatkezelés, ezen belül az adatok előállítása, tárolása, összesítése, előkészítése, bejelentése, közlése vagy megsemmisítése ne járjon kockázattal a pénzügyi szervezet számára.

V. FEJEZET

A harmadik féltől eredő IKT-kockázat kezelése

I. szakasz

A harmadik féltől eredő IKT-kockázat megbízható kezelésének alapelvei

28. cikk

Általános elvek

(1) A pénzügyi szervezeteknek a harmadik féltől eredő IKT-kockázatot az IKT-kockázat integráns összetevőjeként kell kezelniük a 6. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszerükön belül és a következő elvekkel összhangban:

a) azon pénzügyi szervezeteknek, amelyek üzleti tevékenységük folytatásához IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodást kötöttek, mindenkor teljes felelősséggel kell tartozniuk az e rendeletben és az alkalmazandó, pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt kötelezettségeknek való megfelelésért;

b) a pénzügyi szervezeteknek a harmadik féltől eredő IKT-kockázat kezelését az arányosság elvének megfelelően, a következők figyelembevételével kell megvalósítaniuk:

i. az IKT-vonatkozású függőségek jellege, nagyságrendje, összetettsége és fontossága;

ii. a harmadik fél IKT-szolgáltatókkal kötött, IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokból eredő kockázatok, figyelembe véve a vonatkozó szolgáltatás, folyamat vagy funkció kritikusságát vagy fontosságát, valamint a pénzügyi szolgáltatások és tevékenységek folytonosságára és rendelkezésre állására egyedi és csoportszinten gyakorolt potenciális hatást.

(2) Az IKT-kockázatkezelési keretrendszerük részeként a 16. cikk (1) bekezdésének első albekezdésében említett szervezetektől eltérő és mikrovállalkozásnak nem minősülő pénzügyi szervezeteknek – adott esetben a 6. cikk (9) bekezdésében említett, több beszállítóra épülő stratégia figyelembevételével – a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát kell elfogadniuk és rendszeresen felülvizsgálniuk. A harmadik féltől eredő IKT-kockázatra vonatkozó azon stratégiának, amelyet az egyedi szervezet szintjén, valamint adott esetben szubkonszolidált és konszolidált alapon is alkalmazni kell, magában kell foglalnia a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkozó szabályzatot. A vezető testületnek a pénzügyi szervezet általános kockázati profiljának, valamint az üzleti szolgáltatások nagyságrendjének és összetettségének értékelése alapján rendszeresen felül kell vizsgálnia a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokkal kapcsolatban azonosított kockázatokat.

(3) IKT-kockázatkezelési keretrendszerük részeként a pénzügyi szervezeteknek az egyedi szervezet szintjén, valamint szubkonszolidált és konszolidált szinten információ-nyilvántartást kell vezetniük és naprakészen tartaniuk a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló valamennyi szerződéses megállapodásról.

Az első albekezdésben említett szerződéses megállapodásokat megfelelően dokumentálni kell, megkülönböztetve azokat, amelyek kiterjednek a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokra, és azokat, amelyek nem.

A pénzügyi szervezeteknek legalább évente jelentést kell tenniük az illetékes hatóságoknak az IKT-szolgáltatások igénybevételéről szóló új megállapodások számáról, a harmadik fél IKT-szolgáltatók kategóriáiról, a szerződéses megállapodások típusairól, valamint a nyújtott IKT-szolgáltatásokról és -funkciókról.

A pénzügyi szervezeteknek az illetékes hatóság kérésére annak rendelkezésére kell bocsátaniuk a teljes információ-nyilvántartást, vagy a kérésnek megfelelően annak meghatározott részeit, a pénzügyi szervezet eredményes felügyeletéhez szükségesnek ítélt bármely információval együtt.

A pénzügyi szervezeteknek időben tájékoztatniuk kell az illetékes hatóságot bármely, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló, tervezett szerződéses megállapodásról, valamint arról, ha egy funkció kritikussá vagy fontossá válik.

(4) Az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások megkötése előtt a pénzügyi szervezetek:

a) értékelik, hogy a szerződéses megállapodás érinti-e kritikus vagy fontos funkciót támogató IKT-szolgáltatások igénybevételét;

b) értékelik, hogy teljesülnek-e a szerződéskötés felügyeleti feltételei;

c) azonosítják és értékelik a szerződéses megállapodással összefüggő valamennyi releváns kockázatot, beleértve annak lehetőségét is, hogy a szerződéses megállapodás hozzájárulhat a 29. cikkben említett IKT-koncentrációs kockázat erősödéséhez;

d) elvégzik a leendő harmadik fél IKT-szolgáltató teljeskörű átvilágítását, továbbá a kiválasztási és értékelési folyamatok során meggyőződnek a harmadik fél IKT-szolgáltató alkalmasságáról;

e) azonosítják és értékelik a szerződéses megállapodással esetlegesen okozott összeférhetetlenséget.

(5) A pénzügyi szervezetek csak azon harmadik fél IKT-szolgáltatókkal köthetnek szerződéses megállapodást, amelyek megfelelnek a rájuk vonatkozó információbiztonsági szabványoknak. Amennyiben az említett szerződéses megállapodások kritikus vagy fontos funkciókat érintenek, a pénzügyi szervezeteknek a megállapodások megkötése előtt kellően figyelembe kell venniük a legfrissebb és legjobb minőségű információbiztonsági szabványok harmadik fél IKT-szolgáltatók általi alkalmazását.

(6) A harmadik fél IKT-szolgáltató kapcsán a hozzáférési, ellenőrzési és audit jogok gyakorlásakor a pénzügyi szervezetek kockázatalapú megközelítés alapján előzetesen megállapítják az auditok és ellenőrzések gyakoriságát, valamint azon területeket, amelyeket az általánosan elfogadott audit standardoknak és az ilyen audit standardok alkalmazására és beépítésére vonatkozó felügyeleti utasításnak megfelelően auditálni szükséges.

Amennyiben a harmadik fél IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételéről kötött szerződéses megállapodások nagy fokú technikai összetettséggel járnak, a pénzügyi szervezetnek meg kell győződnie arról, hogy az ellenőrök – attól függetlenül, hogy belső vagy külső ellenőrről, vagy ellenőrök csoportjáról van szó – rendelkeznek-e a releváns auditok és értékelések eredményes elvégzéséhez szükséges készségekkel és ismeretekkel.

(7) A pénzügyi szervezetek biztosítják, hogy az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokat meg lehessen szüntetni a következő körülmények bármelyikének fennállása esetén:

a) a harmadik fél IKT-szolgáltató jelentősen megsérti az alkalmazandó jogszabályi, hatósági és szerződéses rendelkezéseket;

b) a harmadik féltől eredő IKT-kockázat monitorozása olyan körülményeket tár fel, amelyek alkalmasnak tekinthetők arra, hogy befolyásolják a szerződéses megállapodás keretében ellátott funkciók teljesítményét, ideértve a megállapodást vagy a harmadik fél IKT-szolgáltató helyzetét érintő lényeges módosításokat is;

c) a harmadik fél IKT-szolgáltatónál az általános IKT-kockázatkezelését érintő, bizonyítható gyengeségek tapasztalhatók és különösen azon mód, ahogyan biztosítja az adatok akár személyes, akár egyébként érzékeny adatok, vagy nem személyes adatok rendelkezésre állását, hitelességét, integritását és bizalmas jellegét;

d) amennyiben a vonatkozó szerződéses megállapodással kapcsolatos feltételek vagy körülmények eredményeként az illetékes hatóság már nem tudja eredményesen felügyelni a pénzügyi szervezetet.

(8) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások esetében a pénzügyi szervezeteknek kilépési stratégiákat kell bevezetniük. A kilépési stratégiáknak figyelembe kell venniük a harmadik fél IKT-szolgáltatók szintjén esetlegesen felmerülő kockázatokat, így különösen a részükről bekövetkező lehetséges mulasztást, a nyújtott IKT-szolgáltatások minőségének romlását, a szolgáltatások nem megfelelő nyújtása vagy meghiúsulása miatt az üzletmenetben okozott súlyos zavart, vagy a vonatkozó IKT-szolgáltatás megfelelő és folyamatos ellátásával kapcsolatban felmerülő bármely lényeges kockázatot, vagy a harmadik fél IKT-szolgáltatókkal kötött szerződéses megállapodások felmondását a (7) bekezdésben felsorolt körülmények bármelyikének esetében.

A pénzügyi szervezetek biztosítják, hogy képesek kilépni a szerződéses megállapodásokból anélkül, hogy:

a) zavar keletkezne üzleti tevékenységükben;

b) korlátozottá válna a szabályozási követelményeknek való megfelelésük;

c) sérülne az ügyfeleknek nyújtott szolgáltatások folytonossága és minősége.

A kilépési terveknek átfogóaknak kell lenniük, azokat dokumentálni kell, valamint – a 4. cikk (2) bekezdésében foglalt kritériumokkal összhangban – megfelelően tesztelni és időszakonként felülvizsgálni.

A pénzügyi szervezeteknek alternatív megoldásokat kell azonosítaniuk és átállási terveket kidolgozniuk, amelyek lehetővé teszik számukra, hogy a szerződéses megbízásba adott IKT-szolgáltatásokat és a releváns adatokat leválasszák a harmadik fél IKT-szolgáltatóról, és azokat biztonságosan és teljeskörűen alternatív szolgáltatókhoz telepítsék, vagy visszaszervezzék a saját működésükbe.

A pénzügyi szervezeteknek az üzletmenet folytonosságát biztosító, megfelelő rendkívüli intézkedésekkel kell rendelkezniük az első albekezdésben említett körülmények esetén.

(9) Az EFH-knak a vegyes bizottság keretében olyan végrehajtás-technikai standardtervezeteket kell kidolgozniuk, amelyek meghatározzák a (3) bekezdésben említett információ-nyilvántartás céljából a mintadokumentumokat, ideértve az IKT-szolgáltatások igénybevételéről szóló valamennyi szerződéses megállapodás esetében közös információkat. Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az első albekezdésben említett végrehajtás-technikai standardokat.

(10) Az EFH-knak a vegyes bizottság keretében szabályozástechnikai standardtervezeteket kell kidolgozniuk, amelyek részletesen meghatározzák a (2) bekezdésben említett szabályzat tartalmi elemeit a harmadik fél IKT-szolgáltatók által nyújtott, kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások tekintetében.

Az említett szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét. Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. január 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

29. cikk

Az IKT-koncentrációs kockázat szervezetszintű előzetes értékelése

(1) A kockázatoknak a 28. cikk (4) bekezdésének c) pontjában említett azonosítása és értékelése során a pénzügyi szervezeteknek figyelembe kell venniük azt is, hogy a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokkal kapcsolatos szerződéses megállapodás tervezett megkötése a következők valamelyikét eredményezné-e:

a) olyan harmadik fél IKT-szolgáltatóval történő szerződéskötés, amely nem helyettesíthető könnyen; vagy

b) kritikus vagy fontos funkciókat támogató IKT-szolgáltatások nyújtásával kapcsolatban többszörös szerződéses megállapodás megléte ugyanazzal a harmadik fél IKT-szolgáltatóval, vagy egymással szoros kapcsolatban álló harmadik fél IKT-szolgáltatókkal.

A pénzügyi szervezeteknek mérlegelniük kell az alternatív megoldások így például a különböző harmadik fél IKT-szolgáltatók igénybevételének előnyeit és költségeit, figyelembe véve, hogy az előirányzott megoldások illeszkednek-e és hogyan a szervezetek digitális rezilienciára vonatkozó stratégiájában meghatározott üzleti igényekhez és célkitűzésekhez.

(2) Amennyiben a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokban szerepel az a lehetőség, hogy egy harmadik fél IKT-szolgáltató egy kritikus vagy fontos funkciót támogató IKT-szolgáltatást más harmadik fél IKT-szolgáltatóknak ad alvállalkozásba, a pénzügyi szervezeteknek mérlegelniük kell az alvállalkozó ezen igénybevételéből esetlegesen származó előnyöket és kockázatokat, különösen egy harmadik országban letelepedett IKT-alvállalkozó esetén.

Amennyiben a szerződéses megállapodások kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételére vonatkoznak, a pénzügyi szervezeteknek kellő figyelmet kell fordítaniuk a harmadik fél IKT-szolgáltató csődje esetén alkalmazandó fizetésképtelenségi jogi rendelkezésekre, valamint a pénzügyi szervezet adatainak haladéktalan visszaszerzése kapcsán esetlegesen felmerülő akadályokra.

Amennyiben egy harmadik országban letelepedett, harmadik fél IKT-szolgáltatóval jön létre kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodás, a pénzügyi szervezeteknek – a második albekezdésben említett megfontolásokon túlmenően – figyelembe kell venniük az uniós adatvédelmi szabályoknak való megfelelést és a jog hatékony érvényesítését az említett harmadik országban.

Amennyiben a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodások alvállalkozó igénybevételéről rendelkeznek, a pénzügyi szervezeteknek értékelniük kell, hogy a potenciálisan hosszú vagy összetett alvállalkozói láncok érinthetik-e – és ha igen, hogyan – a szervezet képességét a szerződéses megbízásba adott funkciók teljeskörű nyomon követésére, valamint az illetékes hatóság képességét arra, hogy e tekintetben eredményesen ellássa a pénzügyi szervezet felügyeletét.

30. cikk

Főbb szerződéses rendelkezések

(1) A pénzügyi szervezet és a harmadik fél IKT-szolgáltató jogait és kötelezettségeit egyértelműen meg kell határozni, és írásban kell rögzíteni. A teljes szerződésnek magában kell foglalnia a szolgáltatási szintekre vonatkozó megállapodást is, és azt egyetlen, írásba foglalt dokumentumban kell rögzíteni, amelynek nyomtatott vagy egyéb, letölthető, tartós és hozzáférhető formátumú dokumentumban kell a felek rendelkezésére állnia.

(2) Az IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásoknak legalább a következő elemeket kell magukban foglalniuk:

a) a harmadik fél IKT-szolgáltató által biztosítandó funkciók és IKT-szolgáltatások egyértelmű és teljeskörű leírása annak feltüntetésével, hogy valamely kritikus vagy fontos funkciót támogató IKT-szolgáltatásnak vagy annak érdemi részeinek alvállalkozásba adása megengedett-e, és ha igen, milyen feltételek alkalmazandók az ilyen alvállalkozásba adásra;

b) azon helyszínek – nevezetesen azon régiók és országok –, ahol a szerződéses megbízásba vagy alvállalkozásba adott funkciók vagy IKT-szolgáltatások nyújtása és az adatkezelés történik, ideértve a tárolás helyét is, továbbá annak előírása, hogy a harmadik fél IKT-szolgáltatónak előzetesen értesítenie kell a pénzügyi szervezetet, ha tervezi az ilyen helyszínek megváltoztatását;

c) az adatok – köztük a személyes adatok – védelmével kapcsolatban a rendelkezésre állásra, hitelességre, integritásra és bizalmas jellegre vonatkozó rendelkezések;

d) az olyan személyes és nem személyes adatok – könnyen hozzáférhető formátumban történő – hozzáférésének, helyreállításának és visszaszolgáltatásának biztosítására vonatkozó rendelkezések, amelyeket a pénzügyi szervezet a harmadik fél IKT-szolgáltató fizetésképtelensége, szanálása vagy üzleti tevékenységének megszüntetése, vagy a szerződéses megállapodások megszűnése esetén kezel;

e) a szolgáltatási szintek leírása, ideértve annak frissítéseit és módosításait is;

f) a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy valamely, a pénzügyi szervezetnek nyújtott IKT-szolgáltatással kapcsolatos, IKT-biztonsági esemény bekövetkezésekor többletköltség nélkül vagy előzetesen megállapított költség mellett támogatást nyújtson a pénzügyi szervezetnek;

g) a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy teljes mértékben együttműködjön az illetékes hatóságokkal és a pénzügyi szervezet szanálási hatóságaival, beleértve az általuk kinevezett személyeket is;

h) a szerződéses megállapodások megszüntetésére vonatkozó felmondási jogok és az azokhoz kapcsolódó minimális felmondási idő az illetékes hatóságok és a szanálási hatóságok elvárásainak megfelelően;

i) a harmadik fél IKT-szolgáltatóknak a pénzügyi szervezetek 13. cikk (6) bekezdése szerinti IKT-biztonsági tudatosságot elősegítő programjain és a digitális működési rezilienciával kapcsolatos képzésein való részvételére vonatkozó feltételek.

(3) A kritikus vagy fontos funkciókat támogató IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásoknak a (2) bekezdésben említett elemeken felül tartalmazniuk kell legalább a következőket:

a) a szolgáltatási szintek teljeskörű leírása, beleértve annak frissítéseit és felülvizsgálatait is, a megállapodás szerinti szolgáltatási szinteken belüli pontos mennyiségi és minőségi teljesítménycélokkal együtt, hogy lehetővé váljon az IKT-szolgáltatásoknak a pénzügyi szervezet általi eredményes nyomon követése, és lehetővé váljon megfelelő korrekciós intézkedések indokolatlan késedelem nélküli meghozatala, amikor a megállapodás szerinti szolgáltatási szintek nem teljesülnek;

b) a harmadik fél IKT-szolgáltatóra vonatkozó felmondási idők és a pénzügyi szervezettel szembeni bejelentési kötelezettségei, ideértve bármely olyan fejlemény bejelentését, amely lényeges hatást gyakorolhat a harmadik fél IKT-szolgáltató azon képességére, hogy a megállapodás szerinti szolgáltatási szinteknek megfelelően eredményesen biztosítsa a kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokat;

c) arra vonatkozó követelmények, hogy a harmadik fél IKT-szolgáltató vezessen be és teszteljen vészhelyzeti terveket, továbbá rendelkezzen olyan IKT-biztonsági intézkedésekkel, eszközökkel és szabályzatokkal, amelyek biztosítják a megfelelő biztonsági szintet ahhoz, hogy a pénzügyi szervezet a szabályozási keretével összhangban nyújtson szolgáltatásokat;

d) a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy – a 26. és a 27. cikkben említettek szerint – részt vegyen és teljes mértékben együttműködjön a pénzügyi szervezet által végzett TLPT-ben;

e) a pénzügyi szervezet azon joga, hogy folyamatosan monitorozza a harmadik fél IKT-szolgáltató teljesítményét, ami a következőkkel jár:

i. a pénzügyi szervezet vagy egy kinevezett harmadik fél, valamint az illetékes hatóság korlátlan hozzáférési, ellenőrzési és audit joga és a releváns dokumentumokról a helyszínen való másolatkészítés joga – amennyiben azok kritikusak a harmadik fél IKT-szolgáltató műveletei szempontjából –, amelynek tényleges gyakorlását nem akadályozza vagy korlátozza más szerződéses megállapodás vagy végrehajtási szabályzat;

ii. az alternatív bizonyossági szintekről való megállapodás joga, ha más ügyfelek jogai érintettek;

iii. a harmadik fél IKT-szolgáltató azon kötelezettsége, hogy maradéktalanul együttműködjön az illetékes hatóságok, a vezető felvigyázó, a pénzügyi szervezet vagy egy kinevezett harmadik fél által végzett helyszíni ellenőrzések és auditok során; és

iv. az ilyen ellenőrzések és auditok terjedelmével, követendő eljárásaival és gyakoriságával kapcsolatos részletek megadásának kötelezettsége;

f) kilépési stratégiák, különösen egy kötelező megfelelő átmeneti időszak meghatározása:

i. amelynek során a harmadik fél IKT-szolgáltató folytatja a vonatkozó funkciók és IKT-szolgáltatások nyújtását annak érdekében, hogy csökkentse a pénzügyi szervezetnél keletkező zavar kockázatát, vagy biztosítsa annak eredményes szanálását és szerkezetátalakítását;

ii. amely lehetővé teszi a pénzügyi szervezet számára, hogy valamely egyéb harmadik fél IKT-szolgáltatóhoz migráljon, vagy házon belüli megoldásokra állhasson át a nyújtott szolgáltatás összetettségének megfelelően.

Az e) ponttól eltérve, a harmadik fél IKT-szolgáltató és a mikrovállalkozásként működő pénzügyi szervezet megállapodhat arról, hogy a pénzügyi szervezet hozzáférési, ellenőrzési és audit jogai átruházhatók a harmadik fél IKT-szolgáltató által kinevezett független harmadik félre, valamint hogy a pénzügyi szervezet bármikor tájékoztatást és biztosítékot kérhet a független harmadik féltől a harmadik fél IKT-szolgáltató teljesítése tekintetében.

(4) A szerződéses megállapodásokat előkészítő tárgyalások során a pénzügyi szervezeteknek és a harmadik fél IKT-szolgáltatóknak mérlegelniük kell az egyes szolgáltatásokra a hatóságok által kidolgozott általános szerződéses rendelkezések alkalmazását.

(5) Az EFH-knak a vegyes bizottságon keresztül szabályozástechnikai standardtervezeteket kell kidolgozniuk a (2) bekezdés a) pontjában említett azon elemek további pontosítása céljából, amelyeket a pénzügyi szervezetnek meg kell határoznia és értékelnie kell a kritikus vagy fontos funkciókat támogató IKT-szolgáltatások alvállalkozásba adásakor.

A szabályozástechnikai standardtervezetek kidolgozása során az EFH-knak figyelembe kell venniük a pénzügyi szervezet méretét és általános kockázati profilját, valamint szolgáltatásai, tevékenységei és műveletei jellegét, nagyságrendjét és összetettségét.

Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkével összhangban az első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

II. szakasz

A kritikus harmadik fél IKT-szolgáltatókra vonatkozó felvigyázási keretrendszer

31. cikk

A kritikus harmadik fél IKT-szolgáltatók kijelölése

(1) Az EFH-k a vegyes bizottság keretében, a 32. cikk (1) bekezdése alapján létrehozott felvigyázási fórum ajánlása alapján:

a) kijelölik azon harmadik fél IKT-szolgáltatókat, amelyek – a (2) bekezdésben meghatározott kritériumok figyelembevételével végzett értékelés nyomán – a pénzügyi szervezetek számára kritikusak;

b) a kritikus harmadik fél IKT-szolgáltatók mindegyikére vonatkozóan azon EFH-t nevezik ki vezető felvigyázóként, amely – az 1093/2010/EU, az 1094/2010/EU vagy az 1095/2010/EU rendeletnek megfelelően – azon pénzügyi szervezetekért felelős, amelyek teljes eszközértéke együttesen – amint azt az említett pénzügyi szervezetek egyedi mérlegeinek összesítése tanúsítja – a legnagyobb részt teszi ki a releváns kritikus harmadik fél IKT-szolgáltató szolgáltatásait igénybe vevő valamennyi pénzügyi szervezet teljes eszközértékén belül.

(2) Az (1) bekezdés a) pontjában említett kijelölésnek a harmadik fél IKT-szolgáltató által nyújtott IKT-szolgáltatásokkal kapcsolatban a következő kritériumokon kell alapulnia:

a) azon rendszerszintű hatás, amely a pénzügyi szolgáltatások nyújtásának stabilitását, folytonosságát vagy minőségét érné akkor, ha a releváns harmadik fél IKT-szolgáltató kiterjedt működési hiányosság miatt nem képes a szolgáltatásait nyújtani, figyelembe véve azon pénzügyi szervezetek számát, valamint azon pénzügyi szervezetek eszközeinek összértékét, amelyek részére a harmadik fél IKT-szolgáltató szolgáltatásokat nyújt;

b) a releváns harmadik fél IKT-szolgáltató szolgáltatásait igénybe vevő pénzügyi szervezetek rendszerszintű jellege vagy fontossága, a következő paraméterekkel összhangban értékelve:

   i. a vonatkozó harmadik fél IKT-szolgáltató szolgáltatásait igénybe vevő, globális rendszerszinten jelentős intézmények vagy egyéb rendszerszinten jelentős intézmények száma;

   ii. az i. alpontban említett globális rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények kölcsönös függése, beleértve azon helyzeteket is, amikor a globális rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények más pénzügyi szervezetek részére nyújtanak pénzügyi infrastrukturális szolgáltatásokat;

c) a releváns harmadik fél IKT-szolgáltató által nyújtott szolgáltatások igénybevétele a pénzügyi szervezetek olyan kritikus vagy fontos funkciói kapcsán, amelyek ellátására végső soron ugyanezen harmadik fél IKT-szolgáltató közreműködésével kerül sor függetlenül attól, hogy a pénzügyi szervezetek az említett szolgáltatásokat közvetlenül vagy közvetetten, alvállalkozási megállapodások útján veszik-e igénybe;

d) a harmadik fél IKT-szolgáltató helyettesíthetőségének mértéke, a következő paraméterek figyelembevételével:

   i. valós – legalább részleges – alternatívák hiánya, amely egy konkrét piacon működő harmadik fél IKT-szolgáltatók korlátozott számának, a releváns harmadik fél IKT-szolgáltató piaci részesedésének, vagy a megoldás technikai összetettségének vagy fejlettségének tulajdonítható, többek között bármely szabadalmaztatott technológia, vagy a harmadik fél IKT-szolgáltató szervezeti felépítésének vagy tevékenységének egyedi jellemzői kapcsán;

   ii. a releváns adatoknak és munkamennyiségnek a releváns harmadik fél IKT-szolgáltatótól egy másik harmadik fél IKT-szolgáltatóhoz történő részleges vagy teljes migrálásával járó nehézségek, amelyek okai lehetnek vagy a migrálási folyamattal esetleg együttjáró jelentős pénzügyi költségek, idő- vagy egyéb erőforrásigény, vagy azon megnövekedett IKT-kockázat vagy egyéb működési kockázatok, amelyeknek a pénzügyi szervezet ki lehet téve az ilyen migráció révén.

(3) Amennyiben a harmadik fél IKT-szolgáltató egy csoporthoz tartozik, a (2) bekezdésben említett kritériumokat a csoport egésze által nyújtott IKT-szolgáltatások tekintetében kell figyelembe venni.

(4) A csoport részét képező harmadik fél IKT-szolgáltatóknak koordinációs pontként ki kell jelölniük egy jogi személyt a megfelelő képviselet és a vezető felvigyázóval való kommunikáció biztosítása érdekében.

(5) A vezető felvigyázónak értesítenie kell a harmadik fél IKT-szolgáltatót az (1) bekezdés a) pontjában említett kijelöléshez vezető értékelés eredményéről. Az értesítés időpontjától számított 6 héten belül a harmadik fél IKT-szolgáltató indokolással ellátott nyilatkozatot nyújthat be a vezető felvigyázónak, amely tartalmazza az értékelés céljából releváns információkat. A vezető felvigyázónak meg kell vizsgálnia az indokolással ellátott nyilatkozatot, és az ilyen nyilatkozat kézhezvételétől számított 30 naptári napon belül további információk benyújtását kérheti.

Miután egy harmadik fél IKT-szolgáltatót kritikusnak jelöltek ki, az EFH-knak a vegyes bizottságon keresztül értesíteniük kell a harmadik fél IKT-szolgáltatót az ilyen kijelölésről és azon kezdőidőpontról, amelytől ténylegesen felvigyázási tevékenységek alá fog esni. Az említett kezdő időpontot az értesítéstől számított egy hónapon belül kell meghatározni. A harmadik fél IKT-szolgáltatónak értesítenie kell azon pénzügyi szervezeteket, amelyeknek szolgáltatásokat nyújt, a kritikusnak való kijelöléséről.

(6) A Bizottság felhatalmazást kap arra, hogy – az 57. cikkel összhangban – 2024. július 17-ig felhatalmazáson alapuló jogi aktust fogadjon el, amely az e cikk (2) bekezdésében említett kritériumok részletesebb meghatározásával egészíti ki ezt a rendeletet.

(7) Az (1) bekezdés a) pontjában említett kijelölés csak azt követően alkalmazható, hogy a Bizottság a (6) bekezdésnek megfelelően felhatalmazáson alapuló jogi aktust fogadott el.

(8) Az (1) bekezdés a) pontjában említett kijelölés nem alkalmazható a következők tekintetében:

i. azon pénzügyi intézmények, amelyek más pénzügyi intézményeknek nyújtanak IKT-szolgáltatásokat;

ii. azon harmadik fél IKT-szolgáltatók, amelyek az Európai Unió működéséről szóló szerződés 127. cikkének (2) bekezdésében említett feladatok támogatásának céljából létrehozott felvigyázási keretrendszerek hatálya alá tartoznak;

iii. a vállalatcsoporton belüli IKT-szolgáltatók;

iv. olyan harmadik fél IKT-szolgáltatók, amelyek kizárólag egy tagállamban nyújtanak IKT-szolgáltatásokat olyan pénzügyi szervezetek számára, amelyek csak az említett tagállamban tevékenykednek.

(9) Az EFH-knak a vegyes bizottság keretében össze kell állítaniuk, közzé kell tenniük és évente frissíteniük kell a kritikus harmadik fél IKT-szolgáltatók uniós szintű jegyzékét.

(10) Az (1) bekezdés a) pontjának alkalmazásában az illetékes hatóságok összesített formában évente átadják a 32. cikk alapján létrehozott felvigyázási fórumnak a 28. cikk (3) bekezdésének harmadik albekezdésében említett jelentéseket. A felvigyázási fórum az illetékes hatóságoktól kapott információk alapján értékeli a pénzügyi szervezetek harmadik féltől való IKT-függőségét.

(11) Azon harmadik fél IKT-szolgáltatók, amelyek nem szerepelnek a (9) bekezdésben említett jegyzékben, kérhetik, hogy az (1) bekezdés a) pontjának megfelelően kritikusnak legyenek kijelölve.

Az első albekezdés alkalmazásában a harmadik fél IKT-szolgáltatónak indokolással ellátott kérelmet kell benyújtania az EBH, az ESMA vagy az EIOPA részére, amely a vegyes bizottságon keresztül határoz arról, hogy az említett harmadik fél IKT-szolgáltatót az (1) bekezdés a) pontjának megfelelően kritikusnak jelöljék-e ki.

A kérelem beérkezésétől számított 6 hónapon belül kell elfogadni a második albekezdésben említett határozatot, és arról értesíteni a harmadik fél IKT-szolgáltatót.

(12) A pénzügyi szervezetek csak akkor vehetik igénybe egy harmadik országban letelepedett és az (1) bekezdés a) pontjával összhangban kritikusnak kijelölt harmadik fél IKT-szolgáltató szolgáltatásait, ha az utóbbi a kijelölést követő 12 hónapon belül leányvállalatot létesített az Unióban.

(13) A (12) bekezdésben említett kritikus harmadik fél IKT-szolgáltatónak értesítenie kell a vezető felvigyázót az Unióban letelepedett leányvállalat irányítási struktúráját érintő bármely változásról.

32. cikk

A felvigyázási keretrendszer felépítése

(1) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 57. cikkének (1) bekezdésével összhangban a vegyes bizottság albizottságként hozza létre a felvigyázási fórumot abból a célból, hogy támogassa a vegyes bizottság és a 31. cikk (1) bekezdésének b) pontjában említett vezető felvigyázó munkáját a pénzügyi ágazatokban fennálló, harmadik féltől eredő IKT-kockázat terén. A felvigyázási fórum előkészíti a vegyes bizottságnak az említett területet érintő közös álláspontokat és közös fellépéstervezeteit.

A felvigyázási fórum rendszeresen megvitatja az IKT-kockázattal és -sérülékenységgel kapcsolatos releváns fejleményeket, és következetes megközelítést szorgalmaz a harmadik féltől eredő IKT-kockázat uniós szintű nyomon követése terén.

(2) A felvigyázási fórum évente együttes értékelést végez a kritikus harmadik fél IKT-szolgáltatókra vonatkozó felvigyázási tevékenységek eredményeiről és megállapításairól, és koordinációs intézkedéseket mozdít elő, amelyek célja a pénzügyi szervezetek digitális működési rezilienciájának növelése, az IKT-koncentrációs kockázat kezelése terén elérhető legjobb gyakorlatok támogatása, továbbá a kockázat ágazatok közötti átterjedését mérséklő eszközök vizsgálata.

(3) A felvigyázási fórum a kritikus harmadik fél IKT-szolgáltatókra vonatkozó átfogó referenciamutatókat terjeszt elő, amelyeket a vegyes bizottság az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 56. cikkének (1) bekezdésével összhangban az EFH-k közös álláspontjaként fogad el.

(4) A felvigyázási fórum a következőkből áll:

a) az EFH-k elnökei;

b) az egyes tagállamoknak a 46. cikkben említett releváns illetékes hatósága mindenkori személyzetének egy-egy magas rangú képviselője;

c) megfigyelőként az egyes EFH-k ügyvezető igazgatója, valamint a Bizottság, az ERKT, az EKB és az ENISA egy-egy képviselője;

d) adott esetben megfigyelőként az egyes tagállamok valamely, a 46. cikkben említett illetékes hatóságának egy-egy további képviselője;

e) megfigyelőként adott esetben az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott – valamely kritikus harmadik fél IKT-szolgáltatónak kijelölt, az említett irányelv hatálya alá tartozó alapvető vagy fontos szervezet felügyeletéért felelős – illetékes hatóságok képviselője.

A felvigyázási fórum adott esetben kikérheti a (6) bekezdéssel összhangban kinevezett független szakértők tanácsát.

(5) Minden egyes tagállam kijelöli azon releváns illetékes hatóságot, amely személyzetének egyik tagja a (4) bekezdés első albekezdésének b) pontjában említett magas rangú képviselő, és erről tájékoztatja a vezető felvigyázót.

Az EFH-k a honlapjukon közzéteszik a releváns illetékes hatóság jelenlegi személyzetéből a tagállamok által kijelölt magas rangú képviselők jegyzékét.

(6) A (4) bekezdés második albekezdésében említett független szakértőket a felvigyázási fórum nevezi ki egy nyilvános és átlátható pályázati eljárást követően kiválasztott szakértői állományból.

A független szakértőket a pénzügyi stabilitással, a digitális működési rezilienciával és az IKT-biztonsággal kapcsolatos szakértelmük alapján kell kinevezni. Függetlenül és objektíven járnak el, kizárólag az Unió egészének érdekében, nem kérhetnek és nem fogadhatnak el utasítást sem uniós intézménytől vagy szervtől, sem tagállami kormánytól, sem más közjogi vagy magánjogi szervtől.

(7) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 16. cikkével összhangban az EFH-k 2024. július 17-ig – e szakasz alkalmazásában – iránymutatásokat adnak ki az EFH-k és az illetékes hatóságok között folytatandó együttműködésről, amely iránymutatások kiterjednek az illetékes hatóságok és az EFH-k közötti feladatok elosztására és végrehajtására vonatkozó részletes eljárásokra és feltételekre, valamint az ahhoz szükséges információcserék részleteire, hogy az illetékes hatóságok biztosítsák a 35. cikk (1) bekezdésének d) pontja alapján a kritikus harmadik fél IKT-szolgáltatóknak címzett ajánlások utókövetését.

(8) Az e szakaszban meghatározott követelmények nem érintik az (EU) 2022/2555 irányelv és a felhőszolgáltatókra alkalmazandó, felvigyázásra vonatkozó egyéb uniós szabályok alkalmazását.

(9) Az EFH-k a vegyes bizottságon keresztül és a felvigyázási fórum által végzett előkészítő munka alapján évente jelentést nyújtanak be e szakasz alkalmazásáról az Európai Parlamentnek, a Tanácsnak és a Bizottságnak.

33. cikk

A vezető felvigyázó feladatai

(1) A 31. cikk (1) bekezdésének b) pontjával összhangban kijelölt vezető felvigyázó elvégzi a kijelölt, kritikus harmadik fél IKT-szolgáltatók felvigyázását, és a felvigyázással kapcsolatos valamennyi kérdés céljából elsődleges kapcsolattartóként áll az említett kritikus harmadik fél IKT-szolgáltatók rendelkezésére.

(2) Az (1) bekezdés alkalmazásában a vezető felvigyázónak értékelnie kell, hogy a kritikus harmadik fél IKT-szolgáltatók mindegyike rendelkezik-e átfogó, megbízható és hatékony szabályokkal, eljárásokkal, mechanizmusokkal és intézkedésekkel azon tőle eredő IKT-kockázat kezeléséhez, amellyel a pénzügyi szervezetek szembesülhetnek.

Az első albekezdésben említett értékelésnek a kritikus harmadik fél IKT-szolgáltató által nyújtott IKT-szolgáltatások közül elsősorban a pénzügyi szervezetek kritikus vagy fontos funkcióit támogató szolgáltatásokra kell összpontosítania. Amennyiben az valamennyi releváns kockázat kezeléséhez szükséges, az említett értékelésnek ki kell terjednie a kritikus vagy fontos funkcióktól eltérő funkciókat támogató IKT-szolgáltatásokra is.

(3) A (2) bekezdésben említett értékelésnek ki kell terjednie a következőkre:

a) IKT-vonatkozású követelmények, hogy biztosítsák különösen azon szolgáltatások biztonságát, rendelkezésre állását, folytonosságát, skálázhatóságát és minőségét, amelyeket a kritikus harmadik fél IKT-szolgáltató nyújt pénzügyi szervezeteknek, valamint az adatok rendelkezésre állására, hitelességére, integritására vagy bizalmas jellegére vonatkozó magas szintű normák mindenkori fenntartásának képességét;

b) az IKT-biztonság biztosítását elősegítő fizikai biztonság, ezen belül a telephelyek, létesítmények, adatközpontok biztonsága;

c) a kockázatkezelési folyamatok, ezen belül az IKT-kockázatkezelési szabályzatok, az IKT-üzletmenetfolytonossági politika, valamint az IKT-reagálási és -helyreállítási tervek;

d) az irányítási rendszer, ezen belül az olyan szervezeti felépítés, amelyben az egyértelmű, átlátható és következetes felelősségi körök és elszámoltathatósági szabályok lehetővé teszik az eredményes IKT-kockázatkezelést;

e) a pénzügyi szervezeteket érő lényeges IKT-vonatkozású események azonosítása, nyomon követése és haladéktalan bejelentése, valamint az ilyen események, különösen a kiberbiztonsági események kezelése és elhárítása;

f) az adathordozhatóságot, valamint az alkalmazások hordozhatóságát és kölcsönös átjárhatóságát biztosító mechanizmusok, amelyek biztosítják a pénzügyi szervezetek számára a felmondási jogok tényleges gyakorlását;

g) az IKT-rendszerek, -infrastruktúrák és -kontrollok tesztelése;

h) az IKT-auditok;

i) a pénzügyi szervezetek részére nyújtott IKT-szolgáltatásokra alkalmazandó releváns nemzeti és nemzetközi szabványok használata.

(4) A (2) bekezdésben említett értékelés alapján és a 34. cikk (1) bekezdésében említett közös felvigyázási hálózattal (KFH) koordinálva, a vezető felvigyázónak egyértelmű, részletes és indokolással ellátott egyéni felvigyázási tervet kell elfogadnia, amelyben az egyes kritikus harmadik fél IKT-szolgáltatók számára kitűzött éves felvigyázási célok és tervezett főbb felvigyázási intézkedések szerepelnek. A tervről évente értesíteni kell a kritikus harmadik fél IKT-szolgáltatót.

A felvigyázási terv elfogadása előtt a vezető felvigyázónak ismertetnie kell a felvigyázásiterv-javaslatot a kritikus harmadik fél IKT-szolgáltatóval.

A felvigyázásiterv-javaslat kézhezvételét követően a kritikus harmadik fél IKT-szolgáltató 15 naptári napon belül indokolással ellátott nyilatkozatot nyújthat be, amelyben igazolja az e rendelet hatályán kívül eső ügyfelekre gyakorolt várható hatást, és adott esetben kockázatcsökkentő megoldásokat mutat be.

(5) A (4) bekezdésben említett éves felvigyázási tervek elfogadását és arról a kritikus harmadik fél IKT-szolgáltatók értesítését követően az illetékes hatóságok csak a vezető felvigyázó egyetértésével hozhatnak az ilyen kritikus harmadik fél IKT-szolgáltatókra vonatkozó intézkedéseket.

34. cikk

A vezető felvigyázók közötti operatív koordináció

(1) A felvigyázási tevékenységek következetes megközelítésének biztosítása céljából, valamint a koordinált általános felvigyázási stratégiák és a koherens operatív megközelítések és módszertanok lehetővé tétele érdekében a 31. cikk (1) bekezdésének b) pontjával összhangban kinevezett három vezető felvigyázónak KFH-t kell létrehozniuk, hogy egymás között koordináljanak az előkészítő szakaszokban, és koordinálják az általuk felvigyázott, kritikus harmadik fél IKT-szolgáltatók feletti felvigyázási tevékenységek végzését, valamint koordináljanak a 42. cikk alapján esetlegesen szükségessé váló bármely intézkedés során.

(2) Az (1) bekezdés alkalmazásában a vezető felvigyázóknak közös felvigyázási protokollt kell kidolgozniuk, amely meghatározza a napi koordinációs feladatok végzése, valamint a gyors információcsere és reagálás biztosítása érdekében követendő részletes eljárásokat. A protokollt időszakonként felül kell vizsgálni, hogy tükrözze az operatív igényeket, különösen a gyakorlati felvigyázási intézkedések alakulását.

(3) A vezető felvigyázók eseti alapon felkérhetik az EKB-t és az ENISA-t szakvélemény kiadására, gyakorlati tapasztalataik megosztására vagy a KFH bizonyos koordinációs ülésein való részvételre.

35. cikk

A vezető felvigyázó hatáskörei

(1) Az e szakaszban meghatározott feladatok elvégzése céljából a vezető felvigyázó a következő hatáskörökkel rendelkezik a kritikus harmadik fél IKT-szolgáltatók tekintetében:

a) a 37. cikknek megfelelően bekérhet minden releváns információt és dokumentumot;

b) a 38., illetve a 39. cikknek megfelelően általános vizsgálatokat, illetve ellenőrzéseket tarthat;

c) a felvigyázási tevékenységek elvégzését követően jelentést kérhet arról, hogy a kritikus harmadik fél IKT-szolgáltatók milyen intézkedéseket tettek vagy korrekciókat hajtottak végre az e bekezdés d) pontjában említett ajánlásokkal kapcsolatban;

d) ajánlásokat adhat ki a 33. cikk (3) bekezdésében említett területekre, különösen a következőkre vonatkozóan:

   i. specifikus IKT-biztonsági és -minőségi követelmények vagy folyamatok alkalmazása, különösen a javítócsomagok, a frissítések, a titkosítás és azon egyéb biztonsági intézkedések bevezetése kapcsán, amelyek a vezető felvigyázó megítélése szerint relevánsak a pénzügyi szervezeteknek nyújtott szolgáltatások IKT-biztonsága szempontjából;

   ii. a technikai megvalósításra is kiterjedően a kritikus harmadik fél IKT-szolgáltatók által a pénzügyi szervezetek részére nyújtott IKT-szolgáltatásokra vonatkozó feltételek közül azoknak az alkalmazása, amelyek a vezető felvigyázó megítélése szerint relevánsak az egyedi meghibásodási pontok kialakulása, az ezzel kapcsolatos kockázat felerősödése, vagy az IKT-koncentrációs kockázat esetében az uniós pénzügyi ágazat egészére kiterjedő esetleges rendszerszintű hatás csökkentése szempontjából;

   iii. olyan tervezett alvállalkozói tevékenységek, amelyek esetében a vezető felvigyázó megítélése szerint a további alvállalkozásba adás – ideértve a kritikus harmadik fél IKT-szolgáltatók által más kritikus harmadik fél IKT-szolgáltatókkal vagy harmadik országban letelepedett IKT-alvállalkozókkal megkötni tervezett alvállalkozói megállapodásokat is – a 37. és a 38. cikkel összhangban gyűjtött információ vizsgálata alapján kockázatokat eredményezhet a pénzügyi szervezet általi szolgáltatásnyújtásra vagy a pénzügyi stabilitására nézve;

   iv. a további alvállalkozási megállapodástól való tartózkodás, amennyiben a következő kumulatív feltételek teljesülnek:

      – a bevonni tervezett alvállalkozó harmadik fél IKT-szolgáltató vagy harmadik országban letelepedett IKT-alvállalkozó;

      – az alvállalkozó bevonása a pénzügyi szervezet kritikus vagy fontos funkcióinak ellátására irányul; és

– a vezető felvigyázó megítélése szerint az ilyen alvállalkozói szerződés alkalmazása egyértelmű és súlyos kockázatot jelent az Unió pénzügyi stabilitására vagy a pénzügyi szervezetekre nézve, ideértve a pénzügyi szervezetek azon képességét is, hogy megfeleljenek a felügyeleti követelményeknek.

E pont iv. alpontjának alkalmazásában a harmadik fél IKT-szolgáltatóknak a 41. cikk (1) bekezdésének b) pontjában említett sablon használatával továbbítaniuk kell az alvállalkozásba adásra vonatkozó információkat a vezető felvigyázónak.

(2) Az e cikkben említett hatáskörök gyakorlása során a vezető felvigyázó:

a) biztosítja a KFH-n belüli rendszeres koordinációt, és adott esetben következetes megközelítésekre törekszik a kritikus harmadik fél IKT-szolgáltatók felvigyázása tekintetében;

b) megfelelően figyelembe veszi az (EU) 2022/2555 irányelv által létrehozott keretet, és szükség esetén konzultál az említett irányelvvel összhangban kijelölt vagy létrehozott releváns illetékes hatóságokkal, hogy elkerüljék az egymást átfedő technikai és szervezeti intézkedéseket, amelyek az említett irányelv értelmében a kritikus harmadik fél IKT-szolgáltatókra vonatkozhatnak;

c) minimalizálni törekszik a kritikus harmadik fél IKT-szolgáltatók által az e rendelet hatályán kívül eső ügyfeleknek nyújtott szolgáltatások megszakadásának kockázatát.

(3) A vezető felvigyázónak az (1) bekezdésben említett hatáskörök gyakorlását megelőzően egyeztetnie kell a felvigyázási fórummal.

Mielőtt az (1) bekezdés d) pontjával összhangban ajánlásokat adna ki, a vezető felvigyázónak lehetőséget kell biztosítania a harmadik fél IKT-szolgáltató számára, hogy 30 naptári napon belül releváns információkat nyújtson be, amelyek igazolják az e rendelet hatályán kívül eső ügyfelekre gyakorolt várható hatást, és adott esetben kockázatcsökkentő megoldásokat körvonalaznak.

(4) A vezető felvigyázónak tájékoztatnia kell a KFH-t az (1) bekezdés a) és b) pontjában említett hatáskörök gyakorlásának eredményéről. A vezető felvigyázónak az (1) bekezdés c) pontjában említett jelentéseket indokolatlan késedelem nélkül továbbítania kell a KFH-nak és a kritikus harmadik fél IKT-szolgáltató IKT-szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságainak.

(5) A kritikus harmadik fél IKT-szolgáltatóknak jóhiszeműen együtt kell működniük a vezető felvigyázóval, és segíteniük kell a feladatai ellátásában.

(6) Az (1) bekezdés a), b) és c) pontja szerinti hatáskörök gyakorlása alapján meghozandó intézkedéseknek való teljes vagy részleges meg nem felelés esetén és azon naptól számított legalább 30 naptári nap elteltével, amelyen a kritikus harmadik fél IKT-szolgáltató megkapta a vonatkozó intézkedésekről szóló értesítést, a vezető felvigyázónak határozatot kell elfogadnia, amelyben időszaki büntető bírság kiszabásával kényszeríti a kritikus harmadik fél IKT-szolgáltatót az említett intézkedéseknek való megfelelésre.

(7) A (6) bekezdésben említett időszaki büntető bírságot naponta ki kell szabni a megfelelés eléréséig, a kritikus harmadik fél IKT-szolgáltatónak az időszaki büntető bírság kiszabásáról szóló határozatról való értesítését követő legfeljebb hathónapos időszakban.

(8) Az időszaki büntető bírság összege az időszaki büntető bírság kiszabásáról szóló határozatban megjelölt naptól számítandó, mértéke a kritikus harmadik fél IKT-szolgáltató előző üzleti évben elért átlagos napi világpiaci forgalmának legfeljebb 1 %-a. A büntető bírság összegének meghatározásakor a vezető felvigyázónak a (6) bekezdésben említett intézkedések be nem tartása tekintetében a következő kritériumokat kell figyelembe vennie:

a) a meg nem felelés súlyossága és időtartama;

b) a meg nem felelés szándékos cselekmény vagy gondatlanság eredménye-e;

c) a harmadik fél IKT-szolgáltató és a vezető felvigyázó közötti együttműködés szintje.

Az első albekezdés alkalmazásában – a következetes megközelítés biztosítása érdekében – a vezető felvigyázónak konzultációt kell folytatnia a KFH-n belül.

(9) A büntető bírság közigazgatási jellegű és behajtható. A behajtásra azon tagállam hatályos polgári eljárásjogi szabályai vonatkoznak, amelynek területén az ellenőrzésre és a hozzáférésre sor kerül. A behajtás szabálytalanságára vonatkozó panaszok tekintetében az érintett tagállam bíróságai rendelkeznek joghatósággal. A büntető bírság összege az Európai Unió általános költségvetését illeti.

(10) A vezető felvigyázónak nyilvánosságra kell hoznia minden kiszabott időszaki büntető bírságot, kivéve, ha az ilyen nyilvánosságra hozatal súlyosan veszélyeztetné a pénzügyi piacokat, vagy aránytalan károkat okozna az érintett feleknek.

(11) Az időszaki büntető bírságnak a (6) bekezdés alapján történő kiszabása előtt a vezető felvigyázónak a megállapítások kapcsán meghallgatási lehetőséget kell biztosítania az eljárás alá vont kritikus harmadik fél IKT-szolgáltató képviselői számára, és a határozathozatal során kizárólag azon megállapításokat veheti figyelembe, amelyek kapcsán a kritikus harmadik fél IKT-szolgáltató lehetőséget kapott észrevételei megtételére.

Az eljárás alá vont személyek védelemhez való jogát az eljárás során teljes mértékben tiszteletben kell tartani. Az eljárás alá vont, kritikus harmadik fél IKT-szolgáltatónak jogában áll betekinteni az ügyiratba, amennyiben ez nem sérti más személyeknek az üzleti titkok védelméhez fűződő jogos érdekét. Az ügyiratba való betekintés joga nem terjed ki a bizalmas információkra és a vezető felvigyázó belső előkészítő dokumentumaira.

36. cikk

A vezető felvigyázó hatásköreinek gyakorlása az Unión kívül

(1) Amennyiben a felvigyázási célok nem érhetők el a 31. cikk (12) bekezdésének alkalmazásában létrehozott leányvállalattal való interakcióval vagy a felvigyázási tevékenységeknek az Unióban található telephelyeken történő gyakorlásával, a vezető felvigyázó a következő rendelkezésekben említett hatásköröket bármely olyan, harmadik országban található telephelyen gyakorolhatja, amely egy kritikus harmadik fél IKT-szolgáltató tulajdonában van, vagy amelyet egy kritikus harmadik fél IKT-szolgáltató uniós pénzügyi szervezetek részére történő szolgáltatásnyújtás céljából bármely módon használ az üzleti műveleteivel, funkcióival vagy szolgáltatásaival kapcsolatban – ideértve az adminisztratív, üzleti és üzemeltetési irodákat, telephelyeket, földterületeket, épületeket vagy egyéb ingatlanokat is:

a) a 35. cikk (1) bekezdésének a) pontja; és

b) a 35. cikk (1) bekezdésének b) pontja, összhangban a 38. cikk (2) bekezdésének a), b) és d) pontjával, valamint a 39. cikk (1) bekezdésével és (2) bekezdésének a) pontjával.

Az első albekezdésben említett hatáskörök valamennyi következő feltétel fennállása esetén gyakorolhatók:

i. a vezető felvigyázó szükségesnek tartja egy harmadik országbeli ellenőrzés lefolytatását ahhoz, hogy teljes mértékben és eredményesen el tudja látni az e rendelet szerinti feladatait;

ii. a harmadik országbeli ellenőrzés közvetlenül kapcsolódik az Unióban működő pénzügyi szervezetek számára nyújtott IKT-szolgáltatásokhoz;

iii. az érintett kritikus harmadik fél IKT-szolgáltató hozzájárul egy harmadik országbeli ellenőrzés lefolytatásához; és

iv. a vezető felvigyázó hivatalosan értesítette az érintett harmadik ország releváns hatóságát, és az nem emelt kifogást.

(2) Az uniós intézmények és a tagállamok vonatkozó hatásköreinek sérelme nélkül, az (1) bekezdés alkalmazásában az EBH, az ESMA vagy az EIOPA igazgatási együttműködési megállapodásokat köt a harmadik ország releváns hatóságával annak érdekében, hogy a vezető felvigyázó és az említett harmadik országbeli kiküldetésre kijelölt csoportja az érintett harmadik országban zökkenőmentesen lefolytathassa az ellenőrzéseket. Az említett együttműködési megállapodások nem keletkeztethetnek jogi kötelezettségeket az Unióval és tagállamaival szemben, és nem akadályozhatják meg a tagállamokat és illetékes hatóságaikat abban, hogy két- vagy többoldalú megállapodásokat kössenek az említett harmadik országokkal és azok releváns hatóságaival.

Az említett együttműködési megállapodásoknak tartalmazniuk kell legalább a következő elemeket:

a) az e rendelet alapján végzett felvigyázási tevékenységek és bármely hasonló, az érintett harmadik ország releváns hatósága által folytatott, a harmadik féltől eredő IKT-kockázatnak a pénzügyi ágazatban való nyomon követését célzó tevékenység koordinálására vonatkozó eljárások, beleértve a harmadik ország releváns hatósága által ahhoz adott hozzájárulás továbbításának részletes szabályait, hogy a joghatósága alá tartozó területen a vezető felvigyázó és az általa kijelölt csoport lefolytathassa az (1) bekezdés első albekezdésében említett általános vizsgálatokat és helyszíni ellenőrzéseket;

b) a releváns információknak az EBH, az ESMA vagy az EIOPA, valamint az érintett harmadik ország releváns hatósága közötti továbbításának mechanizmusa, különösen a vezető felvigyázó által a 37. cikk alapján kérhető információkkal kapcsolatban;

c) azon mechanizmusok, amelyek révén az érintett harmadik ország releváns hatósága haladéktalanul értesíti az EBH-t, az ESMA-t vagy az EIOPA-t azon esetekről, amikor úgy tekinthető, hogy egy harmadik országban letelepedett és a 31. cikk (1) bekezdésének a) pontjával összhangban kritikusnak kijelölt IKT-szolgáltató megsértette azon követelményeket, amelyeket az érintett harmadik ország alkalmazandó joga értelmében köteles betartani, amikor az említett harmadik országban pénzügyi intézményeknek nyújt szolgáltatásokat, továbbá az alkalmazott jogorvoslatok és szankciók;

d) az érintett harmadik országban lévő pénzügyi intézmények harmadik féltől eredő IKT-kockázatának nyomon követésével kapcsolatos szabályozási vagy felügyeleti fejleményekkel kapcsolatos naprakész információk rendszeres továbbítása;

e) az annak engedélyezésével kapcsolatos részletek, hogy szükség esetén a harmadik országbeli illetékes hatóság egy képviselője részt vegyen a vezető felvigyázó és a kijelölt csoport által végzett ellenőrzéseken.

(3) Amennyiben a vezető felvigyázó nem képes az (1) és (2) bekezdésben említett, Unión kívüli felvigyázási tevékenységeket végezni, a vezető felvigyázónak:

a) a 35. cikk szerinti hatáskörét a rendelkezésére álló valamennyi tény és dokumentum alapján kell gyakorolnia;

b) dokumentálnia kell és ki kell fejtenie az e cikkben említett tervezett felvigyázási tevékenységek végzésére való képtelenségének lehetséges következményeit.

Az e bekezdés b) pontjában említett lehetséges következményeket figyelembe kell venni a vezető felvigyázónak a 35. cikk (1) bekezdésének d) pontja alapján kiadott ajánlásaiban.

37. cikk

Információkérés

(1) A vezető felvigyázó egyszerű kérés vagy határozat útján előírhatja a kritikus harmadik fél IKT-szolgáltatók számára, hogy adják át a részére az e rendelet szerinti feladatainak elvégzéséhez szükséges információkat, ideértve a releváns üzleti vagy működési dokumentumokat, szerződéseket, szabályzatokat, dokumentációkat, az IKT-biztonsági auditjelentéseket, az IKT-vonatkozású eseményekről készült jelentéseket, valamint az olyan felekkel kapcsolatos információkat, akikhez a kritikus harmadik fél IKT-szolgáltató operatív funkciókat vagy tevékenységeket szervezett ki.

(2) Az (1) bekezdés szerinti egyszerű információkérés megküldésekor a vezető felvigyázónak:

a) a kérés jogalapjaként e cikkre kell hivatkoznia;

b) meg kell jelölnie a kérés célját;

c) pontosan meg kell határoznia a kért információt;

d) meg kell határoznia az információnyújtás határidejét;

e) tájékoztatnia kell a kritikus harmadik fél IKT-szolgáltató azon képviselőjét, akitől az információt kérik, hogy nem köteles megadni az információt, de amennyiben önkéntesen válaszol a kérésre, a nyújtott információ nem lehet helytelen vagy félrevezető.

(3) Az (1) bekezdés szerinti, határozat útján történő információkérés esetén a vezető felvigyázónak:

a) a kérés jogalapjaként e cikkre kell hivatkoznia;

b) meg kell jelölnie a kérés célját;

c) pontosan meg kell határoznia a kért információt;

d) meg kell határoznia az információnyújtás határidejét;

e) meg kell jelölnie a 35. cikk (6) bekezdésében azon esetre előírt időszaki büntető bírságot, amennyiben a kért információk nyújtása hiányos, vagy amikor az ilyen információkat az e bekezdés d) pontjában említett határidőn belül nem biztosítják;

f) meg kell jelölnie azon jogot, hogy – az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 60. és 61. cikkével összhangban – a határozat ellen fellebbezni lehet az EFH fellebbezési tanácsa előtt, és a határozat felülvizsgáltatható az Európai Unió Bíróságával (Bíróság).

(4) A kritikus harmadik fél IKT-szolgáltatók képviselői benyújtják a kért információkat. Megfelelően meghatalmazott ügyvédek az ügyfelük nevében nyújthatják be az információkat. A harmadik fél IKT-szolgáltatók teljes felelősséggel tartoznak, ha a szolgáltatott információ hiányos, helytelen vagy félrevezető.

(5) A vezető felvigyázó a határozat példányának haladéktalan továbbításával tájékoztatja a releváns kritikus harmadik fél IKT-szolgáltatók szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságait és a KFH-t.

38. cikk

Általános vizsgálatok

(1) Az e rendelet szerinti feladatainak elvégzése érdekében a vezető felvigyázó a 40. cikk 1) bekezdésében említett közös vizsgálócsoport támogatásával – szükség esetén – lefolytathatja a kritikus harmadik fél IKT-szolgáltatók vizsgálatait.

(2) A vezető felvigyázó a következő hatáskörökkel rendelkezik:

a) a feladatainak végrehajtása szempontjából releváns nyilvántartások, adatok, eljárások és egyéb anyagok megvizsgálása, az adathordozótól függetlenül;

b) az ilyen nyilvántartásokból, adatokból, dokumentált eljárásokból és bármely egyéb anyagból hiteles másolatok vagy kivonatok készítése vagy bekérése;

c) a kritikus harmadik fél IKT-szolgáltató képviselőinek felszólítása a személyes megjelenésre, és szóbeli vagy írásbeli magyarázat kérése a vizsgálat tárgyával és céljával összefüggő tényekkel és dokumentumokkal kapcsolatban, valamint a válaszok rögzítése;

d) bármely egyéb olyan természetes vagy jogi személy meghallgatása, aki vagy amely hozzájárul ahhoz, hogy a vizsgálat tárgyával kapcsolatos információgyűjtés céljából meghallgassák;

e) a telefon- és adatforgalmi nyilvántartások kikérése.

(3) Az (1) bekezdésben említett vizsgálat céljából a vezető felvigyázó által felhatalmazott tisztviselőknek és más személyeknek hatáskörük gyakorlásához fel kell mutatniuk a vizsgálat tárgyát és célját feltüntető írásbeli felhatalmazást.

Az említett felhatalmazásban szintén fel kell tüntetni a 35. cikk (6) bekezdésében azon esetre előírt időszaki büntető bírságokat, amennyiben a kért nyilvántartásokat, adatokat, dokumentált eljárásokat vagy egyéb anyagokat nem vagy hiányosan nyújtják be, vagy ha a harmadik fél IKT-szolgáltató képviselői a feltett kérdésekre nem vagy hiányosan válaszolnak.

(4) A kritikus harmadik fél IKT-szolgáltatók képviselői kötelesek alávetni magukat a vezető felvigyázó határozata alapján elrendelt vizsgálatoknak. A határozatban fel kell tüntetni a vizsgálat tárgyát és célját, a 35. cikk (6) bekezdésében előírt időszaki büntető bírságokat, az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet alapján igénybe vehető jogorvoslatokat, valamint azon jogot, hogy a határozat az Európai Unió Bíróságával felülvizsgáltatható.

(5) A vezető felvigyázónak a vizsgálat kezdete előtt kellő időben tájékoztatnia kell a tervezett vizsgálatról és a felhatalmazott személyek személyazonosságáról az említett kritikus harmadik fél IKT-szolgáltató IKT-szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságait.

A vezető felvigyázónak az első albekezdés alapján átadott valamennyi információt közölnie kell a KFH-val.

39. cikk

Ellenőrzések

(1) Az e rendelet szerinti feladatainak elvégzése érdekében a vezető felvigyázó a 40. cikk (1) bekezdésében említett közös vizsgálócsoportok támogatásával beléphet a harmadik fél IKT-szolgáltatók bármely telephelyére, területére vagy ingatlanára, beleértve a szolgáltató székhelyét, üzemeltetési központjait, egyéb telephelyeit is, és elvégezhet minden szükséges helyszíni ellenőrzést, valamint helyszínen kívüli ellenőrzést végezhet.

Az első albekezdésben említett hatáskörök gyakorlása céljából a vezető felvigyázónak konzultálnia kell a KFH-val.

(2) A vezető felvigyázó által a helyszíni ellenőrzés lefolytatására felhatalmazott tisztviselők és egyéb személyek jogosultak arra, hogy:

a) belépjenek bármely ilyen telephelyre, területre vagy ingatlanra; és

b) az ellenőrzéshez szükséges időre és mértékben zár alá vegyenek bármely ilyen telephelyet, könyvet vagy feljegyzést.

A vezető felvigyázó által felhatalmazott tisztviselőknek és egyéb személyeknek hatáskörük gyakorlásához fel kell mutatniuk az ellenőrzés tárgyát és célját feltüntető írásbeli felhatalmazást, amely megjelöli a 35. cikk (6) bekezdésében azon esetre előírt időszaki büntető bírságokat, amennyiben az érintett kritikus harmadik fél IKT-szolgáltatók képviselői nem vetik alá magukat az ellenőrzésnek.

(3) A vezető felvigyázónak az ellenőrzés kezdete előtt kellő időben értesítést kell küldenie az említett harmadik fél IKT-szolgáltatót igénybe vevő pénzügyi szervezetek illetékes hatóságainak.

(4) Az ellenőrzéseknek ki kell terjedniük a pénzügyi szervezeteknek nyújtott IKT-szolgáltatások teljesítéséhez felhasznált vagy ahhoz hozzájáruló releváns IKT-rendszerek, -hálózatok, -eszközök, -információk és -adatok teljes körére.

(5) A tervezett helyszíni ellenőrzést megelőzően a vezető felvigyázónak észszerű értesítést kell adnia a kritikus harmadik fél IKT-szolgáltatóknak, kivéve, ha az ilyen értesítés veszélyhelyzet vagy válsághelyzet miatt nem lehetséges, vagy ha az meghiúsítaná az eredményes ellenőrzést vagy auditot.

(6) A kritikus harmadik fél IKT-szolgáltatónak alá kell vetnie magát a vezető felvigyázó határozata alapján elrendelt helyszíni ellenőrzéseknek. A határozatban fel kell tüntetni az ellenőrzés tárgyát és célját, rögzíteni kell az ellenőrzés megkezdésének időpontját, valamint meg kell jelölni a 35. cikk (6) bekezdésében előírt időszaki büntető bírságokat, az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet alapján igénybe vehető jogorvoslatokat, valamint azon jogot, hogy a határozat az Európai Unió Bíróságával felülvizsgáltatható.

(7) Amennyiben a vezető felvigyázó által felhatalmazott tisztviselők és más személyek azt állapítják meg, hogy a kritikus harmadik fél IKT-szolgáltató ellenzi az e cikk alapján elrendelt ellenőrzést, a vezető felvigyázónak tájékoztatnia kell a kritikus harmadik fél IKT-szolgáltatót az ilyen ellenkezés következményeiről, beleértve annak lehetőségét, hogy a releváns pénzügyi szervezetek illetékes hatóságai előírják a pénzügyi szervezetek számára, hogy szüntessék meg az említett kritikus harmadik fél IKT-szolgáltatóval kötött szerződéses megállapodásokat.

40. cikk

Folyamatos felvigyázás

(1) A vezető felvigyázót a felvigyázási tevékenységek folytatása során, különösen általános vizsgálatok vagy ellenőrzések lefolytatásakor az egyes kritikus harmadik fél IKT-szolgáltatók tekintetében létrehozott közös vizsgálócsoport támogatja.

(2) Az (1) bekezdésben említett közös vizsgálócsoport a következő intézmények személyzetének tagjaiból áll:

a) az EFH-k;

b) azon releváns illetékes hatóságok, amelyek a kritikus harmadik fél IKT-szolgáltató IKT-szolgáltatásait igénybe vevő pénzügyi szervezeteket felügyelik;

c) a 32. cikk (4) bekezdésének e) pontjában említett illetékes nemzeti hatóság, önkéntes alapon;

d) a kritikus harmadik fél IKT-szolgáltató letelepedésének helye szerinti tagállam egy illetékes nemzeti hatósága, önkéntes alapon.

A közös vizsgálócsoport tagjainak tapasztalattal kell rendelkezniük az IKT-vel kapcsolatos kérdések és a működési kockázatok terén. A közös vizsgálócsoport munkáját a vezető felvigyázó személyzete egy kijelölt tagjának (a továbbiakban: a vezető felvigyázó koordinátora) kell koordinálnia.

(3) A vizsgálat vagy ellenőrzés befejezését követő 3 hónapon belül a vezető felvigyázónak a felvigyázási fórummal történt egyeztetés után a 35. cikkben említett hatáskörében ajánlásokat kell megfogalmaznia a harmadik fél IKT-szolgáltató számára.

(4) A vezető felvigyázónak haladéktalanul közölnie kell a (3) bekezdésben említett ajánlásokat a kritikus harmadik fél IKT-szolgáltatóval és az annak IKT-szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságaival.

A felvigyázási tevékenységek céljából a vezető felvigyázó figyelembe veheti a kritikus harmadik fél IKT-szolgáltató által rendelkezésére bocsátott, harmadik fél által kiállított tanúsítványokat, valamint harmadik fél által készített belső és külső IKT-audit jelentéseket.

41. cikk

A felvigyázási tevékenységek végzését lehetővé tevő előfeltételek harmonizálása

(1) Az EFH-knak a vegyes bizottság keretében szabályozástechnikai standardtervezeteket kell kidolgozniuk, amelyekben részletesen meghatározzák:

a) a 31. cikk (11) bekezdése szerinti kritikusként való kijelölés iránti saját kezdeményezésű kérelemben a harmadik fél IKT-szolgáltató által benyújtandó információkat;

b) a 35. cikk (1) bekezdése alapján a harmadik fél IKT-szolgáltató által benyújtandó, közzéteendő vagy jelentendő információk tartalmát, struktúráját és formátumát, beleértve az alvállalkozási megállapodásokról szóló információk benyújtására szolgáló sablont is;

c) a közös vizsgálócsoport összetételének meghatározására vonatkozó kritériumokat, amelyek biztosítják az EFH-k és a releváns illetékes hatóságok személyzete tagjainak kiegyensúlyozott részvételét, valamint kijelölésüket, feladataikat és munkafeltételeiket;

d) a kritikus harmadik fél IKT-szolgáltató által a vezető felvigyázó ajánlásai alapján végrehajtott intézkedések alapján a 42. cikk (3) bekezdése szerint végzendő illetékes hatósági értékelés részleteit.

(2) Az EFH-knak az említett szabályozástechnikai standardtervezeteket 2024. július 17-ig be kell nyújtaniuk a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1094/2010/EU és az 1095/2010/EU rendelet 10–14. cikkében megállapított eljárással összhangban az (1) bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

42. cikk

Az illetékes hatóságok által végzett utókövetés

(1) A vezető felvigyázó által a 35. cikk (1) bekezdésének d) pontja alapján kiadott ajánlások kézhezvételét követő 60 naptári napon belül a kritikus harmadik fél IKT-szolgáltatónak vagy értesítenie kell a vezető felvigyázót arról, hogy végre kívánja hajtani az ajánlásokat, vagy indokolással ellátott magyarázatot kell adnia a vezető felvigyázónak arról, hogy miért nem kívánja végrehajtani az ajánlásokat. A vezető felvigyázónak a kapott tájékoztatást haladéktalanul továbbítania kell az érintett pénzügyi szervezetek illetékes hatóságainak.

(2) A vezető felvigyázónak nyilvánosságra kell hoznia, ha a kritikus harmadik fél IKT-szolgáltató nem értesíti a vezető felvigyázót az (1) bekezdésnek megfelelően, vagy ha a kritikus harmadik fél IKT-szolgáltató által nyújtott magyarázat nem tekinthető elégségesnek. A közzétett információknak tartalmazniuk kell a kritikus harmadik fél IKT-szolgáltató kilétét, valamint a meg nem felelés típusára és jellegére vonatkozó információkat. Az ilyen információknak a nyilvánosság tájékoztatásának biztosítása céljából releváns és arányos mértékre kell korlátozódniuk, kivéve, ha az ilyen közzététel aránytalan kárt okozna az érintett feleknek, vagy súlyosan veszélyeztethetné a pénzügyi piacok szabályos működését és integritását vagy az Unió pénzügyi rendszere egészének vagy egy részének stabilitását.

A vezető felvigyázónak értesítenie kell a harmadik fél IKT-szolgáltatót a nyilvánosságra hozatalról.

(3) Az illetékes hatóságoknak tájékoztatniuk kell a releváns pénzügyi szervezeteket a 35. cikk (1) bekezdésének d) pontjával összhangban megfogalmazott, a kritikus harmadik fél IKT-szolgáltatók számára tett ajánlásokban azonosított kockázatokról.

A harmadik féltől eredő IKT-kockázat kezelése során a pénzügyi szervezeteknek figyelembe kell venniük az első albekezdésben említett kockázatokat.

(4) Amennyiben az illetékes hatóság úgy ítéli meg, hogy a pénzügyi szervezet nem veszi figyelembe vagy nem kezeli megfelelően a harmadik féltől eredő IKT-kockázat saját kezelésén belül az ajánlásokban azonosított konkrét kockázatokat, értesítenie kell a pénzügyi szervezetet annak lehetőségéről, hogy az ilyen kockázatok kezelését célzó megfelelő szerződéses megállapodások hiányában a (6) bekezdés alapján az ilyen értesítés kézhezvételétől számított 60 naptári napon belül határozatot hozzon.

(5) A 35. cikk (1) bekezdésének c) pontjában említett jelentések kézhezvételét követően és az e cikk (6) bekezdésében említett határozat meghozatala előtt az illetékes hatóságok önkéntes alapon konzultálhatnak az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságokkal, amelyek felelősek valamely, kritikus harmadik fél IKT-szolgáltatóként kijelölt, az említett irányelv hatálya alá tartozó alapvető vagy fontos szervezet felügyeletéért.

(6) Az illetékes hatóságok végső eszközként – az értesítést és adott esetben az e cikk (4) és (5) bekezdésében meghatározottak szerinti konzultációt követően – az 50. cikkel összhangban határozhatnak úgy, hogy előírják a pénzügyi szervezetek számára a kritikus harmadik fél IKT-szolgáltató által nyújtott szolgáltatás igénybevételének vagy bevezetésének átmeneti – részleges vagy teljes – felfüggesztését a kritikus harmadik fél IKT-szolgáltató részére megfogalmazott ajánlásokban azonosított kockázatok kezeléséig. Az illetékes hatóságok szükség esetén előírhatják a kritikus harmadik fél IKT-szolgáltatóval kötött, releváns szerződéses megállapodások részleges vagy teljes megszüntetését.

(7) Amennyiben egy kritikus harmadik fél IKT-szolgáltató a vezető felvigyázó által javasolttól eltérő megközelítés alapján elutasítja az ajánlások jóváhagyását, és az ilyen eltérő megközelítés hátrányosan érintheti a pénzügyi szervezetek nagy számát, vagy a pénzügyi ágazat jelentős részét, és az illetékes hatóságok által kiadott egyedi figyelmeztetések nem vezettek a pénzügyi stabilitást fenyegető potenciális kockázatot csökkentő következetes megközelítésekhez, a vezető felvigyázó a felvigyázási fórummal folytatott konzultációt követően adott esetben nem kötelező erejű és nem nyilvános véleményeket fogalmazhat meg az illetékes hatóságok számára a következetes és konvergens felügyeleti utókövetési intézkedések előmozdítása érdekében.

(8) A 35. cikk (1) bekezdésének c) pontjában említett jelentések kézhezvételét követően az illetékes hatóságoknak az e cikk (6) bekezdésében említett határozat meghozatala során figyelembe kell venniük a kritikus harmadik fél IKT-szolgáltató által nem kezelt kockázat jellegét és nagyságát, továbbá a meg nem felelés jelentőségét, szem előtt tartva a következő kritériumokat:

a) a meg nem felelés súlyossága és időtartama;

b) a meg nem felelés súlyos gyengeségeket tárt-e fel a kritikus harmadik fél IKT-szolgáltató eljárásaiban, irányítási rendszereiben, kockázatkezelésében és belső kontrolljaiban;

c) a meg nem felelés megkönnyítette-e pénzügyi bűncselekmény elkövetését, előidézte-e azt, vagy egyébként annak tulajdonítható-e;

d) a meg nem felelés szándékos volt-e, vagy gondatlanság eredménye;

e) a szerződéses megállapodások felfüggesztése vagy megszüntetése kockázatot jelent-e a pénzügyi szervezet üzleti tevékenységeinek folytonosságára nézve, a pénzügyi szervezet arra irányuló erőfeszítéseinek ellenére, hogy elkerülje a szolgáltatásnyújtás zavarát;

f) adott esetben az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott azon illetékes hatóságok – önkéntes alapon, az e cikk (5) bekezdésével összhangban kikért – véleménye, amelyek felelősek valamely, kritikus harmadik fél IKT-szolgáltatóként kijelölt, az említett irányelv hatálya alá tartozó alapvető vagy fontos szervezet felügyeletéért.

Az illetékes hatóságoknak biztosítaniuk kell a pénzügyi szervezetek számára a szükséges időt ahhoz, hogy módosíthassák a kritikus harmadik fél IKT-szolgáltatókkal kötött szerződéses megállapodásaikat a digitális működési rezilienciájukra gyakorolt káros hatások elkerülése érdekében, valamint hogy lehetővé tegyék számukra a kilépési stratégiák és átállási tervek bevezetését, a 28. cikkben említetteknek megfelelően.

(9) Az e cikk (6) bekezdésében említett határozatról értesíteni kell a 32. cikk (4) bekezdésének a), b) és c) pontjában említett felvigyázási fórum tagjait és a KFH-t.

A (6) bekezdésben előírt határozatok által érintett, kritikus harmadik fél IKT-szolgáltatóknak teljes mértékben együtt kell működniük az érintett pénzügyi szervezetekkel, különösen szerződéses megállapodásaik felfüggesztésének vagy felmondásának folyamatával összefüggésben.

(10) Az illetékes hatóságoknak rendszeresen tájékoztatniuk kell a vezető felvigyázót a pénzügyi szervezetekkel kapcsolatos felügyeleti feladataik ellátása során alkalmazott megközelítésekről és intézkedésekről, valamint a pénzügyi szervezetek által azon esetekben alkalmazott szerződéses intézkedésekről, amikor a kritikus harmadik fél IKT-szolgáltatók részben vagy teljes egészében nem hagyták jóvá a vezető felvigyázó nekik szóló ajánlásait.

(11) A vezető felvigyázó kérésre további pontosításokat adhat a kiadott ajánlásokkal kapcsolatban, hogy iránymutatást nyújtson az illetékes hatóságoknak az utókövetési intézkedésekkel kapcsolatban.

43. cikk

Felvigyázási díjak

(1) A vezető felvigyázónak – az e cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktussal összhangban – díjakat kell felszámítania a kritikus harmadik fél IKT-szolgáltatókkal szemben, amelyek teljes mértékben fedezik a vezető felvigyázónál az e rendelet alapján végzett felvigyázási feladatokkal kapcsolatban felmerült szükséges kiadásokat, beleértve azon költségek megtérítését, amelyek a 40. cikkben említett közös vizsgálócsoport által végzett munka eredményeként merülhetnek fel, valamint a 32. cikk (4) bekezdésének második albekezdésében említett független szakértők által a közvetlen felvigyázási tevékenységek hatóköre alá tartozó kérdésekkel kapcsolatos tanácsadás költségeinek megtérítését is.

A kritikus harmadik fél IKT-szolgáltatónak felszámított díj összegének fedeznie kell az e szakaszban előírt feladatok ellátásából eredő valamennyi költséget, és arányosnak kell lennie annak forgalmával.

(2) A Bizottság felhatalmazást kap arra, hogy az 57. cikkel összhangban felhatalmazáson alapuló jogi aktust fogadjon el, amely a díj összegének és a díjfizetés 2024. július 17-ig történő megfizetése módjának meghatározásával kiegészíti ezt a rendeletet.

44. cikk

Nemzetközi együttműködés

(1) A 36. cikk sérelme nélkül az EBH, az ESMA és az EIOPA az 1093/2010/EU, az 1095/2010/EU és az 1094/2010/EU rendelet 33. cikkével összhangban igazgatási megállapodásokat köthet harmadik országbeli szabályozó és felügyeleti hatóságokkal annak érdekében, hogy előmozdítsa a különböző pénzügyi ágazatokra kiterjedő, harmadik féltől eredő IKT-kockázattal kapcsolatos nemzetközi együttműködést, különösen legjobb gyakorlatok kidolgozásával az IKT-kockázatkezelési gyakorlatok és kontroll, a kockázatcsökkentő intézkedések és az IKT-biztonsági eseményekre való reagálásra irányuló intézkedések területén.

(2) Az EFH-knak a vegyes bizottság keretében ötévenként közös, bizalmas jelentést kell benyújtaniuk be az Európai Parlamentnek, a Tanácsnak és a Bizottságnak, amelyben összefoglalják az (1) bekezdésben említett harmadik országbeli hatóságokkal folytatott releváns egyeztetések megállapításait, kiemelt figyelmet fordítva a harmadik féltől eredő IKT-kockázat alakulására, valamint a pénzügyi stabilitással, a piaci integritással, a befektetővédelemmel és a belső piac működésével kapcsolatos vonatkozásokra.

VI. FEJEZET

Információmegosztásra vonatkozó megállapodások

45. cikk

A kiberfenyegetéssel kapcsolatos információk és hírszerzés megosztására vonatkozó megállapodások

(1) A pénzügyi szervezetek kiberfenyegetésekkel kapcsolatban többek között az illetéktelen hozzáférésre utaló körülményekre, taktikákra, módszerekre, eljárásokra, kiberbiztonsági riasztásokra és konfigurációs eszközökre is kiterjedő információkat és hírszerzést oszthatnak meg egymással, amennyiben az ilyen információ- és hírszerzés-megosztás:

a) arra irányul, hogy a pénzügyi szervezetek javíthassák digitális működési rezilienciájukat, különösen a kiberfenyegetésekkel kapcsolatos tudatosság növelésével, a kiberfenyegetések terjedési képességének korlátozásával vagy megakadályozásával, a védelmi képességek, a fenyegetésészlelési módszerek, a mérséklési stratégiák vagy a reagálási és helyreállítási megoldások támogatásával;

b) pénzügyi szervezetek megbízható közösségein belül történik;

c) olyan információmegosztási megállapodások keretében történik, amelyek védik a megosztott információk esetlegesen érzékeny jellegét, és amelyek irányadó magatartási szabályai biztosítják az üzleti titoktartás, a személyes adatoknak az (EU) 2016/679 rendelettel összhangban történő védelme, valamint a versenypolitikára vonatkozó iránymutatások maradéktalan betartását.

(2) Az (1) bekezdés c) pontjának alkalmazásában az információmegosztási megállapodásoknak meg kell határozniuk a részvétel feltételeit, valamint adott esetben rögzíteniük kell a hatóságok bevonásának részleteit és azt, hogy azok milyen minőségben kapcsolódhatnak az információmegosztási megállapodásokhoz, a harmadik fél IKT-szolgáltatók bevonásának részleteit és a működési elemeket, ideértve a célzott informatikai platformok alkalmazását.

(3) A pénzügyi szervezeteknek értesíteniük kell az illetékes hatóságokat az (1) bekezdésben említett információmegosztási megállapodásban való részvételükről a tagságuk érvényesítésekor, vagy adott esetben a tagságuk megszűnéséről annak hatálybalépésekor.

VII. FEJEZET

Illetékes hatóságok

46. cikk

Illetékes hatóságok

A harmadik fél IKT-szolgáltatókra vonatkozó, e rendelet V. fejezetének II. szakaszában említett felvigyázási keretrendszer rendelkezéseinek sérelme nélkül az e rendeletnek való megfelelést a vonatkozó jogi aktusokban rájuk ruházott hatásköröknek megfelelően a következő illetékes hatóságok biztosítják:

a) hitelintézetek és a 2013/36/EU irányelv alapján mentesített intézmények esetében az említett irányelv 4. cikkével összhangban kijelölt illetékes hatóság, valamint az 1024/2013/EU rendelet 6. cikke (4) bekezdésével összhangban jelentősnek minősített hitelintézetek esetében az EKB, az említett rendeletben rá ruházott hatáskörökkel és feladatokkal összhangban;

b) pénzforgalmi intézmények, többek között az (EU) 2015/2366 irányelv alapján mentesített pénzforgalmi intézmények, elektronikuspénz-kibocsátó intézmények, többek között a 2009/110/EK irányelv alapján mentesített elektronikuspénz-kibocsátó intézmények és az (EU) 2015/2366 irányelv 33. cikkének (1) bekezdésében említett, számlainformációkat összesítő szolgáltatók esetében az (EU) 2015/2366 irányelv 22. cikkével összhangban kijelölt illetékes hatóság;

c) befektetési vállalkozások esetében az (EU) 2019/2034 európai parlamenti és tanácsi irányelv ([38]) 4. cikkével összhangban kijelölt illetékes hatóság;

d) a kriptoeszközök piacairól szóló rendelet alapján engedélyezett kriptoeszköz-szolgáltatók és az eszközalapú tokenek kibocsátói esetében az említett rendelet releváns rendelkezésével összhangban kijelölt illetékes hatóság;

e) központi értéktárak esetében a 909/2014/EU rendelet 11. cikkével összhangban kijelölt illetékes hatóság;

f) központi szerződő felek esetében a 648/2012/EU rendelet 22. cikkével összhangban kijelölt illetékes hatóság;

g) kereskedési helyszínek és adatszolgáltatók esetében a 2014/65/EU irányelv 67. cikkével összhangban kijelölt illetékes hatóság és a 600/2014/EU rendelet 2. cikke (1) bekezdésének 18. pontjában meghatározott illetékes hatóság;

h) kereskedési adattárak esetében a 648/2012/EU rendelet 22. cikkével összhangban kijelölt illetékes hatóság;

i) alternatívbefektetésialap-kezelők esetében a 2011/61/EU irányelv 44. cikkével összhangban kijelölt illetékes hatóság;

j) alapkezelő társaságok esetében a 2009/65/EK irányelv 97. cikkével összhangban kijelölt illetékes hatóság;

k) biztosítók és viszontbiztosítók esetében a 2009/138/EK irányelv 30. cikkével összhangban kijelölt illetékes hatóság;

l) biztosításközvetítők, viszontbiztosítás-közvetítők és kiegészítő biztosításközvetítői tevékenységet végző személyek esetében az (EU) 2016/97 irányelv 12. cikkével összhangban kijelölt illetékes hatóság;

m) foglalkoztatói nyugellátást szolgáltató intézmények esetében az (EU) 2016/2341 irányelv 47. cikkével összhangban kijelölt illetékes hatóság;

n) hitelminősítő intézetek esetében az 1060/2009/EK rendelet 21. cikkével összhangban kijelölt illetékes hatóság;

o) kritikus referenciamutatók kezelői esetében az (EU) 2016/1011 rendelet 40. és 41. cikkével összhangban kijelölt illetékes hatóság;

([38]) Az Európai Parlament és a Tanács (EU) 2019/2034 irányelve (2019. november 27.) a befektetési vállalkozások prudenciális felügyeletéről, valamint a 2002/87/EK, a 2009/65/EK, a 2011/61/EU, a 2013/36/EU, a 2014/59/EU és a 2014/65/EU irányelv módosításáról (HL L 314., 2019.12.5., 64. o.).

p) közösségi finanszírozási szolgáltatók esetében az (EU) 2020/1503 rendelet 29. cikkével összhangban kijelölt illetékes hatóság;

q) értékpapírosítási adattárak esetében az (EU) 2017/2402 rendelet 10. cikkével és 14. cikkének (1) bekezdésével összhangban kijelölt illetékes hatóság.

47. cikk

Együttműködés az (EU) 2022/2555 irányelvvel létrehozott struktúrákkal és hatóságokkal

(1) Az együttműködés elősegítése, valamint az e rendelet alapján kijelölt illetékes hatóságok és az (EU) 2022/2555 irányelv 14. cikkével létrehozott együttműködési csoport közötti felügyeleti kapcsolattartás lehetővé tétele érdekében az EFH-k és az illetékes hatóságok részt vehetnek az együttműködési csoport tevékenységeiben a pénzügyi szervezetekhez kapcsolódó felügyeleti tevékenységeiket illető kérdésekben. Az EFH-k és az illetékes hatóságok kérhetik, hogy felkérjék őket az együttműködési csoport tevékenységeiben való részvételre az (EU) 2022/2555 irányelv hatálya alá tartozó, azon alapvető vagy fontos szervezetekhez kapcsolódó kérdések tekintetében, amelyeket harmadik fél IKT-szolgáltatóként is kijelöltek e rendelet 31. cikkének értelmében.

(2) Adott esetben az illetékes hatóságok konzultálhatnak, és megoszthatnak információkat az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott egyedüli kapcsolattartó pontokkal és a CSIRT-ekkel.

(3) Az illetékes hatóságok adott esetben releváns szakvéleményt és technikai segítségnyújtást kérhetnek az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságoktól, és együttműködési megállapodásokat köthetnek a hatékony és gyors reagálásra képes koordinációs mechanizmusok létrehozása érdekében.

(4) Az e cikk (3) bekezdésében említett megállapodások meghatározhatják többek között az (EU) 2022/2555 irányelv hatálya alá tartozó, azon alapvető vagy fontos szervezetekkel kapcsolatos felügyeleti és felvigyázási tevékenységek koordinációjára vonatkozó eljárásokat, amelyeket e rendelet 31. cikke alapján harmadik fél IKT-szolgáltatókként jelöltek ki, beleértve a vizsgálatok és helyszíni ellenőrzések nemzeti joggal összhangban történő lefolytatása, továbbá az e rendelet szerinti illetékes hatóságok és az említett irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságok közötti, olyan információcserére vonatkozó mechanizmusok tekintetében, amely magában foglalja az utóbbi hatóságok által kért információkhoz való hozzáférést is.

48. cikk

A hatóságok közötti együttműködés

(1) Az illetékes hatóságoknak szorosan együtt kell működniük egymással és adott esetben a vezető felvigyázóval.

(2) Az illetékes hatóságoknak és a vezető felvigyázónak megfelelő időben kölcsönösen ki kell cserélniük egymással a harmadik fél IKT-szolgáltatókra vonatkozó minden olyan releváns információt, amely az e rendelet szerinti feladataik ellátásához szükséges, különösen a vezető felvigyázó felvigyázási feladatainak részeként azonosított kockázatokkal, megközelítésekkel és intézkedésekkel kapcsolatban.

49. cikk

Több pénzügyi ágazatra kiterjedő műveletek, kommunikáció és együttműködés

(1) Az EFH-k a vegyes bizottságon keresztül és együttműködve adott esetben az illetékes hatóságokkal, a 2014/59/EU irányelv 3. cikkében említett szanálási hatóságokkal, az EKB-val, a 806/2014/EU rendelet hatálya alá tartozó szervezetekre vonatkozó információk tekintetében az Egységes Szanálási Testülettel, az ERKT-val, valamint az ENISA-val mechanizmusokat alakíthatnak ki, amelyek lehetővé teszik az eredményes módszerek pénzügyi ágazatok közötti megosztását a helyzetismeret javítása, valamint az egyes ágazatok tekintetében közös kiber-sérülékenységek és -kockázatok azonosítása céljából.

Válságkezelési és vészhelyzeti műveleteket dolgozhatnak ki kibertámadási forgatókönyvek felhasználásával kommunikációs csatornák kialakítása, valamint az eredményes, koordinált uniós szintű reagálás fokozatos lehetővé tétele érdekében, hogy kezelhessék a jelentős, határokon átnyúló IKT-vonatkozású eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazat egészére.

Az említett műveletek adott esetben tesztelhetik a pénzügyi ágazat más gazdasági ágazatoktól való függőségeit is.

(2) Az illetékes hatóságoknak, az EFH-knak és az EKB-nek szorosan együtt kell működniük és információcserét kell folytatniuk a 47–54. cikk szerinti feladataik ellátása céljából. Felügyeleti tevékenységüket szorosan összehangolva kell végezniük annak érdekében, hogy azonosítsák és orvosolják e rendelet megsértésének eseteit, kidolgozzák és terjesszék a bevált módszereket, megkönnyítsék az együttműködést, előmozdítsák az egységes értelmezést, továbbá vitás esetekben joghatóságokon átívelő értékelést készítsenek.

50. cikk

Közigazgatási szankciók és korrekciós intézkedések

(1) Az illetékes hatóságoknak rendelkezniük kell minden olyan felügyeleti, vizsgálati és szankcionálási hatáskörrel, amely az e rendelet szerinti feladataik ellátásához szükséges.

(2) Az (1) bekezdésben említett hatásköröknek legalább a következő hatásköröket kell magukban foglalniuk:

a) bármilyen formájú betekintés bármilyen iratba vagy adatba, amelyet az illetékes hatóság feladatainak teljesítése szempontjából relevánsnak ítél, valamint másolat beszerzése vagy készítése azokról;

b) helyszíni ellenőrzések vagy vizsgálatok elvégzése, amelyek magukban foglalják többek között a következőket, ugyanakkor nem korlátozódnak azokra:

   i. a pénzügyi szervezetek képviselőinek felszólítása szóbeli vagy írásbeli magyarázatok szolgáltatására a vizsgálat tárgyával és céljával összefüggő tényekkel és dokumentumokkal kapcsolatban, valamint a válaszok rögzítése;

   ii. bármely egyéb olyan természetes vagy jogi személy meghallgatása, aki vagy amely hozzájárul ahhoz, hogy a vizsgálat tárgyával kapcsolatos információgyűjtés céljából meghallgassák;

c) az e rendeletben meghatározott követelmények megsértésével kapcsolatos korrekciós intézkedések előírása.

(3) A tagállamok azon jogának sérelme nélkül, hogy az 52. cikkel összhangban büntetőjogi szankciókat szabjanak ki, a tagállamok meghatározzák az e rendelet megsértése esetén alkalmazandó megfelelő közigazgatási szankciók és korrekciós intézkedések megállapításának szabályait, és biztosítják azok eredményes végrehajtását.

A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.

(4) A tagállamok hatáskörrel ruházzák fel az illetékes hatóságokat arra, hogy e rendelet megsértése esetén legalább a következő közigazgatási szankciókat vagy korrekciós intézkedéseket alkalmazzák:

a) végzés kibocsátása, amely előírja a természetes vagy jogi személy számára, hogy hagyjon fel az ezen rendeletet sértő magatartással, és tartózkodjon a magatartás megismétlésétől;

b) az illetékes hatóság által e rendelet rendelkezéseivel ellentétesnek ítélt gyakorlat vagy magatartás ideiglenes vagy tartós beszüntetésének az előírása, és az ilyen gyakorlat vagy magatartás ismételt előfordulásának a megakadályozása;

c) bármilyen típusú, akár pénzügyi jellegű intézkedés meghozatala, amely biztosítja, hogy a pénzügyi szervezetek folyamatosan betartsák a jogszabályi követelményeket;

d) amilyen mértékig ezt a nemzeti jog megengedi, a meglévő, valamely távközlési üzemeltető birtokában lévő adatforgalmi nyilvántartások bekérése, amennyiben észszerűen feltételezhető e rendelet megsértése, és amennyiben ezen nyilvántartások relevánsak lehetnek e rendelet megsértésének kivizsgálása szempontjából; és

e) nyilvános közlemény kiadása, ideértve a rendeletet megsértő természetes vagy jogi személy személyazonosságának és a jogsértés jellegének nyilvános közzétételét is.

(5) Amennyiben a (2) bekezdés c) pontjában és a (4) bekezdésben említett rendelkezések jogi személyekre alkalmazandók, a tagállamok arra vonatkozó hatáskört ruháznak az illetékes hatóságokra, hogy a közigazgatási szankciókat és korrekciós intézkedéseket – a nemzeti jogban megállapított feltételek mellett – a vezető testület azon tagjaira és más olyan egyénekre is alkalmazzák, akik a nemzeti jog szerint felelősséggel tartoznak a rendelet megsértéséért.

(6) A tagállamok biztosítják, hogy a (2) bekezdés c) pontjában meghatározott közigazgatási szankciókat vagy korrekciós intézkedéseket kiszabó bármely határozatot kellően megindokolják, és azzal szemben jogorvoslattal lehessen élni.

51. cikk

A közigazgatási szankciók és korrekciós intézkedések kiszabására vonatkozó hatáskörök gyakorlása

(1) Az illetékes hatóságoknak az 50. cikkben említett közigazgatási szankciók és korrekciós intézkedések kiszabására vonatkozó hatáskörüket adott esetben a nemzeti jogi kereteikkel összhangban kell gyakorolniuk a következők szerint:

a) közvetlenül;

b) más hatóságokkal együttműködve;

c) saját felelősségi körükön belül, más hatóságokra történő hatáskör-átruházás útján; vagy

d) az illetékes igazságügyi hatóságok megkeresése útján.

(2) Az illetékes hatóságoknak az e rendelet 50. cikke alapján kiszabandó közigazgatási szankció vagy korrekciós intézkedés típusának és szintjének meghatározása során figyelembe kell venniük, hogy a jogsértés mennyiben szándékos, vagy mennyiben származik gondatlanságból, valamint minden egyéb releváns körülményt, többek között – adott esetben – a következőket:

a) a jogsértés lényegessége, súlyossága és időtartama;

b) a jogsértésért felelős természetes vagy jogi személy felelősségének mértéke;

c) a felelős természetes vagy jogi személy pénzügyi stabilitása;

d) a felelős természetes vagy jogi személy által elért nyereség vagy elkerült veszteség fontossága, amennyiben azok meghatározhatók;

e) a jogsértés által harmadik feleknek okozott veszteség, amennyiben az meghatározható;

f) a felelős természetes vagy jogi személynek az illetékes hatósággal való együttműködésének szintje, nem érintve annak szükségességét, hogy biztosítani kell az említett természetes vagy jogi személy által – nyereség elérésével vagy veszteség elkerülésével – szerzett haszon visszaszolgáltatását;

g) a felelős természetes vagy jogi személy által elkövetett korábbi jogsértések.

52. cikk

Büntetőjogi szankciók

(1) A tagállamok dönthetnek úgy, hogy a nemzeti joguk alapján büntetőjogi szankciók hatálya alá tartozó jogsértésekre vonatkozóan nem állapítanak meg közigazgatási szankciókat vagy korrekciós intézkedéseket előíró szabályokat.

(2) Amennyiben a tagállamok úgy döntöttek, hogy büntetőjogi szankciókat írnak elő e rendelet megsértésére vonatkozóan, megfelelő intézkedésekkel biztosítják, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörökkel, hogy a joghatóságukon belül kapcsolatba lépjenek az igazságügyi, bűnüldöző vagy egyéb bűnügyi igazságszolgáltatási hatóságokkal annak érdekében, hogy az e rendelet megsértése miatt indított bűnügyi nyomozásokhoz vagy eljárásokhoz kapcsolódó konkrét információkat szerezzenek be, és azokat továbbítsák más illetékes hatóságoknak és az EBH-nak, az ESMA-nak vagy az EIOPA-nak, hogy e rendelet céljából teljesítsék együttműködési kötelezettségeiket.

53. cikk

Értesítési kötelezettség

A tagállamok 2025. január 17-ig értesítik a Bizottságot, az ESMA-t, az EBH-t és az EIOPA-t az e fejezetet végrehajtó törvényi, rendeleti és közigazgatási rendelkezésekről, ideértve bármely releváns büntetőjogi rendelkezést is. A tagállamok indokolatlan késedelem nélkül értesítik a Bizottságot, az ESMA-t, az EBH-t és az EIOPA-t az e rendelkezéseket érintő későbbi módosításokról is.

54. cikk

A közigazgatási szankciók nyilvánosságra hozatala

(1) Az illetékes hatóságoknak a hivatalos honlapjukon haladéktalanul közzé kell tenniük bármely, közigazgatási szankciót kiszabó határozatot, amellyel szemben nincs helye fellebbezésnek azt követően, hogy a szankció címzettjét értesítették az említett határozatról.

(2) Az (1) bekezdésben említett közzétételnek ki kell kiterjednie a jogsértés típusára és jellegére vonatkozó információkra, valamint a felelős személyek személyazonosságára és a kiszabott szankciókra.

(3) Amennyiben az illetékes hatóság eseti értékelés alapján úgy ítéli meg, hogy a jogi személyek kilétének vagy a természetes személyek személyazonosságának és személyes adatainak a közzététele aránytalan lenne, többek között a személyes adatok védelméhez kapcsolódó kockázatok miatt, vagy a közzététel veszélyeztetné a pénzügyi piacok stabilitását vagy egy folyamatban lévő nyomozást, vagy – amennyiben annak mértéke megállapítható – az érintett személynek aránytalan kárt okozna, az illetékes hatóságnak a közigazgatási szankciót kiszabó határozat tekintetében a következő megoldások egyikét kell alkalmaznia:

a) elhalasztja a közzétételt addig, amíg a közzététel ellen szóló indokok meg nem szűnnek;

b) a határozatot a nemzeti jogszabályokkal összhangban anonim jelleggel teszi közzé; vagy

c) mellőzi a közzétételt akkor, ha úgy ítéli meg, hogy az a) és b) pont szerinti megoldások elégtelenek, vagy nem garantálják, hogy a pénzügyi piacok stabilitása nem kerül veszélybe, vagy ha az ilyen közzététel nem állna arányban a kiszabott szankció engedékenységével.

(4) A közigazgatási szankció anonim közzétételéről szóló, a (3) bekezdés b) pontja szerinti határozat meghozatala esetén a releváns adatok közzététele elhalasztható.

(5) Amennyiben az illetékes hatóság olyan közigazgatási szankciót elrendelő határozatot tesz közzé, amely ellen az illetékes igazságügyi hatóságnál fellebbezés van folyamatban, az illetékes hatóságnak a hivatalos honlapján haladéktalanul közzé kell tennie az említett információt és bármely későbbi, az ilyen fellebbezés eredményével kapcsolatos információkat is. A közigazgatási szankciót elrendelő határozatot megsemmisítő bírósági határozatokat szintén közzé kell tenni.

(6) Az illetékes hatóságoknak biztosítaniuk kell, hogy az (1)–(4) bekezdésben említett bármely közzététel csak azon időszakra maradjon hivatalos honlapjukon, amely szükséges e cikk érvényesítéséhez. Ezen időszak nem haladhatja meg a közzétételtől számított öt évet.

55. cikk

Szakmai titoktartás

(1) A szakmai titoktartásnak a (2) bekezdésben meghatározott feltételeit az e rendelet alapján megkapott, kicserélt vagy továbbított minden bizalmas információra alkalmazni kell.

(2) Szakmai titoktartási kötelezettség alkalmazandó minden olyan személyre, aki az e rendelet szerint kijelölt illetékes hatóságnak vagy olyan hatóságnak vagy piaci vállalkozásnak vagy természetes vagy jogi személynek dolgozik vagy dolgozott, akire vagy amelyre az illetékes hatóság hatásköröket ruházott át, beleértve az illetékes hatóság által megbízott ellenőröket és szakértőket is.

(3) A szakmai titoktartás hatálya alá tartozó információk – többek között az e rendelet szerinti illetékes hatóságok és az (EU) 2022/2555 irányelvvel összhangban kijelölt vagy létrehozott illetékes hatóságok közötti információcsere – semmilyen más személlyel vagy hatósággal nem közölhetők, kivéve, ha ezt uniós vagy nemzeti joggal megállapított rendelkezések írják elő.

(4) Az e rendelet alapján az illetékes hatóságok között folytatott bármilyen, üzleti vagy működési feltételekkel, valamint más gazdasági vagy személyes jellegű ügyekkel kapcsolatos információcsere bizalmas adatközlésnek minősül, és a szakmai titoktartás követelményeinek hatálya alá tartozik, kivéve, ha az illetékes hatóság az információközléssel egyidejűleg megállapítja, hogy az ilyen információ nyilvánosságra hozható, vagy ha az ilyen nyilvánosságra hozatalt bírósági eljárás teszi szükségessé.

56. cikk

Adatvédelem

(1) Az EFH-k és az illetékes hatóságok csak akkor kezelhetnek személyes adatokat, ha az az e rendelet szerinti kötelezettségeik és feladataik teljesítéséhez szükséges, különösen vizsgálat, ellenőrzés, információkérés, kommunikáció, közzététel, értékelés, ellenőrzés, felmérés és felvigyázási tervek kidolgozása céljából. A személyes adatokat az (EU) 2016/679 vagy az (EU) 2018/1725 rendelettel összhangban kell kezelni, attól függően, hogy a két rendelet közül melyik alkalmazandó.

(2) Amennyiben más ágazati jogi aktusok másként nem rendelkeznek, az (1) bekezdésben említett személyes adatok az alkalmazandó felügyeleti feladatok teljesítéséig, de legfeljebb 15 évig őrizhetők meg, kivéve, ha az ilyen adatok további megőrzését igénylő bírósági eljárás van folyamatban.

VIII. FEJEZET

Felhatalmazáson alapuló jogi aktusok

57. cikk

A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás gyakorlásának feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 31. cikk (6) bekezdésében és a 43. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól 2024. január 17-én kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. Amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal az egyes időtartamok letelte előtt, a felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 31. cikk (6) bekezdésében és a 43. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban megállapított elvekkel összhangban konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 31. cikk (6) bekezdése és a 43. cikk (2) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő három hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam három hónappal meghosszabbodik.

IX. FEJEZET

Átmeneti és záró rendelkezések

I. szakasz

58. cikk

Felülvizsgálati záradék

(1) A Bizottság 2028. január 17-ig – adott esetben az EFH-kkal és az ERKT-val folytatott konzultációt követően – felülvizsgálatot végez, és – adott esetben jogalkotási javaslattal együtt – jelentést nyújt be az Európai Parlamentnek és a Tanácsnak. A felülvizsgálatnak ki kell terjednie legalább a következőkre:

a) a harmadik fél IKT-szolgáltatóknak a 31. cikk (2) bekezdése szerinti kijelölésére vonatkozó kritériumok;

b) a 19. cikkben említett, jelentős kiberfenyegetésekről szóló értesítés önkéntes jellege;

c) a 31. cikk (12) bekezdésében említett rendszer és a vezető felvigyázónak a 35. cikk (1) bekezdése d) pontja iv. alpontjának első francia bekezdésében meghatározott hatásköre, annak értékelése céljából, hogy az említett rendelkezések mennyire hatékonyak a harmadik országban letelepedett, harmadik fél IKT-szolgáltatók hatékony felvigyázásának biztosítása tekintetében, valamint hogy szükség van-e leányvállalat létrehozására az Unióban.

   E pont első albekezdésének alkalmazásában a felülvizsgálatnak ki kell terjednie a 31. cikk (12) bekezdésében említett rendszer elemzésére, többek között az uniós pénzügyi szervezetek harmadik országokból származó szolgáltatásokhoz való hozzáférését és az ilyen szolgáltatásoknak az uniós piacon való rendelkezésre állását illetően, és figyelembe kell vennie az e rendelet hatálya alá tartozó szolgáltatások piacán bekövetkező további fejleményeket, a pénzügyi szervezeteknek, illetve a pénzügyi felügyeleteknek az említett rendszer alkalmazása, illetve felügyelete tekintetében szerzett gyakorlati tapasztalatait, valamint a nemzetközi szinten bekövetkező releváns szabályozási és felügyeleti fejleményeket;

d) arra, hogy helyénvaló-e e rendelet hatálya alá vonni a 2. cikk (3) bekezdésének e) pontjában említett, automatizált értékesítési rendszereket alkalmazó pénzügyi szervezeteket az ilyen rendszerek használatával kapcsolatos jövőbeli piaci fejlemények fényében;

e) a KFH működése és hatékonysága a felvigyázás következetességének és a felvigyázási keretrendszeren belüli információcsere hatékonyságának támogatása terén.

(2) Az (EU) 2015/2366 irányelv felülvizsgálatával összefüggésben a Bizottság értékeli, hogy szükség van-e a fizetési rendszerek és a fizetésfeldolgozási tevékenységek kiber-rezilienciájának növelésére, valamint azt, hogy helyénvaló-e e rendelet hatályát kiterjeszteni a fizetési rendszerek üzemeltetőire és a fizetésfeldolgozási tevékenységekben részt vevő szervezetekre. Ezen értékelés fényében a Bizottság az (EU) 2015/2366 irányelv felülvizsgálatának részeként legkésőbb 2023. július 17-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak.

Az említett felülvizsgálati jelentés alapján, valamint az EFH-kal, az EKB-val és az ERKT-val folytatott konzultációt követően a Bizottság – adott esetben és azon jogalkotási javaslat részeként, amelyet az (EU) 2015/2366 irányelv 108. cikkének második bekezdése alapján fogadhat el – javaslatot nyújthat be annak biztosítására, hogy valamennyi fizetésirendszer-üzemeltető és valamennyi fizetésfeldolgozási tevékenységekben részt vevő szervezet megfelelő felvigyázás alatt álljon, figyelembe véve ugyanakkor a központi bank általi meglévő felügyeletet.

(3) A Bizottság 2026. január 17-ig – az EFH-kkal és a Európai Könyvvizsgálat-felügyeleti Szervek Bizottságával való konzultációt követően – felülvizsgálatot végez és indokolt esetben jogalkotási javaslattal együtt jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a jogszabály szerint engedélyezett könyvvizsgálókra és könyvvizsgáló cégekre vonatkozó megerősített követelményeknek a digitális működési reziliencia tekintetében való megfelelőségéről a jogszabály szerint engedélyezett könyvvizsgálóknak és könyvvizsgáló cégeknek e rendelet hatálya alá vonása vagy a 2006/43/EK európai parlamenti és tanácsi irányelv ([39]) módosítása révén.

II. szakasz

Módosítások

59. cikk

Az 1060/2009/EK rendelet módosításai

Az 1060/2009/EK rendelet a következőképpen módosul:

1. Az I. melléklet A. szakasza 4. pontja első albekezdésének helyébe a következő szöveg lép:

„A hitelminősítő intézetnek megbízható adminisztratív és számviteli eljárásokkal, belső ellenőrzési mechanizmusokkal, hatékony kockázatértékelési eljárásokkal, valamint az IKT-rendszerek kezelésére vonatkozó hatékony ellenőrzési és biztonsági szabályozással kell rendelkeznie az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333.., 2022.12.27., 1. o.).”

2. A III. melléklet 12. pontjának helyébe a következő szöveg lép:

„12. A hitelminősítő intézet megsérti a 6. cikk (2) bekezdését az I. melléklet A. szakasza 4. pontjával összefüggésben azáltal, ha nem rendelkezik megbízható adminisztratív vagy számviteli eljárásokkal, belső ellenőrzési mechanizmusokkal, hatékony kockázatértékelési eljárásokkal, vagy az IKT-rendszerek kezelésére vonatkozó hatékony ellenőrzési és biztonsági szabályozással az (EU) 2022/2554 rendelettel összhangban; vagy nem vezet be vagy nem tart fenn az említett pont által előírt határozathozatali eljárásokat vagy szervezeti felépítéseket.”

60. cikk

A 648/2012/EU rendelet módosításai

A 648/2012/EU rendelet a következőképpen módosul:

1. A 26. cikk a következőképpen módosul:

a) a (3) bekezdés helyébe a következő szöveg lép:

„(3) A központi szerződő félnek olyan szervezeti struktúrát kell fenntartania és üzemeltetnie, amely biztosítja a szolgáltatásnyújtás és a tevékenységvégzés folyamatosságát és rendes működését. Megfelelő és arányos rendszereket, erőforrásokat és eljárásokat, többek között az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban kezelt IKT-rendszereket kell alkalmaznia.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333.., 2022.12.27., 1. o.).”;

([39]) Az Európai Parlament és a Tanács 2006/43/EK irányelve (2006. május 17.) az éves és összevont (konszolidált) éves beszámolók jog szerinti könyvvizsgálatáról, a 78/660/EGK és a 83/349/EGK tanácsi irányelv módosításáról, valamint a 84/253/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 157., 2006.6.9., 87. o.).

b) a (6) bekezdést el kell hagyni.

2. A 34. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A központi szerződő fél megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet – beleértve az (EU) 2022/2554 rendelettel összhangban bevezetett és végrehajtott IKT-vonatkozású üzletmenet-folytonossági politikát, valamint IKT-reagálási és helyreállítási tervet – hoz létre, hajt végre és tart fenn annak céljából, hogy biztosítsa a központi szerződő fél funkcióinak megőrzését, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését.”;

b) a (3) bekezdés első albekezdésének helyébe a következő szöveg lép:

„(3) E cikk következetes alkalmazása érdekében az EÉPH a KBER tagjaival folytatott konzultációt követően kidolgozza az üzletmenet-folytonossági politika, valamint a vészhelyzeti helyreállítási terv minimális tartalmát és követelményeit meghatározó szabályozástechnikai standardok tervezetét, kivéve az IKT-vonatkozású üzletmenet-folytonossági politikát és a vészhelyzeti helyreállítási terveket.”.

3. Az 56. cikk (3) bekezdése első albekezdésének helyébe a következő szöveg lép:

„(3) E cikk következetes alkalmazása érdekében az ESMA kidolgozza – az IKT-kockázatkezelésre vonatkozó követelmények kivételével – az (1) bekezdésben említett, nyilvántartásba vétel iránti kérelem részleteit meghatározó szabályozástechnikai standardok tervezetét.”

4. A 79. cikk (1) és (2) bekezdésének helyébe a következő szöveg lép:

„(1) A kereskedési adattár azonosítja a működési kockázat forrásait, és minimalizálja azokat többek között a megfelelő rendszerek, ellenőrzések és eljárások kidolgozása révén, beleértve az (EU) 2022/2554 rendelettel összhangban kezelt IKT-rendszereket is.

(2) A kereskedési adattár megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet – beleértve az (EU) 2022/2554 rendelettel összhangban létrehozott IKT-vonatkozású üzletmenet-folytonossági politikát, valamint IKT-reagálási és helyreállítási tervet – hoz létre, hajt végre és tart fenn annak céljából, hogy biztosítsa a kereskedési adattár funkcióinak fenntartását, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését.”

5. A 80. cikk (1) bekezdését el kell hagyni.

6. Az I. melléklet II. szakasza a következőképpen módosul:

a) az a) és a b) pont helyébe a következő szöveg lép:

„a) a kereskedési adattár megsérti a 79. cikk (1) bekezdését azáltal, hogy nem azonosítja a működési kockázat forrásait, és nem minimalizálja azokat a megfelelő rendszerek, ellenőrzések és eljárások kidolgozása révén, beleértve az (EU) 2022/2554 rendelettel összhangban kezelt IKT-rendszereket is;

b) a kereskedési adattár megsérti a 79. cikk (2) bekezdését azáltal, hogy nem hoz létre, nem hajt végre és nem tart fenn az (EU) 2022/2554 rendelettel összhangban bevezetett megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet annak céljából, hogy biztosítsa a kereskedési adattár funkcióinak fenntartását, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését;”

b) a c) pontot el kell hagyni.

7. A III. melléklet a következőképpen módosul:

a) a II. szakasz a következőképpen módosul:

i. a c) pont helyébe a következő szöveg lép:

„c) a 2. szintű központi szerződő fél megsérti a 26. cikk (3) bekezdését, azáltal, hogy nem tart fenn vagy nem működtet olyan szervezeti struktúrát, amely biztosítja szolgáltatásainak és tevékenységeinek folyamatosságát és szabályos működését, vagy nem alkalmaz megfelelő és arányos rendszereket, erőforrásokat vagy eljárásokat, beleértve az (EU) 2022/2554 rendelettel összhangban kezelt IKT-rendszereket is;”

ii. az f) pontot el kell hagyni.

b) a III. szakasz a) pontjának helyébe a következő szöveg lép:

„a) a 2. szintű központi szerződő fél megsérti a 34. cikk (1) bekezdését azáltal, hogy nem hoz létre, hajt végre vagy tart fenn az (EU) 2022/2554 rendelettel összhangban bevezetett megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet annak céljából, hogy biztosítsa a központi szerződő fél működőképességének fenntartását, a műveletek időben történő helyreállítását és a kötelezettségeinek teljesítését, ami lehetővé teszi legalább a zavar bekövetkezésekor folyamatban lévő valamennyi tranzakció helyreállítását, hogy a központi szerződő fél biztonsággal folytatni tudja működését, és a tervezett időpontban le tudja zárni az ügyleteket;”.

61. cikk

A 909/2014/EU rendelet módosításai

A 909/2014/EU rendelet 45. cikke a következőképpen módosul:

1. Az (1) bekezdés helyébe a következő szöveg lép:

„(1) A központi értéktárnak meg kell határoznia a működési kockázatok külső és belső forrásait, és mérsékelnie kell azok hatását az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban létrehozott és kezelt megfelelő IKT-eszközök, -eljárások és -politikák bevezetése révén, valamint a működési kockázat más típusai – többek között az általa üzemeltetett valamennyi értékpapír-kiegyenlítési rendszer – esetében bármely egyéb releváns megfelelő eszközök, ellenőrzések és eljárások révén.

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333.., 2022.12.27., 1. o.).”

2. A (2) bekezdést el kell hagyni.

3. A (3) és a (4) bekezdés helyébe a következő szöveg lép:

„(3) A központi értéktárnak valamennyi nyújtott szolgáltatás és minden egyes üzemeltetett értékpapír-kiegyenlítési rendszer tekintetében megfelelő üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet – beleértve az (EU) 2022/2554 rendelettel összhangban kidolgozott IKT-vonatkozású üzletmenet-folytonossági politikát, valamint IKT-reagálási és helyreállítási tervet – kell kidolgoznia, bevezetnie és fenntartania, hogy biztosítsa a szolgáltatásnyújtása megőrzését, a működése mielőbbi helyreállítását és a kötelezettségei teljesítését olyan események bekövetkeztekor, amelyek komoly kockázatot jelentenek a működés megszakítására nézve.

(4) A (3) bekezdésben említett tervnek – többek közt annak biztosításával, hogy az (EU) 2022/2554 rendelet 12. cikkének (5) és (7) bekezdésében foglaltak szerint a kritikus informatikai rendszerek a leállás időpontjától kezdődően folytassák a működésüket – lehetővé kell tennie az üzemzavar bekövetkeztekor folyamatban lévő valamennyi tranzakciónak és a résztvevők pozícióinak a helyreállítását, hogy a központi értéktár résztvevői biztonsággal folytatni tudják működésüket, és az ütemezésnek megfelelően el tudják végezni a kiegyenlítést.”

4. A (6) bekezdés helyébe a következő szöveg lép:

„(6) A központi értéktárnak azonosítania, nyomon követnie és kezelnie kell azon kockázatokat, amelyeket az általa üzemeltetett értékpapír-kiegyenlítési rendszerek fő résztvevői, valamint a szolgáltatók és közműszolgáltatók vagy más központi értéktárak és piaci infrastruktúrák jelenthetnek a működésére. Kérésre az illetékes és releváns hatóságok rendelkezésére kell bocsátania a feltárt kockázatokkal kapcsolatos információkat. Haladéktalanul tájékoztatnia kell az illetékes hatóságot és a releváns hatóságokat az ilyen kockázatokból eredő működési zavarokról is, kivéve azokat, amelyek IKT-kockázattal összefüggésben következnek be.”

5. A (7) bekezdés első albekezdésének helyébe a következő szöveg lép:

„(7) Az ESMA – a KBER tagjaival szorosan együttműködve – szabályozástechnikai standardtervezeteket dolgoz ki, hogy meghatározza az (1) és a (6) bekezdésben említett, IKT-kockázattól eltérő működési kockázatokat és az e kockázatok tesztelésének, kezelésének vagy minimalizálásának módszereit, ideértve a (3) és a (4) bekezdésben említett üzletmenet-folytonossági politikát és vészhelyzeti helyreállítási tervet, valamint azok értékelési módszereit.”

62. cikk

A 600/2014/EU rendelet módosításai

A 600/2014/EU rendelet a következőképpen módosul:

1. A 27 g. cikk a következőképpen módosul:

   a) a (4) bekezdés helyébe a következő szöveg lép:

   „(4) Az APA-nak meg kell felelnie a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben (*) meghatározott követelményeknek.

   _____

   (*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333.., 2022.12.27., 1. o.).";

   b) a (8) bekezdés c) pontjának helyébe a következő szöveg lép:

   „c) a (3) és az (5) bekezdésben megállapított konkrét szervezeti követelményeket.".

2. A 27h. cikk a következőképpen módosul:

   a) az (5) bekezdés helyébe a következő szöveg lép:

   „(5) A CTP-nek meg kell felelnie a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2554 rendeletben meghatározott követelményeknek.";

   b) a (8) bekezdés e) pontjának helyébe a következő szöveg lép:

   „e) a (4) bekezdésben megállapított konkrét szervezeti követelményeket."

3. A 27i. cikk a következőképpen módosul:

   a) az (3) bekezdés helyébe a következő szöveg lép:

   „(3) Az ARM-nek meg kell felelnie a hálózati és információs rendszerek biztonságára vonatkozó, az (EU) 2022/2554 rendeletben meghatározott követelményeknek.";

   b) az (5) bekezdés b) pontjának helyébe a következő szöveg lép:

   „b) a (2) és a (4) bekezdésben megállapított konkrét szervezeti követelményeket."

63. cikk

Az (EU) 2016/1011 rendelet módosításai

Az (EU) 2016/1011 rendelet 6. cikke a következő bekezdéssel egészül ki:

„(6) A kritikus referenciamutatók tekintetében a referenciamutató-kezelőnek megbízható adminisztratív és számviteli eljárásokkal, belső kontrollmechanizmusokkal, hatékony kockázatértékelési eljárásokkal, valamint az IKT-rendszerek kezelésére vonatkozó hatékony kontroll- és biztonsági szabályozással kell rendelkeznie az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel (*) összhangban.

_____

(*) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333.., 2022.12.27., 1. o.)."

64. cikk

Hatálybalépés és alkalmazás

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

Ezt a rendeletet 2025. január 17-től kell alkalmazni.

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

Kelt Strasbourgban, 2022. december 14-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	M. BEK