Az Európai Unió
Tanácsa

Brüsszel, 2020. szeptember 24.
(OR. en)

11051/20

Intézményközi referenciaszám:
2020/0266(COD)

EF 228
ECOFIN 846
TELECOM 159
CYBER 168
IA 61
CODEC 871

JAVASLAT

Küldi:	az Európai Bizottság főtitkára részéről Jordi AYET PUIGARNAU igazgató
Az átvétel dátuma:	2020. szeptember 24.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2020) 595 final
Tárgy:	Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról

Mellékelten továbbítjuk a delegációknak a COM(2020) 595 final számú dokumentumot.

Melléklet: COM(2020) 595 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.9.24.
COM(2020) 595 final

2020/0266 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

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

(EGT-vonatkozású szöveg)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

INDOKOLÁS

1. A JAVASLAT HÁTTERE

- A javaslat indokai és céljai

Ez a javaslat a digitális pénzügyi szolgáltatásokra vonatkozó intézkedéscsomag része, amelynek célja, hogy az innováció és a verseny tekintetében még inkább lehetővé tegye és támogassa a digitális pénzügyi szolgáltatásokban rejlő potenciál kiaknázását, ugyanakkor mérsékelje az ezekből eredő kockázatokat. A javaslat összhangban van a Bizottság azon prioritásaival, amelyek célja egyfelől Európának a digitális kor kihívásaira való felkészítése, másfelől a jövő emberközpontú gazdaságának kialakítása. A digitális pénzügyi csomag az uniós pénzügyi ágazatra vonatkozó új, digitális pénzügyi szolgáltatási stratégiát[1] tartalmaz, amelynek célja annak biztosítása, hogy az EU éljen a digitális forradalom lehetőségével és innovatív európai vállalkozásokon keresztül vezető szerepet vállaljon abban, és ezáltal elérhetővé tegye az európai fogyasztók és vállalkozások számára a digitális pénzügyi szolgáltatások előnyeit. E javaslat mellett a csomag magában foglalja a kriptoeszközök piacairól szóló rendeletjavaslatot[2], a megosztott főkönyvi technológián (DLT) alapuló piaci infrastruktúrák kísérleti rendszeréről szóló rendeletjavaslatot[3], valamint a pénzügyi szolgáltatásokra vonatkozó egyes kapcsolódó szabályok pontosításáról, módosításáról szóló irányelvre irányuló javaslatot[4] is. A digitalizáció és a pénzügyi ágazat digitális működési rezilienciája ugyanazon érme két oldalát jelentik. A digitális, másképpen információs és kommunikációs technológiák (IKT) egyaránt hordoznak lehetőségeket és kockázatokat. Ezeket megfelelően kell ismerni és kezelni, különösen stresszhelyzetekben.

A szakpolitikai döntéshozók és a felügyeletek ezért egyre nagyobb figyelmet fordítanak az IKT használatából eredő kockázatokra. Az eddigiek során különösen standardok alkotásával, valamint a szabályozási, illetve felügyeleti munka összehangolásával próbálták erősíteni a vállalkozások rezilienciáját. Ez a munka nemzetközi és európai szinten is zajlott egyrészt ágazatközi jelleggel, másrészt egyes ágazatokra, köztük pénzügyi szolgáltatásokra összpontosítva.

Az IKT-kockázatok ennek ellenére továbbra is kihívást jelentenek az uniós pénzügyi rendszer digitális működési rezilienciája, teljesítménye és stabilitása szempontjából. A 2008. évi pénzügyi válságot követő reform elsősorban az uniós pénzügyi ágazat pénzügyi rezilienciáját[5] erősítette meg, az IKT-kockázatokkal csak közvetve foglalkozott egyes területeken a működési kockázatok átfogóbb kezelésére irányuló intézkedések részeként.

A pénzügyi szolgáltatásokra vonatkozó uniós jogszabályok válságot követő módosításai nyomán a pénzügyi szolgáltatásokkal összefüggő pénzügyi kockázatok jelentős részére kiterjedő egységes szabálykönyv lépett életbe, ennek során ugyanakkor a digitális működési reziliencia nem kapott teljes körű figyelmet. Az utóbbi kapcsán hozott intézkedéseknek

---

1 A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az uniós digitális pénzügyi szolgáltatási stratégiáról (2020. szeptember 23., COM(2020) 591).

2 A kriptoeszközök piacairól, valamint az (EU) 2019/1937 irányelv módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat (COM(2020) 593).

3 A megosztott főkönyvi technológián alapuló piaci infrastruktúrák kísérleti rendszeréről szóló európai parlamenti és tanácsi rendeletre irányuló javaslat (COM(2020)594).

4 A 2006/43/EK, a 2009/65/EK, 2009/138/EU, a 2011/61/EU, a 2013/36/EU, a 2014/65/EU, az (EU) 2015/2366, valamint az (EU) 2016/2341 irányelv módosításáról szóló európai parlamenti és tanácsi irányelvre irányuló javaslat (COM(2020) 596).

5 Az elfogadott különböző intézkedések célja alapvetően a pénzügyi szervezetek tőkeforrásainak és likviditásának bővítése, valamint a piaci és hitelkockázatok csökkentése volt.

számos olyan jellemzője volt, amelyek korlátozták az eredményességüket. Elfogadásuk például sok esetben minimális harmonizációt célzó irányelv vagy elvi rendelet formájában történt, ami jelentős teret hagyott az egymástól eltérő megközelítéseknek az egységes piacon. Az IKT-kockázatok emellett a működési kockázatok fedezésével összefüggésben csupán korlátozott, illetve részleges figyelmet kaptak. Végezetül pedig a pénzügyi szolgáltatásokra vonatkozó ágazati jogszabályok intézkedései sem egységesek. Az uniós szintű beavatkozás ennélfogva nem felelt meg maradéktalanul azoknak az igényeknek, amelyeket az európai pénzügyi szervezetek támasztottak annak kapcsán, hogy a működési kockázatot az IKT-vonatkozású biztonsági események elviselésére, elhárítására, valamint a hatásaik utáni helyreállításra alkalmas módon kezelhessék. Ugyanakkor a pénzügyi felügyeletek számára sem biztosította a legmegfelelőbb eszközöket azon megbízatásuk teljesítéséhez, hogy előzzék meg az ilyen IKT-kockázatok bekövetkezéséből eredő pénzügyi instabilitást.

A digitális működési rezilienciára vonatkozó részletes és átfogó uniós szintű szabályok hiányában egyre nagyobb számban jelentek meg a tagállami szabályozási kezdeményezések (pl. a digitális működési reziliencia tesztelése kapcsán), valamint a felügyeleti megközelítések (pl. a harmadik féltől való IKT-függőség kapcsán). Az IKT-kockázatok határokon átnyúló jellegéből adódóan azonban a tagállami szintű fellépés hatása korlátozott. Ráadásul az egymással össze nem hangolt tagállami kezdeményezések átfedéseket, ellentmondásokat, párhuzamos követelményeket, valamint – különösen a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára – aránytalanul magas adminisztratív és megfelelési költségeket eredményeztek, vagy azt, hogy az IKT-kockázatok felderítése és kezelése nem történt meg. Ez a helyzet az egységes piac széttagoltságához vezet, aláássa az uniós pénzügyi ágazat stabilitását és integritását, továbbá veszélyezteti a fogyasztók és a befektetők védelmét is.

Ezért az uniós pénzügyi szervezetek digitális működési rezilienciájára vonatkozóan részletes és átfogó keret kialakítása szükséges. Ez a keret elmélyíti az egységes szabálykönyv digitáliskockázat-kezelési dimenzióját. Ezen belül különösen bővíteni és észszerűsíteni fogja a pénzügyi szervezetek által végzett IKT-kockázatkezelést, kialakítja az IKT-rendszerek alapos tesztelését, növeli a felügyeletek tudatosságát a pénzügyi szervezeteket érintő kiberkockázatokkal és IKT-vonatkozású biztonsági eseményekkel kapcsolatban, emellett új felvigyázási hatásköröket vezet be a pénzügyi felügyeletek számára a pénzügyi szervezetek harmadik félnek minősülő IKT-szolgáltatóktól való függéséből eredő kockázatok tekintetében. A javaslat a biztonsági események bejelentését szolgáló egységes mechanizmus létrehozásával hozzájárul a pénzügyi szervezetek adminisztratív terheinek mérsékléséhez, valamint az eredményesebb felügyelethez.

- Összhang a szabályozási terület jelenlegi rendelkezéseivel

A javaslat az európai, illetve nemzetközi szinten folyamatban lévő átfogóbb munka része, amelynek célja a kiberbiztonság megerősítése a pénzügyi szolgáltatásokban, valamint az általánosabb működési kockázatok kezelése.[6]

Egyúttal figyelembe veszi az európai felügyeleti hatóságok (EFH-k) 2019. évi közös szakvéleményét[7] is, amely a pénzügyi szolgáltatásokat illetően szorgalmazta az IKT-kockázatok kezelésének koherensebb megközelítését, továbbá javasolta, hogy a Bizottság kifejezetten az uniós ágazatra irányuló kezdeményezés útján, arányosan erősítse meg a

[6] Bázeli Bankfelügyeleti Bizottság: *Cyber-resilience: Range of practices* (2018. december), valamint *Principles for sound management of operational risk (PSMOR)* (2014. október).

[7] Az európai felügyeleti hatóságok közös tanácsa az Európai Bizottságnak: az uniós pénzügyi ágazaton belüli IKT-kockázatkezelésre vonatkozó követelményekkel kapcsolatban a jogszabályok továbbfejlesztése szükséges (JC 2019 26 (2019)).

pénzügyi szolgáltatási ágazat digitális működési rezilienciáját. Az EFH-k a Bizottság 2018. évi pénzügyi technológiai cselekvési tervére[8] válaszul fogalmazták meg szakvéleményüket.

- Összhang az Unió egyéb szakpolitikáival

Amint azt von der Leyen elnök a politikai iránymutatásában[9], kijelentette, és az Európa digitális jövőjének megtervezéséről szóló közlemény[10] megfogalmazta, Európa számára létfontosságú, hogy a digitális kor minden előnyét kihasználja, és biztonságos és etikus keretek között megerősítse iparát és innovációs kapacitását. Az európai adatstratégia[11] négy pillért – adatvédelem, alapvető jogok, biztonság és kiberbiztonság – határoz meg annak szükséges előfeltételeként, hogy az adatok felhasználása a társadalmi önrendelkezést szolgálja. Újabb fejleményként az Európai Parlament a digitális pénzügyi szolgáltatásokról szóló jelentést készít, amely egyebek mellett közös megközelítés követésére szólít fel a pénzügyi ágazat kiberrezilienciája kapcsán.[12] Az uniós pénzügyi szervezetek digitális működési rezilienciáját megerősítő jogszabályi keret összhangban áll ezekkel a szakpolitikai célkitűzésekkel. A javaslat ezenkívül támogatná a koronavírus-járványt követő helyreállítást célzó szakpolitikai intézkedéseket is annak biztosításával, hogy a digitális pénzügyi szolgáltatások fokozottabb igénybevételét digitális működési reziliencia kísérje.

A kezdeményezés megtartaná a horizontális kiberbiztonsági kerethez (többek között a hálózati és információs rendszerek biztonságáról szóló – kiberbiztonsági – irányelvhez) köthető előnyöket azáltal, hogy annak hatálya változatlanul kiterjedne a pénzügyi ágazatra. A pénzügyi ágazat továbbra is szoros kapcsolatban maradna a Kiberbiztonsági Együttműködési Csoporttal, a pénzügyi felügyeletek pedig a meglévő kiberbiztonsági ökoszisztémán belül adhatnák át egymásnak a releváns információkat. A kezdeményezés összhangban állna az európai kritikus infrastruktúrákról szóló irányelvvel, amelynek folyamatban lévő felülvizsgálata erősíteni kívánja a kritikus infrastruktúrák védelmét és rezilienciáját a kibertéren kívül megjelenő fenyegetésekkel szemben. Végül ez a javaslat teljes összhangban áll a biztonsági unióra vonatkozó uniós stratégiával[13], amely a pénzügyi ágazat digitális működési rezilienciájával kapcsolatos kezdeményezésre hívott fel, tekintettel az ágazat IKT-szolgáltatásoktól való nagy fokú függőségére és a kibertámadásokkal szembeni nagy fokú sebezhetőségére.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

- Jogalap

A rendeletjavaslat az EUMSZ 114. cikkén alapul.

---

8 Európai Bizottság: *Pénzügyi technológiai cselekvési terv* (COM(2018) 109 final).

9 Politikai iránymutatás a hivatalba lépő következő Európai Bizottság számára (2019–2024) (https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_hu.pdf).

10 A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európa digitális jövőjének megtervezése* (COM(2020) 67 final).

11 A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: *Európai adatstratégia* (COM(2020) 66 final).

12 Jelentés a Bizottságnak szóló ajánlásokkal a digitális pénzügyi szolgáltatásokról: a kriptoeszközök miatt újonnan felmerülő kockázatok – szabályozási és felügyeleti kihívások a pénzügyi szolgáltatások, intézmények és piacok területén (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

13 A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A biztonsági unióra vonatkozó uniós stratégia (COM(2020) 605 final).

Javítja a pénzügyi szolgáltatások belső piacának kiépítését és működését biztosító feltételeket, továbbá elhárítja annak akadályait azzal, hogy harmonizálja az IKT-kockázatok kezelése és bejelentése, a tesztelés, valamint a harmadik féltől eredő IKT-kockázatok területén alkalmazandó szabályokat. A területen jelenleg a jogalkotás és a felügyelet szintjén, valamint a tagállamok és az Unió szintjén egyaránt meglévő eltérések akadályozzák a pénzügyi szolgáltatások egységes piacát, mivel a határokon átnyúló tevékenységet végző pénzügyi szervezetek eltérő, más esetekben pedig egymást átfedő szabályozási követelményekkel és felügyeleti elvárásokkal szembesülnek, ami megnehezítheti számukra a letelepedés és a szolgáltatásnyújtás szabadságának gyakorlását. Az eltérő szabályok emellett torzítják a különböző tagállamokban található, azonos típusú pénzügyi szervezetek közötti versenyt. Azokon a területeken, ahol nem, vagy csak részlegesen, illetve korlátozottan valósult meg a harmonizáció, az eltérő nemzeti szabályok és megközelítések, amelyek már hatályosak, vagy amelyek tagállami szintű elfogadása és végrehajtása jelenleg van folyamatban, ugyancsak visszatarthatják a pénzügyi szolgáltatások egységes piacához kapcsolódó szabadságok érvényesítését. Ez különösen igaz a digitális működési reziliencia tesztelési keretei, valamint a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázása kapcsán.

Mivel a javaslat az EUMSZ 53. cikkének (1) bekezdése alapján elfogadott európai parlamenti és tanácsi irányelvek közül többet is érint, egyidejűleg irányelvre irányuló javaslat elfogadására is sor kerül, amely tükrözi az érintett irányelvek szükséges módosításait.

- Szubszidiaritás

A pénzügyi szolgáltatások fokozott összekapcsoltsága, a pénzügyi szervezetek határokon átnyúló jelentős tevékenysége, valamint az, hogy a pénzügyi ágazat egésze nagymértékben függ a harmadik félnek minősülő IKT-szolgáltatóktól, indokolja az erős digitális működési reziliencia elősegítését, ami az uniós pénzügyi piacok stabilitásának megőrzését szolgáló közérdek. Az egyenlőtlen vagy részleges rendszerekből, az átfedésekből, valamint az ugyanazokra a határokon átnyúló tevékenységet végző, illetve az egységes piacon több engedéllyel[14] is rendelkező pénzügyi szervezetekre vonatkozó többszörös követelményekből adódó eltérések csak uniós szinten kezelhetők hatékonyan.

Ez a javaslat egy olyan szorosan integrálódott és összekapcsolt ágazat digitális működési komponensét harmonizálja, amelyre a többi kulcsterület többségén már egységes szabályrendszer és felügyelet vonatkozik. Az olyan kérdésekben, mint az IKT-vonatkozású biztonsági események bejelentése, kizárólag harmonizált uniós szabályokkal mérsékelhetők az azzal összefüggő adminisztratív terhek és pénzügyi költségek, hogy ugyanazt az IKT-vonatkozású biztonsági eseményt különböző uniós és nemzeti hatóságoknál kell bejelenteni. Uniós fellépés szükséges továbbá ahhoz is, hogy a digitális működési reziliencia fejlett módszerekkel kapott teszteredményeinek kölcsönös elismertetése könnyebbé váljon a határokon átnyúló tevékenységet végző szervezetek számára, amelyekre uniós szabályok hiányában eltérő keretek vonatkoznak vagy vonatkozhatnak a különböző tagállamokban. A tagállamok által bevezetett tesztelési módszerek eltérései kizárólag uniós szintű fellépéssel kezelhetők. Ugyancsak uniós szintű fellépés szükséges annak orvoslásához, hogy nincsenek megfelelő felvigyázási hatáskörök, amelyeket gyakorolva a hatóságok figyelemmel kísérhetnék a harmadik félnek minősülő IKT-szolgáltatókkal összefüggő kockázatokat, ezen belül az uniós pénzügyi ágazatot érintő koncentrációs és átterjedési kockázatokat.

[14] Ugyanaz a pénzügyi szervezet bankként, befektetési vállalkozásként és pénzforgalmi intézményként is rendelkezhet engedéllyel, amelyek mindegyikét adott esetben eltérő felügyelet adja ki egy vagy több tagállamban.

- Arányosság

A javasolt szabályok nem lépik túl a javaslatban kitűzött célok eléréséhez szükséges mértéket. A javaslat csak azokra a szempontokra terjed ki, amelyeket a tagállamok önmagukban nem tudnak megvalósítani, és ahol az adminisztratív terhek és költségek arányban állnak az elérendő konkrét és általános célkitűzésekkel.

Az arányosság terjedelem és intenzitás tekintetében kvalitatív és kvantitatív értékelési kritériumok alkalmazásával biztosítható. Ezek célja, hogy az új szabályok minden pénzügyi szervezetre kiterjedjenek, ugyanakkor igazodjanak a méret és üzleti profil szempontjából vett sajátosságaiknak megfelelő kockázatokhoz és szükségletekhez. Az arányosság elve érvényesül továbbá az IKT-kockázatkezeléssel, a digitális reziliencia tesztelésével, a jelentős IKT-vonatkozású biztonsági események bejelentésével, valamint a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázásával kapcsolatos szabályokban is.

- A jogi aktus típusának megválasztása

Az IKT-kockázatkezelés, az IKT-vonatkozású biztonsági események bejelentése, a tesztelés, valamint a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázásának szabályozásához szükséges intézkedéseket rendeletben szükséges előírni annak érdekében, hogy a részletes követelmények eredményesen, közvetlenül és egységesen alkalmazhatók legyenek az arányosság elve és az e rendeletben előírt konkrét szabályok sérelme nélkül. A digitális működési kockázatok egységes kezelése hozzájárul a pénzügyi rendszerbe vetett bizalom erősítéséhez, és megóvja annak stabilitását. Mivel rendelet útján csökkenthető a szabályozás összetettsége, elősegíthető a felügyeleti konvergencia és növelhető a jogbiztonság, ez a rendelet hozzájárul a pénzügyi szervezetek – különösen a határokon átnyúló tevékenységet végzők – megfelelési költségeinek mérsékléséhez is, ami viszont segítené a versenytorzulások megszüntetését.

E rendelet megszünteti továbbá az IKT-kockázatokkal kapcsolatos jogalkotási eltéréseket, valamint a heterogén tagállami szabályozási és felügyeleti megközelítéseket, ezáltal elhárítja a pénzügyi szolgáltatások egységes piacának akadályait, különösen azokat, amelyek a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára megnehezítik a letelepedés és a szolgáltatásnyújtás szabadságának zavartalan gyakorlását.

Végül pedig mivel az egységes szabálykönyv kidolgozása nagyrészt rendeletek formájában történt, azt a digitális működési reziliencia komponense tekintetében is célszerű azonos jogi eszköz útján kiegészíteni.

3. AZ UTÓLAGOS ÉRTÉKELÉSEK, AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

- A jelenleg hatályban lévő jogszabályok utólagos értékelése / célravezetőségi vizsgálata

A pénzügyi szolgáltatásokra vonatkozó eddigi uniós jogszabályok egyike sem foglalkozott a digitális működési rezilienciával vagy kezelte átfogóan a digitalizációból eredő kockázatokat, még azok sem, amelyeknek szabályai általánosabban foglalkoznak a működési kockázat dimenziójával, és ezen belül részkomponensként kezelik az IKT-kockázatokat. Az eddigi uniós beavatkozás azoknak a szükségleteknek és problémáknak a kezelését segítette elő, amelyek a 2008. évi pénzügyi válságot követően álltak fenn: a hitelintézetek tőkeellátottsága nem volt megfelelő, a pénzügyi piacok nem voltak kellően integráltak, a korábbi

harmonizáció pedig a minimumra szorítkozott. Az IKT-kockázatok akkor nem számítottak prioritásnak, ennek eredményeként a különböző pénzügyi szolgáltatási alágazatok jogi keretei nem egymással összehangoltan fejlődtek. Ennek ellenére az uniós fellépés elérte az arra irányuló célkitűzéseit, hogy biztosítsa a pénzügyi stabilitást, és egységes, harmonizált prudenciális és piaci magatartási szabályokat alkosson, amelyek hatálya minden pénzügyi szervezetre kiterjed az Unióban. Mivel a jogalkotáson alapuló uniós beavatkozást meghatározó tényezők korábban nem tették lehetővé, hogy akár egyedi, akár átfogó szabályok kezeljék a digitális technológiák széles körű használatát, valamint az ebből eredő kockázatokat a pénzügyi szolgáltatások területén, a közvetlen értékelés nehezen járhatónak tűnik. E rendelet mindegyik pillére a közvetett értékelési műveletet és az abból eredő jogszabály-módosításokat tükrözi.

- Konzultáció az érdekelt felekkel

A Bizottság e javaslat előkészítési folyamata során konzultált az érdekelt felekkel, ennek során:

i. célzott nyilvános konzultációt tartott (2019. december 19. – 2020. március 19.);[15]

ii. a Bizottság bevezető hatásvizsgálat keretében konzultált a nyilvánossággal (2019. december 19. – 2020. január 16.);[16]

iii. A Bizottság szolgálatai két alkalommal konzultációt folytattak a Bizottság banki, fizetési és biztosítási szakértői csoportjában a tagállami szakértőkkel (2020. május 18-án és 2020. július 16-án);[17]

iv. a Bizottság szolgálatai a 2020. évi „Digitális pénzügyi tájékoztatás” rendezvénysorozat részeként külön webináriumot tartottak a digitális működési rezilienciáról (2020. május 19.).

A nyilvános konzultáció útján a Bizottság a digitális működési rezilienciára vonatkozó ágazatközi uniós keret esetleges kialakításával kapcsolatban kívánt tájékozódni. A válaszadók széles körben támogatták egy célzott keretrendszer bevezetését, amelynek intézkedései a konzultáció négy témájára összpontosítanak, ugyanakkor hangsúlyozták, hogy az arányosság elvének érvényesülnie kell, továbbá körültekintően kezelni és ismertetni kell a kiberbiztonsági irányelv horizontális szabályaival való kölcsönhatást is. A bevezető hatásvizsgálattal kapcsolatban két válasz érkezett a Bizottsághoz, amelyekben a válaszadók a tevékenységi területükhöz kapcsolódó konkrét szempontokat emeltek ki.

A Bizottság banki, fizetési és biztosítási szakértői csoportjának 2020. május 18-án tartott megbeszélésén a tagállamok határozottan támogatták a pénzügyi ágazat digitális működési rezilienciájának a Bizottság által vázolt négy elem mentén előirányzott intézkedéseken keresztüli megerősítését. A tagállamok hangsúlyozták továbbá, hogy az új szabályoknak egyértelműen kell illeszkedniük a működési kockázattal kapcsolatos szabályokhoz (a pénzügyi szolgáltatásokkal kapcsolatos uniós jogszabályok keretében), valamint a kiberbiztonság horizontális szabályaihoz (a kiberbiztonsági irányelvhez). A második

15 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

16 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

17 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

megbeszélésen egyes tagállamok hangsúlyozták, hogy az arányosság elvének érvényesülése érdekében figyelemmel kell lenni a kisvállalkozásoknak és a nagyobb csoportok leányvállalatainak a sajátos helyzetére, valamint azt, hogy a felvigyázásban érintett illetékes nemzeti hatóságoknak erőteljes felhatalmazást kell kapniuk.

A javaslat emellett felhasználja és beépíti az érdekelt felekkel, valamint az uniós hatóságokkal és intézményekkel folytatott megbeszéléseken kapott visszajelzéseket is. Az érdekelt felek, köztük a harmadik félnek minősülő IKT-szolgáltatók összességében támogatóak voltak. A kapott visszajelzések elemzése alapján megállapítható az igény arra, hogy a szabályok kialakítására az arányosság megőrzésével, elv- és kockázatalapú megközelítésben kerüljön sor. Intézményi oldalon észrevételek főként az Európai Rendszerkockázati Testülettől (EKRT), az európai felügyeleti hatóságoktól, az Európai Uniós Kiberbiztonsági Ügynökségtől (ENISA), az Európai Központi Banktól, valamint a tagállamok illetékes hatóságaitól érkeztek.

- Szakértői vélemények összegyűjtése és felhasználása

E javaslat előkészítése során a Bizottság elismert forrásokból, köztük az európai felügyeleti hatóságok két közös szakvéleményéből származó kvalitatív és kvantitatív bizonyítékokra támaszkodott. Ezeket egészítették ki a bizalmas közlések, a felügyeleti hatóságok, a nemzetközi szabványügyi testületek és vezető kutatóintézetek nyilvánosan hozzáférhető jelentései, valamint a globális pénzügyi ágazat meghatározott érdekeltjeitől kapott kvalitatív és kvantitatív jelzések.

- Hatásvizsgálat

Ezt a javaslatot a Szabályozói Ellenőrzési Testületnek (RSB) 2020. április 29-én benyújtott és általa 2020. május 29-én jóváhagyott hatásvizsgálat[18] kíséri. Az RSB egyes területeken javításokat ajánlott annak érdekében, hogy a hatásvizsgálat: i. részletesebben mutassa be, hogy milyen módon érvényesülne az arányosság elve; ii. jobban emelje ki az előnyben részesített alternatíva eltéréseit az európai felügyeleti hatóságok két közös szakvéleményéhez képest, valamint azt, hogy miért az adott alternatíva tekinthető optimálisnak; továbbá iii. tegye hangsúlyosabbá a javaslat kölcsönhatását a meglévő uniós jogszabályokkal, beleértve a jelenleg felülvizsgálat alatt álló szabályokat is. A Bizottság a felvetett szempontok, valamint az RSB részletesebb észrevételeinek figyelembevételével módosította a hatásvizsgálatot.

A Bizottság a digitális működési reziliencia keretének kidolgozása kapcsán több szakpolitikai alternatívát mérlegelt:

- Nincs intézkedés: a digitális működési reziliencia szabályait továbbra is a pénzügyi szolgáltatásokra vonatkozó jelenlegi, sokrétű uniós rendelkezések: részben a kiberbiztonsági irányelv, részben pedig a meglévő vagy jövőbeli nemzeti rendszerek határoznák meg;
- 1. alternatíva: a tőkepufferek megerősítése: további tőkepufferek bevezetése, amely növeli a pénzügyi szervezetek képességét a digitális működési reziliencia hiányából eredő veszteségek elviselésére;
- 2. alternatíva: a pénzügyi szolgáltatások digitális működési rezilienciájára vonatkozó jogi aktus bevezetése: átfogó uniós szintű keret feltételeinek megteremtése,

[18] Bizottsági szolgálati munkadokumentum: A pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, valamint a 909/2014/EU rendelet módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatot kísérő hatásvizsgálati jelentés (SWD(2020) 198, 2020.9.24.).

amelyben egységes szabályok mentén kezelhetők a szabályozott pénzügyi szervezetek digitális működési rezilienciával kapcsolatos szükségletei, a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó felvigyázási keret kialakításával;

- 3. alternatíva: a pénzügyi szolgáltatások digitális működési rezilienciájára vonatkozó jogi aktus a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók központosított felügyeletével ötvözve: a digitális működési rezilienciára vonatkozó jogi aktus (2. alternatíva) mellett új hatóság létrehozása a harmadik félnek minősülő IKT-szolgáltatók által nyújtott szolgáltatások felügyelete céljából.

A Bizottság a második alternatívát tartotta meg, mivel az valósítja meg a legnagyobb mértékben az elérni kívánt célkitűzéseket eredményes, hatékony, más uniós szakpolitikákkal koherens módon. Az érdekelt felek többsége is ezt az alternatívát részesíti előnyben.

A választott alternatívával összefüggésben egyszeri és ismétlődő költségek is felmerülnének.[19] Az előbbiek főként az informatikai rendszerekre irányuló beruházásokból adódnak, ennélfogva az egyes vállalkozások összetett informatikai környezetének, ezen belül különösen hagyományos rendszereik eltérő állapota miatt nehezen számszerűsíthetők. Ezzel együtt a nagyvállalatokat valószínűleg csak mérsékelt költségek terhelik az eddig már végrehajtott jelentős IKT-beruházásaikra tekintettel. A költségek várhatóan alacsonyabbak lesznek a kisebb vállalkozások esetében is, amelyekre mérsékeltebb kockázatukkal arányos intézkedések vonatkoznának.

A választott alternatívának pozitív gazdasági, társadalmi és környezeti hatásai lennének a pénzügyi szolgáltatási ágazatban működő kkv-kra. A javaslat egyértelművé teszi a kkv-k számára az alkalmazandó szabályok körét, ami csökkenti a megfelelési költségeket.

A választott szakpolitikai alternatíva elsősorban a fogyasztókra és a befektetőre gyakorolna társadalmi hatást. Az uniós pénzügyi rendszer fokozott digitális működési rezilienciája csökkentené a biztonsági események számát és átlagos költségét. A pénzügyi szolgáltatási ágazat iránti erősebb bizalom a társadalom egésze számára előnyös lenne.

Végül pedig a környezeti hatásokat illetően a választott szakpolitikai alternatíva ösztönözné a legújabb generációs – környezeti szempontból várhatóan fenntarthatóbbá váló – IKT-infrastruktúrák és szolgáltatások nagyobb mértékű igénybevételét.

- Célravezető szabályozás és egyszerűsítés

Az IKT-vonatkozású biztonsági események bejelentésére vonatkozó követelmények közötti átfedések megszüntetése mérsékelné az adminisztratív terheket, és csökkentené a járulékos költségeket is. A digitális működési reziliencia harmonizált tesztelése és az egységes piacon belüli kölcsönös elismerése csökkenti a költségeket, különösen a határokon átnyúló tevékenységet végző vállalkozások számára, amelyeknek enélkül több tagállamban is tesztelniük kellene.[20]

- Alapjogok

Az EU elkötelezett amellett, hogy biztosítsa az alapjogok magas szintű védelmét. A pénzügyi szervezetek közötti minden önkéntes információmegosztásra vonatkozó, e rendelet által előmozdított megállapodás teljesítésére megbízható környezetben, az uniós adatvédelmi

[19] *Uo., 89–94. o.*
[20] *Uo.*

szabályok, nevezetesen az (EU) 2016/679 európai parlamenti és tanácsi rendelet[21] maradéktalan betartásával kerülne sor különösen akkor, ha az adatkezelő jogos érdekének érvényesítéséhez személyes adatok kezelésére van szükség.

(4) KÖLTSÉGVETÉSI VONZATOK

Költségvetési vonzatát illetően e rendelet kibővített szerepkört ír elő az európai felügyeleti hatóságok számára, amelynek kapcsán hatáskört ruház rájuk a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók megfelelő felvigyázására, ennélfogva a javaslat nagyobb erőforrásigényt eredményez különösen a felvigyázási feladatok (helyszíni és online vizsgálatok, ellenőrzési műveletek) elvégzésével, valamint a speciális IKT-biztonsági szakismeretekkel rendelkező munkatársak foglalkoztatásával összefüggésben.

E költségek nagyságrendje és megoszlása az új felvigyázási hatáskörök terjedelmétől, valamint az EFH-k által ellátandó pontos feladatkörtől függ majd. A személyi állomány bővítését illetően az EBH, az ESMA és az EIOPA együttesen teljes munkaidős egyenértékben (FTE) kifejezve 18 (hatóságonként 6) új munkavállalót igényel a javaslat különböző rendelkezéseinek hatálybalépését követően, ennek becsült költsége a 2022–2027 közötti időszakban 15,71 millió EUR. Az európai felügyeleti hatóságoknál ezenkívül járulékos informatikai, a helyszíni ellenőrzésekkel összefüggő feladatellátási, valamint fordítási költségek (együttes becsült összegük a 2022–2027 közötti időszakra 12 millió EUR), továbbá egyéb igazgatási kiadások (becsült összegük a 2022–2027 közötti időszakra 2,48 millió EUR) is felmerülnek. A 2022–2027 közötti időszakra becsült teljes költséghatás tehát mintegy 30,19 millió EUR.

Megjegyzendő továbbá, hogy a közvetlen felvigyázáshoz szükséges létszámot (az új munkatársak számát és az új feladatokkal összefüggő egyéb kiadásokat) a felvigyázás körébe tartozó, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók számának és méretének alakulása határozza meg, ugyanakkor a vonatkozó kiadások finanszírozására teljes egészében az említett piaci szereplőktől beszedendő díjakból kerül majd sor. Ezért a személyi állomány bővítésén túl a javaslat nem számol a költségvetési előirányzatokat érintő hatással.

E javaslat pénzügyi és költségvetési vonzatait az ehhez a javaslathoz csatolt pénzügyi kimutatás ismerteti részletesen.

(5) EGYÉB ELEMEK

- Végrehajtási tervek, valamint a nyomon követés, az értékelés és a jelentéstétel szabályai

A javaslat a konkrét célkitűzésekre gyakorolt hatások nyomon követésére és értékelésére vonatkozó általános tervet is magában foglal, amelynek kapcsán a Bizottságnak legalább a hatálybalépést követően három évvel felülvizsgálatot kell végeznie, és annak főbb megállapításairól be kell számolnia az Európai Parlamentnek és a Tanácsnak.

A felülvizsgálatot a minőségi jogalkotásra vonatkozó bizottsági iránymutatással összhangban kell végezni.

- A javaslat egyes rendelkezéseinek részletes magyarázata

[21] 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.).

Szerkezetileg a javaslat több szakpolitikai terület köré épül, amelyek egymáshoz kapcsolódó pillérei egyezményes alapon szerepelnek a pénzügyi ágazat kiberbiztonsági és digitális működési rezilienciájának erősítését célzó európai és nemzetközi iránymutatások és bevált módszerek között.

A rendelet hatálya, a szükséges intézkedések arányosság elvének megfelelő alkalmazása (2. cikk)

Annak érdekében, hogy a pénzügyi ágazatra egységes IKT-kockázatkezelési követelmények vonatkozzanak, a rendelet hatálya számos uniós szinten szabályozott pénzügyi szervezetre kiterjed, nevezetesen a hitelintézetekre, a pénzforgalmi intézményekre, az elektronikuspénz-kibocsátó intézményekre, a befektetési vállalkozásokra, a kriptoeszköz-szolgáltatókra, a központi értéktárakra, a központi szerződő felekre, a kereskedési helyszínekre, a kereskedési adattárakra, az alternatívbefektetésialap-kezelőkre és az alapkezelőkre, az adatszolgáltatókra, a biztosítókra és a viszontbiztosítókra, a biztosításközvetítőkre, a viszontbiztosítás-közvetítőkre és a kiegészítő biztosításközvetítői tevékenységet végző személyekre, a foglalkoztatói nyugellátást szolgáltató intézményekre, a hitelminősítő intézetekre, a jogszabály szerint engedélyezett könyvvizsgálókra és a könyvvizsgáló társaságokra, a kritikus referenciamutatók kezelőire, valamint az európai közösségi finanszírozási szolgáltatókra.

Az átfogó hatály elősegíti a kockázatkezelés valamennyi összetevőjének egységes és koherens alkalmazását az IKT-vonatkozású területeken, egyúttal az IKT-kockázatokkal kapcsolatos szabályozási kötelezettségek tekintetében biztosítja az egyenlő versenyfeltételeket a pénzügyi szervezetek számára. Ugyanakkor a rendelet figyelembe veszi azt is, hogy a pénzügyi szervezetek méret, üzleti profil, valamint a digitális kockázati kitettség szempontjából jelentősen eltérőek. Mivel a nagyobb pénzügyi szervezetek több erőforrással rendelkeznek, csak a mikrovállalkozásnak nem minősülő pénzügyi szervezetek kötelesek például összetett irányítási rendszereket és külön e célra vezetői funkciókat kialakítani, a hálózati és információs rendszerek infrastruktúrájának jelentősebb változásait követően beható vizsgálatokat végezni, rendszeresen elvégezni az örökölt IKT-rendszerek kockázatelemzését, továbbá az üzletmenet-folytonossági, elhárítási és helyreállítási tervek tesztelését kiterjeszteni az elsődleges IKT-infrastruktúrájuk és a tartalék eszközök közötti átállásra. Ezenfelül a fenyegetettségi szempontú behatolási tesztelés csak az olyan pénzügyi szervezetek számára lesz kötelező, amelyek a digitális működési reziliencia fejlett módszerekkel végzett tesztelése szempontjából jelentősnek minősülnek.

Átfogó jellege ellenére a rendelet hatálya nem teljes. Nem terjed ki különösen a fizetési és értékpapír-elszámolási rendszerekben az elszámolások véglegességéről szóló 98/26/EK európai parlamenti és tanácsi irányelv[22] (SFD) 2. cikkének p) pontjában meghatározott rendszerüzemeltetőkre, sem az ilyen rendszerek résztvevőire, kivéve akkor, ha a résztvevő maga is uniós szinten szabályozott pénzügyi szervezet (hitelintézet, befektetési vállalkozás, központi szerződő fél), amely ennélfogva önmagában is e rendelet hatálya alá tartozik. A rendelet hatálya nem terjed ki továbbá az uniós kibocsátásiegység-forgalmi jegyzékre sem, amely a 2003/87/EK irányelvvel[23] összhangban az Európai Bizottság égisze alatt működik.

[22] Az Európai Parlament és a Tanács 98/26/EK irányelve (1998. május 19.) a fizetési és értékpapír-elszámolási rendszerekben az elszámolások véglegességéről (HL L 166., 1998.6.11., 45. o.).

[23] Az Európai Parlament és a Tanács 2003/87/EK irányelve (2003. október 13.) az üvegházhatást okozó gázok kibocsátási egységei Közösségen belüli kereskedelmi rendszerének létrehozásáról és a 96/61/EK tanácsi irányelv módosításáról, HL L 275., 2003.10.25., 32. o.).

Az SFD hatálya alóli kizárások figyelembe veszik azt, hogy az SFD szerinti rendszerüzemeltetőket és résztvevőket érintő jogi és szakpolitikai kérdések további felülvizsgálata szükséges, ennek során azonban megfelelően mérlegelni kell a központi bankok által üzemeltetett fizetési rendszerek[24] jelenlegi kereteire gyakorolt hatást is. Mivel e kérdések olyan szempontokat is érinthetnek, amelyek nem kapcsolódnak az e rendelettel szabályozott kérdéskörbe, a Bizottság folyamatosan vizsgálja, hogy szükséges-e a rendelet hatályának további, jelenleg azon kívül eső szervezetekre és IKT-infrastruktúrákra történő kiterjesztése, és ha igen, az milyen hatással járna.

Irányítási követelmények (4. cikk)

E rendelet célja, hogy jobban összehangolja egymással a pénzügyi szervezetek üzleti stratégiáit és IKT-kockázatkezelését. Ennek érdekében a vezető testületnek tevékeny és központi szerepet kell játszania az IKT-kockázatkezelési keretrendszer irányításában, és törekednie kell a szigorú kiberhigiénia betartatására. A pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testületet terhelő teljes körű felelősség általános elv, amelyet olyan konkrét követelmények formájában kell érvényesíteni, mint az egyértelmű feladat- és felelősségi körök kijelölése minden IKT-vonatkozású funkcióra vonatkozóan, a folyamatos részvétel az IKT-kockázatkezelés nyomon követésének kontrolljában, valamint a jóváhagyási és kontrollfolyamatok teljes körében, továbbá az IKT-beruházások és -képzések megfelelő elosztása.

IKT-kockázatkezelésre vonatkozó követelmények (5–14. cikk)

Az európai felügyeleti hatóságok közös szakvéleményével összhangban a digitális működési reziliencia az IKT-kockázatkezelési keretrendszerre vonatkozó alapvető elvekből és követelményekből ered. A vonatkozó nemzetközi, nemzeti és ágazati standardok, iránymutatások és ajánlások nyomán kidolgozott követelmények konkrét IKT-kockázatkezelési funkciók köré épülnek (azonosítás, védelem és megelőzés, felderítés, elhárítás és helyreállítás, tanulás és alkalmazkodás, kommunikáció). Ahhoz, hogy lépést tarthassanak a gyorsan változó kiberfenyegetettségi helyzettel, a pénzügyi szervezeteknek reziliens IKT-rendszereket és -eszközöket kell kialakítaniuk és fenntartaniuk, amelyek minimálisra csökkentik az IKT-kockázat hatását, folyamatosan azonosítaniuk kell az IKT-kockázat valamennyi forrását, védelmi és megelőző intézkedéseket kell bevezetniük, azonnal észlelniük kell a rendellenes tevékenységeket, továbbá célzott és átfogó üzletmenet-folytonossági szabályokat, valamint katasztrófaelhárítási és helyreállítási terveket kell bevezetniük operatív üzletmenet-folytonossági politikájuk szerves részeként. Ez utóbbi összetevőkre az IKT-vonatkozású biztonsági eseményeket (különösen a kibertámadásokat) követő azonnali helyreállításhoz van szükség, amelynek során elsődleges a károk mérséklése és a tevékenység biztonságos újraindítása. Maga a rendelet nem ír elő konkrét szabványosítást, inkább az európai és nemzetközileg elismert technikai szabványokra és ágazati bevált módszerekre épít, amennyiben azok teljes mértékben megfelelnek a nemzetközi standardok felhasználására vonatkozó felügyeleti utasításoknak. E rendelet szabályozza továbbá a technológia felhasználását támogató fizikai infrastruktúrák és létesítmények, valamint az ebben érintett IKT-vonatkozású folyamatok és személyek integritását, biztonságát és rezilienciáját a pénzügyi szervezet által végzett tevékenység digitális lábnyomának részeként.

IKT-vonatkozású biztonsági események bejelentése (15–20. cikk)

[24] Az Európai Központi Bank 795/2014/EU rendelete (2014. július 3.) a rendszerszempontból jelentős fizetési rendszerekre vonatkozó felvigyázási követelményekről.

Az IKT-vonatkozású biztonsági események bejelentésének harmonizálása és észszerűsítése először is egy olyan általános követelmény formájában valósul meg, amely szerint a pénzügyi szervezeteknek irányítási folyamatot kell kialakítaniuk és végrehajtaniuk az IKT-vonatkozású biztonsági események nyomon követésére és rögzítésére, majd az eseményeket a rendeletben részletesen kifejtett és az EFH-k által lényegességi küszöbértékek meghatározása céljából továbbfejlesztett kritériumok alapján osztályozniuk kell. Másodszor: csak a jelentősnek minősülő IKT-vonatkozású biztonsági eseményeket kell bejelenteni az illetékes hatóságoknál. A bejelentéseket közös minta alapján, az EFH-k által kialakított, harmonizált eljárás mentén célszerű feldolgozni. A pénzügyi szervezeteknek előzetes, időközi és végleges jelentést kell benyújtaniuk, továbbá tájékoztatniuk kell felhasználóikat és ügyfeleiket, ha az eseménynek hatása volt vagy lehetett pénzügyi érdekeikre. Az illetékes hatóságoknak át kell adniuk a biztonsági események vonatkozó adatait más intézmények és hatóságok: az EFH-k, az EKB, valamint az (EU) 2016/1148 irányelv szerint kijelölt egyedüli kapcsolattartó pontok részére.

A jelentős IKT-vonatkozású biztonsági események bejelentését felügyeleti visszajelzésnek és iránymutatásnak kell kiegészítenie, amely alapján párbeszéd indulhat a pénzügyi szervezetek és az illetékes hatóságok között a hatás mérséklése és a megfelelő korrekciós intézkedések meghatározása céljából.

Végül pedig az IKT-vonatkozású biztonsági események bejelentésének uniós szintű központosítási lehetőségét az EFH-k, az EKB és az ENISA közös jelentésében kell részletesebben vizsgálni, amely értékeli egy egységes uniós központi adatbázis létrehozásának megvalósíthatóságát, amelynek segítségével a pénzügyi szervezetek bejelenthetik a jelentős IKT-vonatkozású biztonsági eseményeket.

A digitális működési reziliencia tesztelése (21–24. cikk)

Az IKT-kockázatkezelési keretrendszerben foglalt képességeket és funkciókat időszakosan tesztelni kell a felkészültség ellenőrzése, a gyenge pontok és hiányosságok azonosítása, valamint a korrekciós intézkedések haladéktalan végrehajtása céljából. Ez a rendelet lehetővé teszi a digitális működési reziliencia tesztelésére vonatkozó követelményeknek a pénzügyi szervezetek méretétől, valamint üzleti és kockázati profiljától függő arányos alkalmazását: IKT-eszközeit és rendszereit minden szervezetnek tesztelnie kell, ugyanakkor a fenyegetettségi szempontú behatolási tesztekre (TLPT) épülő fejlett tesztelés csak olyan szervezetek számára írható elő, amelyeket az illetékes hatóságok az e rendeletben rögzített és az EFH-k által továbbfejlesztett kritériumok alapján jelentősnek és „kiberérettnek” minősítenek. Ez a rendelet követelményeket határoz meg továbbá a tesztelőkre, valamint a több tagállamban működő pénzügyi szervezetek esetében a fenyegetettségi szempontú behatolási tesztek eredményeinek uniós szintű elismerésére vonatkozóan.

Harmadik féltől eredő IKT-kockázat (25–39. cikk)

A rendelet egyik célkitűzése, hogy biztosítsa a harmadik féltől eredő IKT-kockázat megbízható nyomon követését. Ez a célkitűzés először is azoknak az elvalapú szabályoknak a betartásával érhető el, amelyek alkalmazásával a pénzügyi szervezeteknek nyomon kell követniük a harmadik félnek minősülő IKT-szolgáltatók igénybevételéből eredő kockázatokat. Másodszor: a rendelet harmonizálja a harmadik félnek minősülő IKT-szolgáltatóval meglévő kapcsolat és a szolgáltatás fő elemeit. Ezek az elemek az ahhoz minimálisan szükségesnek tekinthető szempontokat foglalják magukban, hogy a pénzügyi szervezet teljeskörűen nyomon kövesse a harmadik féltől eredő IKT-kockázatot a harmadik féllel való kapcsolat létesítése, teljesítése és megszűnése során, valamint annak szerződés utáni szakaszában.

Ezen belül különösen lényeges, hogy a kapcsolatot szabályozó szerződés tartalmazza a szolgáltatások teljes leírását, az adatkezelési helyszínek megjelölését, a szolgáltatási szintek teljes körű leírását a mennyiségi és minőségi teljesítménycélokkal együtt, a személyes adatok hozzáférhetőségére, rendelkezésre állására, integritására, biztonságára és védelmére vonatkozó releváns rendelkezéseket, a harmadik félnek minősülő IKT-szolgáltatók megszűnése esetére vonatkozó hozzáférési, visszaszerzési és visszaszolgáltatási garanciákat, a harmadik félnek minősülő IKT-szolgáltatók felmondási idejét és bejelentési kötelezettségeit, a pénzügyi szervezet vagy az általa kijelölt harmadik fél hozzáférési, vizsgálati és ellenőrzési jogosultságait, a felmondási jog egyértelmű meghatározását, valamint a konkrét kilépési stratégiákat. Ráadásul mivel a felsorolt szerződéses elemek egy része standardizálható, a rendelet előmozdítja a felhőszolgáltatás igénybevételére vonatkozóan a Bizottság által kidolgozandó általános szerződéses rendelkezések önkéntes alkalmazását.

Végül pedig a rendeletnek célja az is, hogy előmozdítsa a pénzügyi ágazat harmadik féltől eredő IKT-kockázatával kapcsolatos felügyeleti megközelítések konvergenciáját azáltal, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra is kiterjeszti az uniós felvigyázási keret hatályát. Egy új, harmonizált jogszabályi keretben az egyes harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók vezető felvigyázójaként kijelölt EFH olyan hatásköröket kap, amelyeket gyakorolva biztosíthatja a pénzügyi ágazat működésében kulcsfontosságú szerepet betöltő technológiai szolgáltatók megfelelő, páneurópai léptékű figyelemmel kísérését. Az e rendeletben meghatározott felvigyázási keret a pénzügyi szolgáltatások területén meglévő intézményi struktúrára épít úgy, hogy az EFH-k vegyes bizottsága – a kiberbiztonsággal kapcsolatos feladataival összhangban – biztosítja az ágazatközi koordinációt az IKT-kockázatot érintő valamennyi kérdésben, ennek során pedig a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó egyedi döntéseket és a részükre megfogalmazott kollektív ajánlásokat előkészítő releváns albizottság (felvigyázási fórum) munkájára támaszkodik.

Információmegosztás (40. cikk)

Annak érdekében, hogy tudatosítsa az IKT-kockázatot, minimálisra csökkentse annak terjedését, továbbá támogassa a pénzügyi szervezetek védelmi képességeit és fenyegetésészlelési módszereit, a rendelet lehetővé teszi a pénzügyi szervezetek számára olyan megállapodások megkötését, amelyek keretében kiberfenyegetettségi adatokat és információkat adhatnak át egymásnak.

2020/0266 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU 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 tervezetének a nemzeti parlamenteknek való továbbítását követően,

tekintettel az Európai Központi Bank véleményére,[25]

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére,[26]

rendes jogalkotási eljárás keretében,

mivel:

(1) A digitális korban a mindennapos társadalmi tevékenységek során alkalmazott összetett rendszereket információs és kommunikációs technológiák (IKT) támogatják. E technológiák biztosítják a gazdaság folyamatos működését a kulcsfontosságú ágazatokban, beleértve a pénzügyi szolgáltatásokat is, emellett javítják az egységes piac működését is. Minél nagyobb méreteket ölt a digitalizáció és az összekapcsoltság, annál nagyobbak az IKT-kockázatok is, ami a társadalom egészét, azon belül pedig különösen a pénzügyi rendszert kiszolgáltatottabbá teszi a kiberfenyegetésekkel és az IKT-zavarokkal szemben. Az IKT-rendszerek általános alkalmazása, valamint a nagy fokú digitalizáció és összekapcsoltság napjainkban az uniós pénzügyi szervezetek valamennyi tevékenységének alapvető jellemzői, a digitális reziliencia egyelőre mégsem épült be kellő mértékben e szervezetek működési kereteibe.

(2) Az IKT használata az elmúlt évtizedekben egyre meghatározóbb szerephez jutott a pénzügyi szolgáltatásokban, ma már pedig alapvető fontossággal bír minden pénzügyi szervezet jellemző mindennapos funkcióinak működésében. A digitalizáció kiterjed például a fizetésekre, ahol a készpénz- és papíralapú módszereket mind inkább a digitális megoldások alkalmazása váltja fel, emellett az értékpapírok elszámolására és kiegyenlítésére, az elektronikus és algoritmikus kereskedésre, a hitelnyújtási és finanszírozási műveletekre, a személyközi finanszírozásra, a hitelminősítésekre, a biztosítási kockázatvállalásra, a követeléskezelésre, valamint a háttértevékenységekre. Amellett, hogy a pénzügyi szolgáltatások az ágazat egészében nagyrészt digitálissá váltak, a digitalizáció fokozottabb összekapcsoltságot és kölcsönös függést is

[25] [*HL-hivatkozás*] HL C […], […], […] o.
[26] [*HL-hivatkozás*] HL C […], […], […] o.

eredményezett mind a pénzügyi ágazaton belül, mind pedig a harmadik felektől igénybe vett infrastruktúrák és szolgáltatások terén.

(3) Az Európai Rendszerkockázati Testület (ERKT) a rendszerszintű kiberkockázattal foglalkozó 2020. évi jelentésében[27] megerősítette, hogy a pénzügyi szervezetek, a pénzügyi piacok és a pénzügyi piaci infrastruktúrák nagy fokú összekapcsoltságából, és különösen IKT-rendszereik kölcsönös függéseiből miképpen származhat rendszerszintű sebezhetőség amiatt, hogy a lokalizált kiberbiztonsági események a mintegy 22 000 uniós pénzügyi szervezet[28] bármelyikéről gyorsan, földrajzi határoktól függetlenül átterjedhetnek a teljes pénzügyi rendszerre. Az IKT-biztonság pénzügyi szolgáltatások ágazatában bekövetkező sérülése nemcsak elszigetelt pénzügyi szervezeteket érint. Lehetővé teszi a lokalizált sebezhetőségek pénzügyi transzmissziós csatornákon keresztüli zavartalan terjedését is, emellett káros következményekkel járhat az uniós pénzügyi rendszer stabilitására nézve is, ami likviditáselvonási hullámokat és a pénzügyi piacokkal szembeni általános bizalomvesztést eredményez.

(4) Az elmúlt években az IKT-kockázatok felkeltették a nemzeti, európai és nemzetközi szakpolitikai döntéshozó, szabályozó és standardalkotó szervezetek figyelmét, amelyek a reziliencia erősítésére, standardok alkotására, a szabályozói és felügyeleti munka összehangolására törekszenek. 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-csoport célja, hogy a különböző joghatósági területek illetékes hatóságai és piaci szereplői a pénzügyi rendszereik rezilienciáját támogató eszközökhöz jussanak.

(5) A tagállami és európai szintű célzott szakpolitikai és jogalkotási kezdeményezések ellenére az IKT-kockázatok továbbra is kihívást jelentenek az uniós pénzügyi rendszer digitális működési rezilienciája, teljesítménye és stabilitása szempontjából. A 2008. évi pénzügyi válságot követő reform elsősorban az uniós pénzügyi ágazat pénzügyi rezilienciáját erősítette meg, és arra irányult, hogy megóvja az Unió versenyképességét, valamint gazdasági, prudenciális és a piaci magatartás szempontjából vett stabilitását. Bár az IKT-biztonság és a digitális reziliencia a működési kockázat kezelésének része, a válság utáni szabályozási menetrendben kisebb hangsúlyt kapott, és fejlesztésére az uniós pénzügyi piacot érintő szakpolitikai és szabályozási területek közül csak egyeseken, vagy csak néhány tagállamban került sor.

(6) A Bizottság 2018. évi pénzügyi technológiai cselekvési terve[29] rámutatott annak kiemelkedő fontosságára, hogy az uniós pénzügyi ágazatot működési szempontból is

---

[27] Az ERKT jelentése: „Rendszerszintű kiberkockázat” (2020. február, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf).

[28] Az európai felügyeleti hatóságok felülvizsgálatát kísérő hatásvizsgálat (SWD(2017) 308) szerint a rendszerben mintegy 5 665 hitelintézet, 5 934 befektetési vállalkozás, 2 666 biztosító, 1 573 foglalkoztatói nyugellátást szolgáltató intézmény, 2 500 befektetési alapkezelő, 350 piaci infrastruktúra (központi szerződő fél, értéktőzsde, rendszeres internalizáló, kereskedési adattár és MTF), 45 hitelminősítő intézet, valamint 2 500 engedélyezett pénzforgalmi intézmény és elektronikuspénz-kibocsátó intézmény található. Az összesen mintegy 21 233 szervezet nem foglalja magában a közösségi finanszírozási szervezeteket, a jogszabály szerint engedélyezett könyvvizsgálókat és a könyvvizsgáló társaságokat, a kriptoeszköz-szolgáltatókat és a referenciamutató-kezelőket.

[29] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Központi Banknak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – *Pénzügyi technológiai cselekvési terv: Egy versenyképesebb és innovatívabb európai pénzügyi ágazat felé* (COM(2018) 0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en).

reziliensebbé kell tenni annak érdekében, hogy garantált legyen technológiai biztonsága, megfelelő működése, továbbá IKT-biztonsági sérüléseket és eseményeket követő gyors helyreállítása, ami végső soron lehetővé teszi a pénzügyi szolgáltatások gyors és zökkenőmentes nyújtását az Unió egészében stresszkörülmények között is, ugyanakkor hozzájárul a fogyasztói és piaci bizalom megóvásához.

(7) 2019 áprilisában az Európai Bankhatóság (EBH), az Európai Értékpapírpiaci Hatóság (ESMA) és az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság (EIOPA) (együtt: európai felügyeleti hatóságok vagy EFH-k) két közös szakvéleményt adtak ki, amelyben szorgalmazták a pénzügyi szolgáltatási ágazat IKT-kockázatának koherens megközelítését, továbbá javaslatot tettek az ágazat digitális működési rezilienciájának ágazatspecifikus uniós kezdeményezésen keresztüli arányos megerősítésére.

(8) Az uniós pénzügyi ágazatot harmonizált, egységes szabálykönyv szabályozza a Pénzügyi Felügyeletek Európai Rendszerének irányításával. 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 stabilitáshoz és a piac integritásához, és legalább olyan fontos, mint például a prudenciális vagy a piaci magatartásra vonatkozó általános előírások. Az egységes szabálykönyvet és a felügyeleti rendszert ezért e komponensre is kiterjedően szükséges fejleszteni, a pénzügyi stabilitás és a piaci integritás nyomon követéséért és védelméért felelős pénzügyi felügyeletek szélesebb körű felhatalmazásával.

(9) Az IKT-kockázatokkal kapcsolatos jogalkotási eltérések, valamint a heterogén tagállami szabályozási és felügyeleti megközelítések akadályozzák a pénzügyi szolgáltatások egységes piacát, megnehezítve a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára a letelepedés és a szolgáltatásnyújtás szabadságának zavartalan gyakorlását. Ugyancsak torzulhat a verseny a több tagállamban is tevékenységet folytató, azonos típusú pénzügyi szervezetek között. Különösen azokon a területeken, ahol az uniós harmonizáció csak nagyon korlátozottan (például a digitális működési reziliencia tesztelése tekintetében) vagy egyáltalán nem valósult meg (például a harmadik féltől eredő IKT-kockázat tekintetében), a nemzeti szintű fejlesztési elképzelésekből adódó eltérések további akadályokat képezhetnek az egységes piac működésében, ami a piaci szereplők és a pénzügyi stabilitás szempontjából egyaránt káros.

(10) Az a részlegesség, amellyel az IKT-kockázatra vonatkozó rendelkezések eddigi uniós szintű kezelése történt, lényeges területeken eredményezett hiányosságokat vagy átfedéseket, például az IKT-vonatkozású biztonsági események bejelentése és a digitális működési reziliencia tesztelése terén, emellett következetlenséghez is vezet az egymástól eltérő nemzeti szabályok kialakulása, valamint az egymást átfedő szabályok nem költséghatékony alkalmazása miatt. Ez különösen hátrányosan érinti az olyan IKT-intenzív felhasználókat, mint a pénzügyi ágazat, mivel a technológiai kockázatok nem ismernek határokat, a pénzügyi ágazat pedig az Unión belül és azon kívül egyaránt kiterjedt, határokon átnyúló jelleggel épít ki szolgáltatásokat.

Azok az egyedi pénzügyi szervezetek, amelyek határokon átnyúló tevékenységet végeznek, vagy többféle engedéllyel rendelkeznek (ugyanaz a pénzügyi szervezet bankként, befektetési vállalkozásként és pénzforgalmi intézményként is rendelkezhet engedéllyel, amelyek mindegyikét más illetékes hatóság adja ki egy vagy több tagállamban), működési kihívásokkal szembesülnek az IKT-kockázatok kezelése,

valamint az IKT-vonatkozású biztonsági események káros hatásainak önálló, koherens és költséghatékony enyhítése során.

(11) Mivel az egységes szabálykönyvet nem egészítette ki átfogó IKT- vagy működésikockázat-kezelési keret, a pénzügyi szervezetek teljes körére kiterjedő, digitális működési rezilienciára vonatkozó követelmények további harmonizációjára van szükség. Az üzemszünetek elviselése céljából kifejlesztett képességek és általános reziliencia révén a pénzügyi szervezetek elősegítenék az uniós pénzügyi piacok stabilitásának és integritásának megőrzését, ezáltal pedig hozzájárulnának a befektetők és fogyasztók fokozott védelméhez az Unióban. E rendelet célja, hogy hozzájáruljon a belső piac zavartalan működéséhez, következésképpen az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkén kell alapulnia, az Európai Unió Bíróságának állandó ítélkezési gyakorlatával összhangban.

(12) E rendelet célja, hogy egyesítse és korszerűsítse azokat az IKT-kockázatokra vonatkozó követelményeket, amelyeket eddig a különböző rendeletek és irányelvek elkülönítetten rögzítettek. Bár ezek az uniós jogi aktusok lefedték a pénzügyi kockázat fő kategóriáit (pl. a hitelkockázatot, a piaci kockázatot, a partnerkockázatot, a likviditási kockázatot és a piaci magatartási kockázatot), elfogadásuk időpontjában nem kezelhették átfogóan a digitális működési reziliencia valamennyi összetevőjét. A működési kockázatra vonatkozó követelményeket ezek az uniós jogi aktusok gyakran a kockázatkezelés hagyományos kvantitatív megközelítését előnyben részesítve (nevezetesen az IKT-kockázatok fedezését célzó tőkekövetelmény előírásával) fejlesztették tovább ahelyett, hogy célzott kvalitatív követelményeket fogalmaztak volna meg, amelyek az IKT-vonatkozású biztonsági eseményekhez kapcsolódó védelmi, észlelési, elszigetelési és helyreállítási képességekre vonatkozó követelmények előírásával, vagy a bejelentési és digitális tesztelési képességek rögzítésével növelnék a szervezetek képességeit. Ezeknek az irányelveknek és rendeleteknek az elsődleges célja a prudenciális felügyeletre, a piaci integritásra és a piaci magatartásra vonatkozó szabályok meghatározása volt.

A mostani művelet, amely egyesíti és aktualizálja az IKT-kockázatra vonatkozó szabályokat, első ízben foglalná következetes módon egyetlen jogalkotási aktusba a pénzügyi szolgáltatásokban rejlő digitális kockázatokra vonatkozó valamennyi rendelkezést. Rendeltetése szerint tehát ez a kezdeményezés pótolja az egyes jogi aktusok hiányosságait, illetve orvosolja következetlenségeiket többek között az alkalmazott terminológia kapcsán, emellett az IKT-kockázatkezelési képességekre, a bejelentésre, a tesztelésre és a harmadik féltől eredő kockázatok nyomon követésére vonatkozó célzott szabályok formájában kifejezetten említi az IKT-kockázatot.

(13) A pénzügyi szervezeteknek az IKT-kockázat kezelésekor ugyanezt a megközelítést és ugyanazokat az elvalapú szabályokat kell alkalmazniuk. A következetesség hozzájárul a pénzügyi rendszerrel szembeni bizalom erősítéséhez és a rendszer stabilitásának megőrzéséhez, különösen az IKT-rendszerek, -platformok és -infrastruktúrák túlzott igénybevétele esetén, amely fokozott digitális kockázattal jár.

Az alapvető kiberhigiénia betartásával egyidejűleg – az IKT-zavarok hatásának és költségeinek minimalizálása révén – elkerülhetők a súlyos gazdasági áldozatok is.

(14) Rendelet útján csökkenthető a szabályozás összetettsége, elősegíthető a felügyeleti konvergencia és növelhető a jogbiztonság, emellett az hozzájárul a megfelelési költségek csökkentéséhez – különösen a határokon átnyúló tevékenységet végző pénzügyi szervezetek esetében –, és a versenytorzulások mérsékléséhez. Az előzőek alapján a pénzügyi szervezetek digitális működési rezilienciájára vonatkozó közös

keret létrehozása céljából a leginkább megfelelő eszköznek a rendelet tekinthető, amellyel garantálható, hogy az uniós pénzügyi ágazatok egységesen és koherensen alkalmazzák az IKT-kockázatkezelés valamennyi összetevőjét.

(15) A pénzügyi szolgáltatásokra vonatkozó jogszabályok mellett jelenleg az (EU) 2016/1148 európai parlamenti és tanácsi irányelv[30] alkotja a kiberbiztonság általános uniós szintű keretét. A hét kulcsfontosságú ágazat között az említett irányelv a pénzügyi szervezetek három típusára, nevezetesen a hitelintézetekre, a kereskedési helyszínekre, valamint a központi szerződő felekre is vonatkozik. Mivel azonban az (EU) 2016/1148 irányelv nemzeti szintű mechanizmust határoz meg az alapvető szolgáltatásokat nyújtó szereplők azonosítására, hatálya a gyakorlatban csak a tagállamok által azonosított egyes hitelintézetekre, kereskedési helyszínekre és központi szerződő felekre terjed ki, ennélfogva az irányelvben az IKT-biztonságra és a biztonsági események bejelentésére vonatkozóan előírt követelményeknek is csak ezek a szervezetek kötelesek megfelelni.

(16) Ez a rendelet a digitális reziliencia összetevői kapcsán fokozza a harmonizáció mértékét azáltal, hogy az IKT-kockázatok kezelése és az IKT-vonatkozású biztonsági események bejelentése tekintetében a pénzügyi szolgáltatásokra vonatkozó jelenlegi uniós jogszabályokban foglaltakhoz képest szigorúbb kötelezettségeket vezet be, ami az (EU) 2016/1148 irányelvben foglalt követelményekhez képest is nagyobb fokú harmonizációt jelent. Következésképpen ez a rendelet az (EU) 2016/1148 irányelvhez kapcsolódó különös szabályt alkot.

Alapvető fontosságú a pénzügyi ágazatnak az uniós horizontális kiberbiztonsági kerettel meglévő erős kapcsolata fenntartásához, ami biztosítaná a tagállamok által már elfogadott kiberbiztonsági stratégiákkal való egységet, emellett lehetővé tenné a pénzügyi felügyeletek számára, hogy értesüljenek az (EU) 2016/1148 irányelv hatálya alá tartozó egyéb ágazatokat érintő kiberbiztonsági eseményekről.

(17) Annak érdekében, hogy ágazatközi tanulási folyamat jöhessen létre, amelyben eredményesen felhasználhatók más ágazatok tapasztalatai a kiberfenyegetettségek kezelésében, fontos, hogy az (EU) 2016/1148 irányelvben említett pénzügyi szervezetek továbbra is az irányelv „ökoszisztémájához” tartozzanak (pl. a Kiberbiztonsági Együttműködési Csoport és a számítógép-biztonsági eseményekre reagáló csoportok keretében).

Az EFH-knak, illetve az illetékes nemzeti hatóságoknak részvételi lehetőséget kell kapniuk a szakpolitikai jellegű stratégiai egyeztetésekben, illetve a Kiberbiztonsági Együttműködési Csoport technikai tevékenységében, emellett információkat kell cserélniük és együtt kell működniük az (EU) 2016/1148 irányelv szerint kijelölt egyedüli kapcsolattartó pontokkal. Az e rendelet szerinti illetékes hatóságoknak ezenkívül egyeztetniük kell és együtt kell működniük a tagállamok számítógép-biztonsági eseményekre reagáló csoportjaival, amelyek kijelölése az (EU) 2016/1148 irányelv 9. cikkével összhangban történik.

(18) Emellett biztosítani kell az összhangot az európai kritikus infrastruktúrákról szóló irányelvvel, amelynek folyamatban lévő felülvizsgálata erősíteni kívánja a kritikus

[30] 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.).

infrastruktúrák védelmét és rezilienciáját a kibertéren kívül megjelenő fenyegetésekkel szemben, ami a pénzügyi ágazatot is érintheti.[31]

(19) A felhőszolgáltatók az (EU) 2016/1148 irányelv hatálya alá tartozó digitális szolgáltatók egyik kategóriáját alkotják. Ennélfogva kiterjed rájuk az említett irányelvnek megfelelően kijelölt nemzeti hatóságok által végzett utólagos felügyeleti ellenőrzés, amely viszont az irányelvben az IKT-biztonságra és a biztonsági események bejelentésére vonatkozóan meghatározott követelményekre korlátozódik. Mivel az e rendeletben meghatározott felvigyázási keret a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók mindegyikére, így a pénzügyi szervezetek részére nyújtott IKT-szolgáltatások kapcsán a felhőszolgáltatókra is kiterjed, a felvigyázást az (EU) 2016/1148 irányelv alapján végzett felügyelet kiegészítésének kell tekinteni. Emellett egy digitális felügyeleti hatóságot létrehozó horizontális, ágazatközi uniós keret hiányában az e rendeletben meghatározott felvigyázási keretnek ki kell terjednie a felhőszolgáltatókra is.

(20) Az IKT-kockázatok feletti teljes kontroll megőrzéséhez a pénzügyi szervezeteknek rendelkezniük kell az erőteljes és eredményes IKT-kockázatkezelést megalapozó átfogó képességekkel, továbbá az IKT-vonatkozású biztonsági események bejelentésére, az IKT-rendszerek, -kontrollok és -folyamatok tesztelésére, valamint a harmadik féltől eredő IKT-kockázat kezelésére vonatkozó konkrét mechanizmusokkal és politikákkal. A digitális működési reziliencia tekintetében emelni kell a mércét a pénzügyi rendszerben, ugyanakkor a 2003/361/EK bizottsági ajánlás[32] meghatározása szerint mikrovállalkozásnak minősülő pénzügyi szervezetek számára lehetővé kell tenni a követelmények arányos alkalmazását.

(21) Az IKT-vonatkozású biztonsági események bejelentésének küszöbértékei és taxonómiái tagállamonként jelentősen eltérnek. Bár az Európai Uniós Kiberbiztonsági Ügynökség (ENISA)[33] és a pénzügyi szervezetek (EU) 2016/1148 irányelv szerinti együttműködési csoportjának releváns munkája közös alapokat teremthet, a küszöbértékek és taxonómiák kapcsán a többi pénzügyi szervezet tekintetében továbbra is maradhatnak, illetve megjelenhetnek tagállamonként eltérő megközelítések. Emiatt a pénzügyi szervezeteknek többszörös követelményeket kell teljesíteniük, különösen akkor, ha az Unión belül több joghatósági területen, vagy pénzügyi csoport tagjaként folytatnak tevékenységet. Ezek az eltérések ráadásul akadályozhatják azoknak a további uniós szinten egységesített vagy központosított mechanizmusoknak a létrehozását, amelyek gyorsítanák a bejelentési folyamatot és támogatnák az illetékes hatóságok közötti gyors és zavartalan információcserét, ami elengedhetetlen az IKT-kockázatok kezeléséhez a kiterjedt, potenciálisan rendszerszintű következményekkel járó támadások esetén.

(22) Ahhoz, hogy az illetékes hatóságok az IKT-vonatkozású biztonsági események jellegével, gyakoriságával, jelentőségével és hatásával kapcsolatban szerzett átfogó ismereteikre támaszkodva elláthassák felügyeleti feladataikat, továbbá az érintett

---

31 A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (HL L 345., 2008.12.23., 75. o.).

32 A Bizottság ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

33 ENISA eseményosztályozási referenciataxonómia (https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy).

hatóságok, ezen belül a bűnüldöző hatóságok és a szanálási hatóságok közötti kiterjedtebb információcsere érdekében szabályokat szükséges rögzíteni, amelyek az IKT-vonatkozású biztonsági események bejelentési rendszerét kiegészítik a pénzügyi szolgáltatási alágazatra vonatkozó jogszabályokból jelenleg hiányzó követelményekkel, továbbá a költségek mérséklése érdekében megszüntetik a fennálló átfedéseket és párhuzamosságokat. Ehhez elengedhetetlen az IKT-vonatkozású biztonsági események bejelentési rendszerének harmonizálása úgy, hogy minden pénzügyi szervezetnek csak a saját illetékes hatósága felé legyen bejelentési kötelezettsége. Ezenkívül az EFH-knak felhatalmazást kell kapniuk arra, hogy részletesebben meghatározzák az IKT-vonatkozású biztonsági események bejelentésének elemeit, köztük a taxonómiákat, az időkereteket, az adatállományokat, a mintadokumentumokat, valamint az alkalmazandó küszöbértékeket.

(23) Egyes pénzügyi szolgáltatási alágazatokban kidolgoztak ugyan a digitális működési reziliencia tesztelésére vonatkozó követelményeket, erre azonban több össze nem hangolt, nemzeti rendszer keretében, ugyanazon problémák eltérő kezelésével került sor. Ez a határokon átnyúló tevékenységet végző pénzügyi szervezetek számára költséghalmozódáshoz vezet, emellett megnehezíti az eredmények kölcsönös elismerését is. Az össze nem hangolt tesztelés ezért az egységes piac széttagolódásával járhat.

(24) Emellett kötelező tesztelés hiányában a sebezhetőségek észlelésére sem kerül sor, ami fokozott kockázatnak teszi ki az adott pénzügyi szervezetet, végső soron pedig a pénzügyi ágazat stabilitását és integritását. Uniós beavatkozás nélkül a digitális működési reziliencia tesztelése továbbra sem lenne egységes, és a teszteredmények különböző joghatósági területek közötti kölcsönös elismerése sem valósulna meg. Emellett mivel valószínűleg más pénzügyi szolgáltatási alágazatok nem vezetnének be ilyen rendszereket érdemi nagyságrendben, nem használhatnák ki azok potenciális előnyeit, többek között a sebezhetőségek és kockázatok feltárását, a védelmi képességek és az üzletmenet-folytonosság tesztelését, továbbá az ügyfelek, beszállítók és üzleti partnerek nagyobb bizalmát sem. Az ilyen átfedések, eltérések és hiányosságok kiküszöbölése céljából a pénzügyi szervezetek és az illetékes hatóságok által végzendő összehangolt tesztelésre vonatkozó szabályokat kell meghatározni, amelyek megkönnyítenék a fejlett tesztmódszerek kölcsönös elismerését a jelentős pénzügyi szervezetek számára.

(25) 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; csökkentette a pénzügyi közvetítés költségeit, lehetővé tette az üzleti tevékenység bővítését és skálázhatóságát a pénzügyi tevékenységek kiépítése során, ugyanakkor IKT-eszközök széles körét is hozzáférhetővé tette az összetett belső folyamatok kezeléséhez.

(26) Az IKT-szolgáltatások kiterjedt felhasználását bizonyítják azok az összetett szerződéses megállapodások is, amelyeknél a pénzügyi szervezetek gyakran szembesülnek nehézségekkel a rájuk vonatkozó prudenciális előírásokhoz vagy egyéb szabályozási követelményekhez igazodó szerződési feltételek kieszközlésében, valamint meghatározott (hozzáférési, ellenőrzési) jogok érvényesítése kapcsán, ha ez utóbbiakat a megállapodás rögzíti. Ráadásul az ilyen szerződések sok esetben nem nyújtanak elegendő biztosítékot az alvállalkozói folyamatok teljes körű nyomon követésére, ezáltal ellehetetlenítik a pénzügyi szervezet számára az e folyamatokkal

összefüggő kockázatok értékelését. Ezenkívül mivel a harmadik félnek minősülő IKT-szolgáltatók gyakran nyújtanak szabványosított szolgáltatásokat különböző típusú ügyfeleknek, az ilyen szerződések nem feltétlenül felelnek meg a pénzügyi szolgáltatási ágazat szereplői által támasztott egyedi vagy sajátos igényeknek.

(27) A pénzügyi szolgáltatásokra vonatkozó egyes uniós jogszabályokban megtalálható néhány kiszervezési szabálytól eltekintve a szerződéses dimenzió nyomon követése nem épült be szervesen az uniós jogszabályokba. A harmadik félnek minősülő IKT-szolgáltatókkal kötött szerződéses megállapodásokra vonatkozó egyértelmű és célzott uniós előírások hiányában az IKT-kockázat külső forrásainak átfogó feltárása sem valósulhat meg. Emiatt szükséges néhány, a pénzügyi szervezetek harmadik féltől eredő IKT-kockázatának kezelésére irányadó alapelvet rögzíteni, azokat a szerződések teljesítésének és megszüntetésének számos elemével kapcsolatban egy sor alapvető szerződéses joggal kiegészítve bizonyos minimális biztosítékok rögzítése érdekében, amelyek alapján a pénzügyi szervezetek eredményesen nyomon követhetik a harmadik félnek minősülő IKT-szolgáltatók szintjén felmerülő kockázatok teljes körét.

(28) A harmadik féltől eredő IKT-kockázat és a harmadik féltől való IKT-függőség tekintetében hiányzik a homogenitás és a konvergencia. A kiszervezés konkrét területének kezelésére irányuló egyes erőfeszítéseket – köztük a felhőszolgáltatókhoz történő kiszervezésről szóló 2017. évi ajánlásokat[34] – leszámítva az uniós jogszabályok alig foglalkoznak a pénzügyi ágazat harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók szűk körével szembeni kitettsége miatt esetlegesen felmerülő rendszerszintű kockázat kérdésével. Ezt az uniós szintű hiányosságot súlyosbítja, hogy a nemzeti felügyeletek nem rendelkeznek konkrét felhatalmazással arra, illetve eszközökkel ahhoz, hogy behatóan megismerhessék a harmadik féltől való IKT-függőségeket, és megfelelően nyomon követhessék az ilyen függőségek koncentrációjából eredő kockázatokat.

(29) Figyelembe véve a kiszervezés egyre elterjedtebb gyakorlatával és a harmadik félnek minősülő IKT-szolgáltatók koncentrációjával járó potenciális rendszerszintű kockázatokat, továbbá szem előtt tartva az olyan nemzeti mechanizmusok elégtelenségét, amelyek lehetővé tennék a pénzügyi felügyeletek számára a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóknál felmerülő IKT-kockázatok mennyiségi és minőségi értékelését, valamint hatásaik elhárítását, megfelelő uniós felvigyázási keretet szükséges létrehozni, amelyben folyamatosan nyomon követhető azoknak a harmadik félnek minősülő IKT-szolgáltatóknak a tevékenysége, amelyek pénzügyi szervezetek részére nyújtanak kulcsfontosságú szolgáltatásokat.

(30) Minél összetettebbé és fejlettebbé válnak az IKT-fenyegetések, az észlelési és megelőző intézkedések eredményessége annál nagyobb mértékben függ a fenyegetettségi és sebezhetőségi információk pénzügyi szervezetek közötti rendszeres megosztásától. Az információk megosztása hozzájárul a kiberfenyegetések fokozott tudatosításához, ez pedig javítja a pénzügyi szervezetek képességét annak megelőzésére, hogy a fenyegetések valóban bekövetkezzenek, emellett lehetővé teszi a pénzügyi szervezetek számára az IKT-vonatkozású biztonsági események hatásainak eredményesebb elszigetelését, továbbá a hatékonyabb helyreállítást. Uniós szintű iránymutatás hiányában az eddigiek során a jelek szerint több tényező is gátolta az értesülések megosztását, különösen az adatvédelmi, trösztellenes és felelősségi szabályokkal való összeegyeztethetőséggel kapcsolatos bizonytalanság.

[34] Ajánlások a felhőszolgáltatókhoz történő kiszervezésről (EBA/REC/2017/03), ezek helyébe utóbb az EBH a felhőszolgáltatókhoz történő kiszervezésre vonatkozó iránymutatásai léptek (EBA/GL/2019/02).

(31) A hasznos információk visszatartásához vezet az azzal kapcsolatos határozatlanság is, hogy milyen típusú információk adhatók át más piaci szereplők, illetve nem felügyeleti hatóságok (pl. elemzési célból az ENISA, bűnüldözési célból az Europol) részére. Az információmegosztás terjedelmében és minőségében továbbra is korlátozott, széttagolt; a releváns információk átadására többnyire helyi szinten (tagállami kezdeményezések keretében) kerül sor, az integrált pénzügyi ágazat igényeihez igazodó, egységes uniós szintű információmegosztási megállapodások pedig nincsenek.

(32) A pénzügyi szervezeteket ezért ösztönözni kell arra, 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, valamint elhárítására. Ezért lehetővé kell tenni az önkéntes információmegosztásra vonatkozó megállapodások uniós mechanizmusainak kialakulását, mivel a megbízható környezetben átadott információk segítségével a pénzügyi közösség megelőzhetné a fenyegetéseket és együttesen háríthatná el azokat az IKT-kockázatok terjedésének gyors lehatárolásával, valamint a pénzügyi csatornákon keresztüli esetleges átterjedés megakadályozásával. E mechanizmusokat a vonatkozó uniós versenyjogi szabályok[35], valamint az uniós adatvédelmi szabályok, elsősorban az (EU) 2016/679 európai parlamenti és tanácsi rendelet[36] maradéktalan betartásával kell működtetni, különösen a személyes adatok olyan kezelésével összefüggésben, amelyre az említett rendelet 6. cikke (1) bekezdésének f) pontja szerint az adatkezelő vagy valamely harmadik fél jogos érdekének érvényesítéséhez van szükség.

(33) Az e rendeletben meghatározott kiterjedt hatály ellenére a digitális működési rezilienciára vonatkozó szabályok alkalmazásakor figyelembe kell venni a pénzügyi szervezetek között méret, üzleti profil és digitális kockázati kitettség tekintetében meglévő jelentős különbségeket. Általános elvként az IKT-kockázatkezelési keretrendszer végrehajtására fordítandó erőforrások és képességek meghatározásakor pénzügyi szervezeteknek megfelelő egyensúlyt kell teremteniük IKT-szükségleteik, valamint méretük és üzleti profiljuk között, míg az illetékes hatóságok részéről a felosztási megközelítés folyamatos ellenőrzése és felülvizsgálata szükséges.

(34) 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 célszerű kötelezővé tenni az összetettebb irányítási rendszerek kidolgozását. Az ilyen szervezeteknek jobb eszközeik vannak főként arra, hogy külön vezetői funkciókat alakítsanak ki a harmadik félnek minősülő IKT-szolgáltatókkal kötött megállapodások felügyelete, illetve válságkezelés céljából, a három védelmi vonalra épülő modellnek megfelelően szervezzék IKT-kockázatkezelésüket, vagy olyan emberierőforrás-gazdálkodási dokumentumot fogadjanak el, amely átfogóan ismerteti a hozzáférési jogosultságok szabályait.

---

35 A Bizottság közleménye – Iránymutatás az Európai Unió működéséről szóló szerződés 101. cikkének a horizontális együttműködési megállapodásokra való alkalmazhatóságáról (HL C 11., 2011.1.14., 1. o.).

36 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.).

Ugyanígy csak e pénzügyi szervezetek számára célszerű kötelezővé tenni, hogy a hálózati és információs rendszerek infrastruktúrájának és folyamatainak jelentősebb változásait követően beható vizsgálatokat végezzenek, rendszeresen elvégezzék az örökölt IKT-rendszerek kockázatelemzését, továbbá az üzletmenet-folytonossági, elhárítási és helyreállítási tervek tesztelését kiterjesszék az elsődleges IKT-infrastruktúrájuk és a tartalékeszközök közötti átállásra.

(35) Ezenfelül mivel a fenyegetettségi szempontú behatolási tesztelést csak az olyan pénzügyi szervezetek számára célszerű kötelezővé tenni, amelyek a digitális működési reziliencia fejlett módszerekkel végzett tesztelése szempontjából jelentősnek minősülnek, indokolt, hogy az ilyen tesztek végrehajtásával járó igazgatási folyamatok és pénzügyi költségek terhét is a pénzügyi szervezetek kis hányada viselje. Végül pedig a szabályozásból eredő terhek enyhítése érdekében csak a mikrovállalkozásnak nem minősülő pénzügyi szervezetektől várható el, hogy rendszeresen beszámoljanak az illetékes hatóságoknak az IKT-zavarokból eredő költségeikről és veszteségeikről, valamint a jelentős IKT-vonatkozású biztonsági eseményeket követő felülvizsgálatok eredményeiről.

(36) A pénzügyi szervezeteknél egyfelől az üzleti stratégiák, másfelől pedig az IKT-kockázatkezelés teljes körű összehangolása és általános összhangja érdekében a vezető testület számára elő kell írni, hogy vállaljon központi és tevékeny szerepet az IKT-kockázatkezelési keretrendszer, valamint a digitális rezilienciára vonatkozó átfogó stratégia irányításában és alakításában. A vezető testület által alkalmazandó megközelítésnek nem elegendő az IKT-rendszerek rezilienciáját biztosító eszközökre összpontosítania: ki kell terjednie a személyekre és a folyamatokra is olyan szabályzatok útján, amelyek a vállalati struktúra minden rétegében, a teljes személyi állományra vonatkozóan hangsúlyozzák a kiberkockázatok tudatosítását és a szigorú kiberhigiéniás normák betartása melletti elkötelezettséget.

A pénzügyi szervezet IKT-kockázatának kezeléséért a vezető testületet terhelő teljes körű felelősség általános elv, amelyet az IKT-kockázatkezelés nyomon követésének kontrolljában való folyamatos vezető testületi részvétel formájában kell érvényesíteni.

(37) Ezenfelül a vezető testület teljes elszámoltathatósága együtt jár az IKT-beruházások és az általános IKT-költségvetés olyan szinten történő megállapításával, amelyen a pénzügyi szervezet teljesítheti a digitális működési reziliencia alapértékeit.

(38) A vonatkozó nemzetközi, nemzeti és ágazati standardok, iránymutatások és ajánlások, valamint kiberkockázat-kezelési megközelítések[37] nyomán kidolgozott rendelet olyan IKT-kockázatkezelési funkciókat mozdít elő, amelyek megkönnyítik az IKT-kockázatkezelés általános strukturálását. A pénzügyi szervezetek szabadon alkalmazhatnak eltérő keretek között, illetve kategóriák mentén kidolgozott IKT-kockázatkezelési modelleket mindaddig, amíg az egyes szervezeteknél meglévő fő képességek megfelelnek az e rendeletben meghatározott funkciók (azonosítás, védelem és megelőzés, felderítés, elhárítás és helyreállítás, tanulás és alkalmazkodás, kommunikáció) célkitűzéseihez kapcsolódó szükségleteknek.

---

[37] CPMI-IOSCO: *Iránymutatás a pénzügyi piaci infrastruktúrák kiberrezilienciájáról* (https://www.bis.org/cpmi/publ/d146.pdf); G7: *A pénzügyi ágazat kiberbiztonságának alapelemei* (https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf); NIST: Kiberbiztonsági keret (https://www.nist.gov/cyberframework); FSB: *CIRR-eszköztár* (https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document).

(39) Ahhoz, hogy lépést tarthassanak a kiberfenyegetettségi helyzet alakulásával, a pénzügyi szervezeteknek naprakész IKT-rendszereket kell fenntartaniuk, amelyek megbízhatóságuk és kapacitásuk révén nemcsak a szervezetek szolgáltatásainak nyújtásához szükséges adatfeldolgozást teszik lehetővé, hanem biztosítják azt a technológiai rezilienciát is, amelyre támaszkodva a pénzügyi szervezetek elláthatják a piaci stresszhelyzet vagy egyéb hátrányos helyzet miatti fokozott adatfeldolgozási igényeket is. Maga a rendelet nem standardizál konkrét IKT-rendszereket, -eszközöket vagy -technológiákat, ugyanakkor épít arra, hogy a pénzügyi szervezetek felhasználják az európai és nemzetközileg elismert technikai szabványokat (pl. ISO) és ágazati bevált módszereket, amennyiben ez teljes mértékben megfelel a nemzetközi szabványok felhasználására vonatkozó konkrét felügyeleti utasításoknak.

(40) Hatékony üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervekre van szükség, hogy a pénzügyi szervezetek az IKT-vonatkozású biztonsági eseményeket, különösen a kibertámadásokat haladéktalanul és gyorsan, a kár mérséklésével, a tevékenység újraindítását és a helyreállítási intézkedéseket előtérbe helyezve oldhassák meg. A készenléti rendszereknek azonnal meg kell kezdeniük az adatfeldolgozást, ugyanakkor az átállás nem veszélyeztetheti sem a hálózati és információs rendszerek integritását és biztonságát, sem a bizalmas adatok védelmét.

(41) Ez a rendelet lehetővé teszi a pénzügyi szervezetek számára, hogy a helyreállítási időre vonatkozó célkitűzéseket rugalmasan, az adott funkció jellegének és kritikus mivoltának, valamint a vonatkozó üzleti igényeknek a maradéktalan figyelembevételével határozzák meg, ugyanakkor a célkitűzések meghatározása kapcsán a piaci hatékonyságot potenciálisan érő általános hatás értékelését is elő kell írni.

(42) A kibertámadások jelentős következményei felerősödnek, ha az esemény a pénzügyi ágazatban fordul elő, ahol sokkal nagyobb a kockázata annak, hogy a közvetlenül a forrásoldalon anyagi haszonszerzésre törekvő rosszindulatú terjesztők célpontjává válik. Az ilyen jellegű kockázatok mérséklése, továbbá annak megelőzése érdekében, hogy az IKT-rendszerek elveszítsék integritásukat vagy elérhetetlenné váljanak, a bizalmas adatok védelme sérüljön, vagy fizikai IKT-infrastruktúrában kár keletkezzen, számottevő mértékben javítani szükséges a jelentős IKT-vonatkozású biztonsági események pénzügyi szervezetek általi bejelentését.

Az IKT-vonatkozású biztonsági események bejelentését harmonizálni kell úgy, hogy minden pénzügyi szervezetnek csak a saját illetékes hatósága felé legyen bejelentési kötelezettsége. A bejelentési kötelezettség minden pénzügyi szervezetre kiterjedne, de nem érintheti őket azonos módon, mivel a vonatkozó lényegességi küszöbértékeket és időbeli kereteket úgy kell kalibrálni, hogy csak a jelentős IKT-vonatkozású biztonsági eseményeket szűrjék ki. A közvetlen bejelentés a pénzügyi felügyeletek számára hozzáférhetővé tenné az IKT-vonatkozású biztonsági eseményekkel kapcsolatos információkat. Ennek ellenére a pénzügyi felügyeleteknek át kell adniuk ezeket az információkat nem pénzügyi hatóságok (kiberbiztonsági illetékes hatóságok, nemzeti adatvédelmi hatóságok, bűncselekmény jellegű események kapcsán a bűnüldöző hatóságok) részére is. Az IKT-vonatkozású biztonsági 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 az adott eseményhez kapcsolódó fenyegetésekre és sebezhetőségekre vonatkozó anonimizált adatokat is meg kell osztaniuk.

(43) Részletesebben vizsgálni kell az IKT-vonatkozású biztonsági események bejelentésének egységes uniós központi adatbázis útján történő esetleges központosítását, amely közvetlenül fogadná a vonatkozó bejelentéseket és automatikusan értesítené az illetékes nemzeti hatóságokat, vagy az illetékes nemzeti hatóságok által továbbított bejelentések központosításával mindössze koordinációs szerepet látna el. Elő kell írni az EFH-k számára, hogy az EKB-val és az ENISA-val folytatott konzultációt követően, meghatározott határidőn belül készítsenek közös jelentést az uniós központi adatbázis létrehozásának megvalósíthatóságáról.

(44) Az erős digitális működési reziliencia megvalósításához, valamint a nemzetközi szabványokkal (pl. G7: A fenyegetettségi szempontú behatolási tesztelés alapelemei) összhangban a pénzügyi szervezeteknek a megelőzési, felderítési, elhárítási és helyreállítási képességek tekintetében rendszeresen tesztelniük kell IKT-rendszereiket és -munkatársaikat, hogy feltárhassák és kezelhessék az esetleges IKT-sebezhetőségeket. A pénzügyi szolgáltatási alágazatok között és azokon belül az egyes pénzügyi szervezetek kiberbiztonsági felkészültségében meglévő különbségek megszüntetése érdekében a tesztelésnek az eszközök és műveletek széles skáláját kell magában foglalnia az alapvető követelmények felmérésétől (sebezhetőségi értékelések és vizsgálatok, nyílt forrású elemzések, hálózatbiztonsági értékelések, hiányelemzések, fizikai biztonsági felülvizsgálatok, kérdőívek, szoftveres megoldások vizsgálata, lehetőség szerint forráskódvizsgálatok, forgatókönyv-alapú tesztek, kompatibilitásvizsgálat, teljesítményvizsgálat vagy végpontok közötti tesztek) a fejlettebb tesztelési módszerekig (fenyegetettségi szempontú behatolási teszt azon pénzügyi szervezetek esetében, amelyek IKT szempontból kellően érettek ahhoz, hogy képesek legyenek ilyen teszteket végezni). A digitális működési reziliencia tesztelésének tehát a jelentős pénzügyi szervezeteket (nagy hitelintézeteket, értéktőzsdéket, központi értéktárakat, központi szerződő feleket stb.) kell nehezebb feladat elé állítania. A digitális működési reziliencia tesztelése ugyanakkor várhatóan egyes alapvető, rendszerszintű szerepet betöltő alágazatok (pénzforgalom, banki tevékenység, elszámolás és kiegyenlítés) esetében nagyobb, míg más alágazatok (eszközkezelők, hitelminősítő intézetek stb.) esetében kisebb relevanciával bír majd. A határokon átnyúló tevékenységet végző, az Unióban a letelepedés és a szolgáltatásnyújtás szabadságát gyakorló pénzügyi szervezetek számára az egységes fejlett tesztelési követelményrendszer (pl. TLPT) saját tagállamukban való teljesítését kell előírni, a tesztnek pedig ki kell terjednie a határokon átnyúló tevékenységű csoport tevékenységével érintett valamennyi joghatósági területen működő minden IKT-infrastruktúrára annak érdekében, hogy az ilyen csoportoknak csak egy joghatósági területen merüljenek fel tesztköltségei.

(45) A harmadik féltől eredő IKT-kockázat megbízható nyomon követése érdekében szükséges a pénzügyi szervezeteknél a harmadik félnek minősülő IKT-szolgáltatókhoz kiszervezett funkciókkal, általánosabban pedig a harmadik féltől való IKT-függőséggel összefüggésben felmerülő kockázatok nyomon követésére irányadó elvalapú szabályokat rögzíteni.

(46) A pénzügyi szervezetnek mindenkor teljes felelősséggel kell tartoznia az e rendeletben előírt kötelezettségekért. A harmadik félnek minősülő IKT-szolgáltató szintjén felmerülő kockázat arányos nyomon követését az IKT-vonatkozású függőségek nagyságrendjének, összetettségének és jelentőségének, továbbá a szerződéses megállapodás tárgyát képező szolgáltatások, folyamatok, funkciók kritikus mivoltának, lényegességének kellő figyelembevételével, végső soron pedig a pénzügyi

szolgáltatások folytonosságát és minőségét az egyedi szervezet, illetve a csoport szintjén esetlegesen érő hatások körültekintő értékelése alapján kell megszervezni.

(47) A nyomon követés során a harmadik féltől eredő IKT-kockázattal kapcsolatban a pénzügyi szervezet vezető testülete által külön e célból elfogadott stratégiaként formalizált stratégiai megközelítést kell alkalmazni, amely a harmadik féltől való IKT-függőségek folyamatos és teljes körű szűrésén alapul. A harmadik féltől való IKT-függőségek fokozottabb felügyeleti tudatosítása, valamint az e rendelettel létrehozott felvigyázási keret további támogatása érdekében a pénzügyi felügyeleteknek a nyilvántartásból rendszeresen meg kell kapniuk az alapvető információkat, amelyek eseti lekérdezését is lehetővé kell tenni a számukra.

(48) A szerződéses megállapodások formális megkötését beható elemzésnek kell megelőznie és megalapoznia, a felmondási okok között pedig szerepeltetni kell legalább egyes olyan körülményeket, amikor a harmadik félnek minősülő IKT-szolgáltatónál hiányosságok állapíthatók meg.

(49) A harmadik félnek minősülő IKT-szolgáltatók koncentrációjával járó kockázat kezelése kiegyensúlyozott megoldást igényel, amelynek kapcsán rugalmas és fokozatos megközelítést kell előmozdítani, mivel a merev értékhatárok és a szigorú korlátozások egyaránt akadályozhatják az üzletvitelt és a szerződési szabadságot. Azt, hogy mekkora valószínűséggel merülhet fel ilyen kockázat, a pénzügyi szervezeteknek a szerződéses megállapodásaik alapos értékelésével meg kell határozniuk, többek között a további szinteken kiszervezett tevékenységekről szóló megállapodások beható elemzésével, különösen akkor, ha azokat harmadik országban letelepedett, harmadik félnek minősülő 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 értékhatárokat és limiteket meghatározni. Az egyes harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázására kijelölt EFH-nak („vezető felvigyázó”) a felvigyázási feladatok ellátása során különös figyelmet kell fordítania a kölcsönös függések teljes körű meghatározására, valamint az olyan konkrét esetek feltárására, ahol a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók Unión belüli magas koncentrációja valószínűleg megterheli az uniós pénzügyi rendszer stabilitását és integritását, és e kockázat megállapítása esetén gondoskodnia kell a párbeszédről a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókkal.[38]

(50) Annak érdekében, hogy rendszeresen értékelhető és nyomon követhető legyen a harmadik félnek minősülő IKT-szolgáltató képessége arra, hogy a pénzügyi szervezet részére annak rezilienciáját érő káros hatások nélkül, biztonságosan nyújtson szolgáltatásokat, a harmadik félnek minősülő IKT-szolgáltatókkal kötött szerződések alapelemeit a teljesítés egészére kiterjedően harmonizálni szükséges. Ezek az elemek csak az ahhoz minimálisan szükségesnek tekinthető szerződéses szempontokat foglalják magukban, hogy a pénzügyi szervezet teljeskörűen nyomon követhesse az IKT-szolgáltatás stabilitására és biztonságára épülő digitális rezilienciáját.

(51) A szerződéses megállapodásoknak pontosan meg kell határozniuk különösen a funkciók és szolgáltatások teljes körű leírását, a funkciók teljesítésének és az adatkezelésnek a helyszíneit, valamint a szolgáltatási szintek teljes körű leírását

[38] Ezenkívül ha felmerül a kockázat, hogy egy erőfölénnyel rendelkező harmadik félnek minősülő IKT-szolgáltató visszaélést követhet el, a pénzügyi szervezeteknek lehetőséget kell kapniuk arra, hogy formális vagy informális panaszt nyújtsanak be az Európai Bizottsághoz vagy a nemzeti versenyjogi hatóságokhoz.

azokkal az egyes szolgáltatási szinteken belüli mennyiségi és minőségi célértékekkel együtt, amelyek alapján a pénzügyi szervezet eredményesen nyomon követheti a teljesítést. A személyes adatok hozzáférhetőségére, rendelkezésre állására, integritására, biztonságára és védelmére vonatkozó rendelkezéseket, valamint a harmadik félnek minősülő IKT-szolgáltató fizetésképtelensége, szanálása, üzleti tevékenységének megszűnése esetére vonatkozó hozzáférési, visszaszerzési és visszaszolgáltatási garanciákat ugyancsak olyan szerződéses alapelemnek kell tekinteni, amelyek lehetővé teszik a pénzügyi szervezet számára a harmadik féltől eredő kockázat nyomon követését.

(52) Ahhoz, hogy a pénzügyi szervezetek megőrizhessék a teljes kontrollt az IKT-biztonságukra potenciálisan ártalmas fejlemények felett, rögzíteni szükséges a harmadik félnek minősülő IKT-szolgáltatóra vonatkozó felmondási időket és beszámolási kötelezettségeket az olyan fejlemények esetére, amelyek jelentős hatást gyakorolhatnak a harmadik félnek minősülő IKT-szolgáltató azon képességére, hogy eredményesen ellássa kulcsfontosságú vagy lényeges funkcióit, ezen belül többletköltség nélkül vagy előzetesen megállapított költség mellett támogatást nyújtson IKT-vonatkozású biztonsági esemény bekövetkezésekor.

(53) A pénzügyi szervezet vagy az általa kijelölt harmadik fél hozzáférési, vizsgálati és ellenőrzési jogosultságai elengedhetetlenek ahhoz, hogy a pénzügyi szervezet folyamatosan nyomon követhesse a harmadik félnek minősülő IKT-szolgáltató teljesítését, ami egyúttal feltételezi a szolgáltató teljes körű együttműködését a vizsgálatok során. Ugyanígy a pénzügyi szervezet illetékes hatóságának is jogosultsággal kell rendelkeznie arra, hogy értesítés alapján, a bizalmas adatok védelmének fenntartásával vizsgálatot és ellenőrzést végezzen a harmadik félnek minősülő IKT-szolgáltatónál.

(54) A szerződéses megállapodásoknak egyértelműen meg kell határozniuk a felmondási jogokat, a kapcsolódó minimális felmondási időket, valamint célzott kilépési stratégiákat is, ez utóbbiakkal lehetővé téve különösen a kötelező átállási időszakokat, amelyek során a harmadik félnek minősülő IKT-szolgáltatók kötelesek folyamatosan biztosítani az érintett funkciókat annak érdekében, hogy a zavar kockázata mérséklődjön a pénzügyi szervezet szintjén, a szervezet eredményesen válthasson a harmadik félnek minősülő IKT-szolgáltatók között, illetve helyszíni megoldásokhoz folyamodhasson, a nyújtott szolgáltatás összetettségének megfelelően.

(55) A Bizottság által a felhőszolgáltatásokra vonatkozóan kidolgozott általános szerződéses rendelkezések önkéntes alkalmazása további garanciát nyújthat a pénzügyi szervezetek és harmadik félnek minősülő IKT-szolgáltatóik számára azáltal, hogy – a pénzügyi szolgáltatások szabályozásában rögzített követelményekkel és elvárásokkal teljes összhangban – javítja a jogbiztonságot a pénzügyi ágazatban igénybe vett felhőszolgáltatások kapcsán. Ez a munka a 2018. évi pénzügyi technológiai cselekvési tervben már előirányzott intézkedésekre épít, amelyben a Bizottság bejelentette, hogy ösztönözni kívánja és elő kívánja mozdítani a pénzügyi szervezetek által igénybe vett kiszervezett felhőszolgáltatásokra vonatkozó általános szerződéses rendelkezések kidolgozását, ennek során pedig támaszkodna a felhőszolgáltatásban érdekeltek ágazatközi erőfeszítéseire, amelyeket a pénzügyi ágazat közreműködésével a Bizottság maga is megkönnyített.

(56) A pénzügyi ágazat harmadik féltől eredő IKT-kockázata kapcsán a konvergencia és a hatékonyság előmozdítása, az operatív funkciók ellátásához harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatót igénybe vevő pénzügyi szervezetek digitális

működési rezilienciájának megerősítése, ezáltal pedig az uniós pénzügyi rendszer stabilitásának, valamint a pénzügyi szolgáltatások egységes piaca integritásának eredményesebb megóvása érdekben az uniós felvigyázási keret hatályának ki kell terjednie a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra.

(57) Mivel a különleges elbánás csak a harmadik félnek minősülő kulcsfontosságú szolgáltatók esetében indokolt, az uniós felvigyázási keret alkalmazása céljából kijelölési mechanizmust kell bevezetni, amely figyelembe veszi azt, hogy a pénzügyi ágazat milyen mértékben és jelleggel vesz igénybe ilyen szolgáltatókat, ez pedig olyan mennyiségi és minőségi kritériumokat feltételez, amelyek alapján meghatározhatók a felvigyázás körébe vonást megalapozó kritikussági paraméterek. Az említett kritériumok alkalmazásával automatikusan nem kijelölt, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók számára lehetővé kell tenni a felvigyázási keretben történő önkéntes részvételt, ugyanakkor azoknak a harmadik félnek minősülő IKT-szolgáltatóknak, amelyek jelenleg is az Európai Unió működéséről szóló szerződés 127. cikkének (2) bekezdésében említett feladatok támogatása céljából az eurórendszer szintjén létrehozott felvigyázási mechanizmusok hatálya alá tartoznak, erre tekintettel mentességet kell kapniuk.

(58) A kulcsfontosságúként kijelölt, harmadik félnek minősülő IKT-szolgáltatók Unióban történő, jog szerinti bejegyzésének követelménye nem valósít meg adatlokalizációt, mivel ez a rendelet nem ír elő az Unióban végzendő adattárolásra, illetve adatkezelésre vonatkozó egyéb követelményt.

(59) A rendeletben előirányzott keret nem sértheti a tagállamok arra vonatkozó kompetenciáját, hogy saját hatáskörben felvigyázási feladatokat hajtsanak végre az olyan harmadik félnek minősülő IKT-szolgáltatók tekintetében, amelyek e rendelet szerint nem kulcsfontosságúak, de nemzeti szinten lényegesnek számíthatnak.

(60) A pénzügyi szolgáltatások területén a jelenlegi többrétegű intézményi struktúra kihasználása érdekében az EFH-k vegyes bizottságának – a kiberbiztonsággal kapcsolatos feladataival összhangban – továbbra is biztosítania kell az átfogó ágazatközi koordinációt az IKT-kockázatot érintő valamennyi kérdésben, ennek során pedig a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókat érintő egyedi döntéseket, valamint a kollektív ajánlásokat előkészítő új albizottság (felvigyázási fórum) munkájára támaszkodik, különösen a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázási programjának összehasonlító teljesítményértékelése és az IKT-koncentrációs kockázattal kapcsolatos kérdések megoldásában alkalmazható bevált módszerek azonosítása kapcsán.

(61) A pénzügyi ágazat működésében kulcsfontosságú szerepet betöltő technológiai szolgáltatók arányos, uniós léptékű figyelemmel kísérése céljából a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók mindegyike esetében ki kell jelölni vezető felvigyázóként az EFH-k valamelyikét.

(62) A vezető felvigyázóknak rendelkezniük kell az ahhoz szükséges hatáskörökkel, hogy vizsgálatot folytassanak, valamint helyszíni és külső ellenőrzést végezzenek a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóknál, beléphessenek minden releváns helyszínre, továbbá beszerezhessék azokat a teljes körű, naprakész információkat, amelyek alapján valós képet alkothatnak a pénzügyi szervezetekkel és végső soron az Unió pénzügyi rendszerével szemben fennálló, harmadik féltől eredő IKT-kockázat jellegéről, mértékéről és hatásáról.

Az EFH-k vezető felvigyázói megbízatása előfeltétel a pénzügyi szolgáltatási ágazatot érintő IKT-kockázat rendszerszintű dimenziójának megértéséhez és kezeléséhez. A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók uniós lábnyoma, valamint az ahhoz kapcsolódó esetleges IKT-koncentrációs kockázati problémák alapján uniós szintű kollektív megközelítés indokolt. Ha számos illetékes hatóság elkülönülten, kismértékű koordináció mellett vagy annak teljes hiányában gyakorol többféle ellenőrzési és hozzáférési jogot, az nem nyújt átfogó képet a harmadik féltől eredő IKT-kockázatról, ugyanakkor felesleges redundanciának, megterhelésnek és összetettségnek teszi ki azokat a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókat, amelyek ilyen többszörös igényekkel szembesülnek.

(63) Emellett lehetővé kell tenni a vezető felvigyázók számára, hogy ajánlásokat fogalmazhassanak meg az IKT-kockázatot érintő kérdésekről és azok megfelelő megoldásáról, ezen belül pedig kifogásolhassák azokat a szerződéses megállapodásokat, amelyek végső soron valamely pénzügyi szervezet vagy a pénzügyi rendszer stabilitását érintik. A vezető felvigyázók által megfogalmazott érdemi ajánlásoknak való megfelelést az illetékes nemzeti hatóságoknak kellően figyelembe kell venniük a pénzügyi szervezetek prudenciális felügyeletével kapcsolatos funkciójuk keretében.

(64) A felvigyázási keret semmilyen tekintetben, részlegesen sem váltja ki vagy helyettesíti a harmadik félnek minősülő IKT-szolgáltatók igénybevételével járó kockázatok pénzügyi szervezetek általi kezelését, így ez utóbbiakat nem mentesíti a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókkal kötött szerződéses megállapodásaik folyamatos nyomon követésére vonatkozó kötelezettség alól sem, továbbá nem érinti a pénzügyi szervezetek teljes felelősségét az e rendeletben és a pénzügyi szolgáltatásokra vonatkozó egyéb jogszabályokban előírt követelmények teljesítéséért. A párhuzamosságok és átfedések elkerülése érdekében az illetékes hatóságoknak tartózkodniuk kell attól, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók kockázatainak nyomon követésére önálló intézkedéseket hozzanak. Minden ilyen jellegű intézkedés a felvigyázási keretben végzett előzetes koordinációt és egyeztetést igényel.

(65) A harmadik félnek minősülő IKT-szolgáltatók digitáliskockázat-kezelésének felülvizsgálatában alkalmazható bevált módszerek kapcsán a nemzetközi konvergencia előmozdítása érdekében ösztönözni kell az EFH-kat arra, hogy a harmadik országbeli érintett felügyeleti és illetékes hatóságokkal kötött együttműködési megállapodások útján könnyítsék meg a harmadik féltől eredő IKT-kockázat kezelésében alkalmazható bevált módszerek kidolgozását.

(66) Az illetékes hatósági szakértők működési és IKT-kockázatkezeléssel kapcsolatos technikai szakértelmének hasznosítása céljából a vezető felvigyázóknak a nemzeti felügyeletek tapasztalatára támaszkodva külön vizsgálócsoportot kell létrehozniuk a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók mindegyikéhez. E multidiszciplináris csoportok támogatják a felvigyázási tevékenységek előkészítését és tényleges végrehajtását, ezen belül a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók helyszíni ellenőrzését, valamint az azt követően szükséges további intézkedéseket.

(67) Az illetékes hatóságoknak rendelkezniük kell minden olyan felügyeleti, vizsgálati és szankcionálási hatáskörrel, amely e rendelet alkalmazásához szükséges. A közigazgatási szankciókat főszabály szerint közzé kell tenni. Mivel a pénzügyi szervezet és a harmadik félnek minősülő IKT-szolgáltató székhelye nem feltétlenül

ugyanabban a tagállamban van, vagy az említettek eltérő ágazati illetékes hatóságok felügyelete alá tartozhatnak, az érintett illetékes hatóságok közötti szoros együttműködést – ideértve az 1024/2013/EU tanácsi rendelettel[39] ráruházott külön feladatok tekintetében az EKB-t is –, valamint az EFH-kkal folytatott konzultációt kölcsönös információcsere és a felügyeleti tevékenységekkel összefüggő segítségnyújtás útján kell biztosítani.

(68) A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók kijelölésére vonatkozó kritériumok mennyiségi és minőségi szempontjainak részletesebb meghatározása, valamint a felvigyázási díjak harmonizálása céljából a Bizottságot az Európai Unió működéséről szóló szerződés 290. cikkével összhangban fel kell hatalmazni jogi aktusok elfogadására a következők pontosabb megállapítása tekintetében: egy harmadik félnek minősülő IKT-szolgáltató megszűnésének rendszerszintű hatása az általa ellátott pénzügyi szervezetekre; az adott harmadik félnek minősülő IKT-szolgáltatót igénybe vevő globálisan rendszerszinten jelentős intézmények és egyéb rendszerszinten jelentős intézmények száma; egy adott piacon működő harmadik félnek minősülő IKT-szolgáltatók száma; a harmadik félnek minősülő IKT-szolgáltatók közötti váltás költségei; azon tagállamok száma, amelyekben az adott harmadik félnek minősülő IKT-szolgáltató szolgáltatásokat nyújt, és amelyekben az e szolgáltatót igénybe vevő pénzügyi szervezetek tevékenységet folytatnak; a felvigyázási díjak összege és megfizetésük 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 megállapodásnak[40] megfelelően kerüljön sor. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

(69) Mivel ez a rendelet az (EU) 20xx/xx európai parlamenti és tanácsi irányelvvel[41] közösen egységes szerkezetbe foglalja a pénzügyi szolgáltatásokra vonatkozó uniós vívmányok különböző rendeleteiben és irányelveiben, többek között az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, valamint a 909/2014/EU rendeletben az IKT-kockázatkezelésre vonatkozóan rögzített rendelkezéseket, a teljes következetesség érdekében az említett rendeleteket módosítani kell annak pontosításával, hogy az IKT-kockázatkezelésre vonatkozó rendelkezéseket e rendelet rögzíti.

A technikai standardoknak biztosítaniuk kell az e rendeletben megállapított követelmények következetes harmonizálását. Helyénvaló, hogy az európai felügyeleti hatóságok jelentős szakértelemmel rendelkező szervként kapjanak megbízást arra, hogy Bizottság részére történő benyújtás céljából olyan szabályozástechnikai standardtervezeteket dolgozzanak ki, amelyek nem igényelnek szakpolitikai döntéseket. Szabályozástechnikai standardokat kell kidolgozni az IKT-kockázatok kezelése, bejelentése és tesztelése, valamint a harmadik féltől eredő IKT-kockázat megbízható nyomon követésére vonatkozó alapkövetelmények területén.

---

39 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.).

40 HL L 123., 2016.5.12., 1. o.

41 [*Cím és HL-hivatkozás*]

(70) Különösen fontos, hogy a Bizottság az előkészítő munkálatok során megfelelő konzultációkat folytasson, többek között szakértői szinten is. A Bizottságnak és az EFH-knak biztosítaniuk kell, hogy az említett standardokat és követelményeket valamennyi pénzügyi szervezet olyan módon tudja alkalmazni, amely arányban áll az adott szervezetek és tevékenységeik jellegével, nagyságrendjével és összetettségével.

(71) A jelentős IKT-vonatkozású biztonsági eseményekkel kapcsolatos bejelentések könnyebb összehasonlíthatósága, valamint a harmadik félnek minősülő IKT-szolgáltatók IKT-szolgáltatásainak igénybevételéről szóló szerződéses megállapodások átláthatósága érdekében az EFH-knak felhatalmazást kell kapniuk végrehajtás-technikai standardtervezetek kidolgozására, amelyek meghatározzák a jelentős IKT-vonatkozású biztonsági események pénzügyi szervezetek általi bejelentésének egységes mintadokumentumait, formanyomtatványait és eljárásait, valamint az információ-nyilvántartás egységes mintadokumentumait. E standardok kidolgozása során az EFH-knak figyelembe kell venniük a szervezetek méretét és összetettségét, valamint tevékenységeik jellegét és kockázati szintjét. A Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 291. cikke szerinti végrehajtási jogi aktusok útján és az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 15. cikkével összhangban elfogadja az említett végrehajtás-technikai standardokat. Mivel az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, valamint a 909/2014/EU rendelet szabályozás- és végrehajtás-technikai standardokra épülő, felhatalmazáson alapuló és végrehajtási jogi aktusok útján már megfogalmazott további követelményeket, helyénvaló felhatalmazni az EFH-kat, hogy akár önállóan, akár a vegyes bizottság keretében együttesen szabályozás- és végrehajtás-technikai standardokat terjesszenek a Bizottság elé felhatalmazáson alapuló és végrehajtási jogi aktusok elfogadása céljából, amelyek átveszik és aktualizálják az IKT-kockázatkezelési szabályokat.

(72) A művelet a pénzügyi szolgáltatásokra vonatkozó jogszabályok különböző területein elfogadott, felhatalmazáson alapuló és végrehajtási jogi aktusok módosításával jár. A működési kockázatra vonatkozó, a végrehajtási és felhatalmazáson alapuló jogi aktusok elfogadására felhatalmazást adó cikkek hatályát módosítani kell annak érdekében, hogy e rendeletbe bele lehessen foglalni az említett rendeletek valamennyi olyan rendelkezését, amely a digitális működési rezilienciára vonatkozik.

(73) Mivel e rendelet célkitűzését, nevezetesen a pénzügyi szervezetek magas szintű digitális működési rezilienciáját a tagállamok nem tudják kielégítően megvalósítani, mert e célkitűzés számos különböző szabály harmonizálását követeli meg, amelyeket jelenleg uniós jogi aktusok vagy a különböző tagállamok jogrendszerei rögzítenek, az Unió szintjén azonban nagyságrendje és hatása miatt jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányossági elvnek megfelelően ez a rendelet nem lépi túl az e célok eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

(1) Ez a rendelet az alábbi egységes követelményeket állapítja meg a pénzügyi szervezetek üzleti folyamatait támogató hálózati és információs rendszerek biztonságára vonatkozóan, amely az általánosan magas szintű digitális működési reziliencia eléréséhez szükséges:

a) a következőkkel kapcsolatban a pénzügyi szervezetekre alkalmazandó követelmények:

– az információs és kommunikációs technológiák (IKT) kockázatkezelése;

– a jelentős IKT-vonatkozású biztonsági események bejelentése az illetékes hatóságoknál;

– a digitális működési reziliencia tesztelése;

– a kiberfenyegetésekkel és sebezhetőségekkel kapcsolatos adatok és információk megosztása;

– a harmadik féltől eredő IKT-kockázat pénzügyi szervezetek általi megbízható kezelésére vonatkozó intézkedések;

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

c) a pénzügyi szervezetek részére szolgáltatást nyújtó, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázási kerete;

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) 2016/1148 irányelv 5. cikkét átültető nemzeti szabályok értelmében alapvető szolgáltatást nyújtó szereplőként azonosított pénzügyi szervezetek tekintetében ez a rendelet az említett irányelv 1. cikke (7) bekezdésének alkalmazásában ágazatspecifikus uniós jogi aktusnak minősül.

2. cikk

Személyi hatály

(1) Ez a rendelet az alábbi szervezetekre alkalmazandó:

a) hitelintézetek;

b) pénzforgalmi intézmények;

c) elektronikuspénz-kibocsátó intézmények;

d) befektetési vállalkozások;

e) kriptoeszköz-szolgáltatók, kriptoeszköz-kibocsátók, eszközalapú tokenek kibocsátói és jelentős eszközalapú tokenek kibocsátói;

f) központi értéktárak;

g) központi szerződő felek;

h) kereskedési helyszínek;

i) kereskedési adattárak;

j) alternatívbefektetésialap-kezelők;

k) alapkezelő társaságok;

l) adatszolgáltatók;

m) biztosítók és viszontbiztosítók;

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

o) foglalkoztatói nyugellátást szolgáltató intézmények;

p) hitelminősítő intézetek;

q) jogszabály szerint engedélyezett könyvvizsgálók és könyvvizsgáló társaságok;

r) kritikus referenciamutatók kezelői;

s) közösségi finanszírozási szolgáltatók;

t) értékpapírosítási adattárak;

u) harmadik félnek minősülő IKT-szolgáltatók.

(2) E rendelet alkalmazásában az a)–t) pontban említett szervezetek együttes megnevezése „pénzügyi szervezetek”.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „digitális működési reziliencia”: a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja technológiai szempontból vett működési integritását azáltal, hogy közvetlenül vagy közvetetten, harmadik félnek minősülő IKT-szolgáltató szolgáltatásainak igénybevételével gondoskodik azon IKT-vonatkozású funkciók teljes körének ellátásáról, amelyek a pénzügyi szervezet által használt, a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogató hálózati és információs rendszerek biztonságának kezeléséhez szükségesek,

2. „hálózati és információs rendszer”: az (EU) 2016/1148 irányelv 4. cikkének 1. pontjában meghatározott hálózati és információs rendszer;

3. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszerek biztonsága az (EU) 2016/1148 irányelv 4. cikkének 2. pontjában meghatározottak szerint;

4. „IKT-kockázat”: minden olyan, a hálózati és információs rendszerek használata kapcsán észszerűen azonosítható körülmény, ideértve a rendellenes működést, a kapacitástúllépést, a meghibásodást, a zavart, az állapotromlást, a rendellenes használatot, a veszteséget, valamint az egyéb típusú rosszindulatú és nem

rosszindulatú eseményt is, amely bekövetkezése esetén veszélyeztetheti a hálózati és információs rendszerek, valamely technológiafüggő eszköz vagy folyamat, a műveletek és folyamatok végrehajtása, vagy a szolgáltatásnyújtás biztonságát, és ezáltal veszélyezteti az adatok, a szoftverek, vagy az IKT-szolgáltatásokban és -infrastruktúrákban foglalt egyéb összetevők integritását vagy rendelkezésre állását, vagy a titoktartás megsértéséhez, a fizikai IKT-infrastruktúra károsodásához, vagy egyéb káros hatáshoz vezet;

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

6. „IKT-vonatkozású biztonsági esemény”: a hálózati és információs rendszerekben előforduló, előre nem látott, azonosított, rosszindulatú vagy nem rosszindulatú tevékenységgel előidézett esemény, amely veszélyezteti a hálózati és információs rendszerek, illetve az e rendszerekben kezelt, tárolt vagy továbbított információk biztonságát, vagy káros hatással van a pénzügyi szervezet által nyújtott pénzügyi szolgáltatások rendelkezésre állására, bizalmas jellegére, folytonosságára vagy hitelességére;

7. „jelentős IKT-vonatkozású biztonsági esemény”: olyan IKT-vonatkozású biztonsági esemény, amely fokozottan káros hatással lehet a pénzügyi szervezet kulcsfontosságú funkcióit támogató hálózati és információs rendszerekre;

8. „kiberfenyegetés”: az (EU) 2019/881 európai parlamenti és tanácsi rendelet[42] 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

9. „kibertámadás”: rosszindulatú IKT-vonatkozású biztonsági esemény, amelynek során egy fenyegető szereplő egy eszköz megsemmisítésére, felfedésére, módosítására, használhatatlanná tételére, eltulajdonítására, jogosulatlan felhasználására, vagy az eszközhöz való jogosulatlan hozzáférésre tesz kísérletet;

10. „fenyegetettségi információk”: döntéshozatalt megalapozó összesített, átalakított, elemzett, értelmezett, gyarapított adatok összessége, amely érdemi és elégséges ismeretet eredményez valamely IKT-vonatkozású biztonsági esemény vagy kiberfenyegetés hatásának enyhítéséhez, és magában foglalja többek között a kibertámadás technikai részleteit, a támadás felelőseinek személyazonosságát, valamint az elkövetés módját és indítékait;

11. „mélységben tagolt védelem”: IKT-vonatkozású stratégia, amely személyeket, folyamatokat és technológiát integrálva képez akadályokat a szervezet több rétege és dimenziója mentén;

12. „sebezhetőség”: valamely eszköz, rendszer, folyamat vagy kontroll olyan gyengesége, érzékenysége vagy hiányossága, amely egy fenyegetés során kihasználható;

13. „fenyegetettségi szempontú behatolási tesztelés”: tényleges kiberfenyegetés forrásaként észlelt, valós fenyegető szereplők taktikájának, módszereinek és eljárásainak utánzásával érdekütköztetéses elemzőcsoport által végzett ellenőrzött, célzott, információkon alapuló teszt a szervezet kulcsfontosságú éles rendszerein;

[42] 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.).

14. „harmadik féltől eredő IKT-kockázat”: a pénzügyi szervezetnél azzal összefüggésben felmerülő esetleges IKT-kockázat, hogy harmadik félnek minősülő IKT-szolgáltatók vagy azok alvállalkozói által nyújtott szolgáltatásokat vesz igénybe;

15. „harmadik félnek minősülő IKT-szolgáltató”: digitális és adatszolgáltatásokat nyújtó vállalkozás, többek között a felhőszolgáltató, a szoftverszolgáltató, az adatelemzési szolgáltatást nyújtó és az adatközpont, kivéve a hardverösszetevő szállítóját, valamint az uniós jog szerint engedélyezett olyan vállalkozást, amely az (EU) 2018/1972 európai parlamenti és tanácsi irányelv[43] 2. cikkének 4. pontjában meghatározott elektronikus hírközlési szolgáltatást nyújt;

16. „IKT-szolgáltatások”: IKT-rendszer útján egy vagy több belső vagy külső felhasználó részére nyújtott digitális és adatszolgáltatások, ideértve az adatok átadását, rögzítését, tárolását, feldolgozását, közlését, nyomon követését, valamint az adatalapú üzleti és döntéstámogató szolgáltatásokat;

17. „kulcsfontosságú vagy lényeges funkció”: olyan funkció, amelynek kiesése, hibás vagy meghiúsult működése jelentősen rontaná a pénzügyi szervezet képességét az engedélyében foglalt feltételek és kötelezettségek, valamint a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt egyéb kötelezettségei folyamatos teljesítésére, illetve pénzügyi teljesítményét, vagy szolgáltatásai, tevékenységei megbízhatóságát, folytonosságát;

18. „harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató”: a 29. cikk szerint kijelölt, harmadik félnek minősülő IKT-szolgáltató, amely a 30–37. cikkben említett felvigyázási keret hatálya alá tartozik;

19. „harmadik országban letelepedett, harmadik félnek minősülő IKT-szolgáltató”: harmadik országban letelepedett, jogi személyiséggel rendelkező, harmadik félnek minősülő IKT-szolgáltató, amely nem hozott létre vállalkozást / nincs jelen az Unióban, és egy pénzügyi szervezettel IKT-szolgáltatások nyújtásáról szóló szerződéses megállapodást kötött;

20. „harmadik országban letelepedett IKT-alvállalkozó”: harmadik országban letelepedett, jogi személyiséggel rendelkező IKT-alvállalkozó, amely nem hozott létre vállalkozást / nincs jelen az Unióban, és harmadik félnek minősülő IKT-szolgáltatóval vagy harmadik országban letelepedett, harmadik félnek minősülő IKT-szolgáltatóval szerződéses megállapodást kötött;

21. „IKT-koncentrációs kockázat”: harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóval vagy több ilyen, egymással kapcsolatban álló szolgáltatóval szembeni kitettség, amely e szolgáltatóktól olyan mértékű függőséget eredményez, hogy kiesésük, megszűnésük vagy egyéb hiányosságuk veszélyeztetheti a pénzügyi szervezet és végső soron a teljes uniós pénzügyi rendszer kulcsfontosságú funkciók ellátására való képességét, vagy egyéb káros hatásokkal, többek között jelentős veszteségekkel járhat;

22. „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 irányelv 2. cikke (1) bekezdésének s. pontjában, a 909/2014/EU rendelet 2. cikke (1) bekezdésének 45. pontjában, az (EU) 2016/1011 európai parlamenti és tanácsi

[43] Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (átdolgozás) (HL L 321., 2018.12.17., 36. o.).

rendelet[44] 3. cikke (1) bekezdésének 20. pontjában és az (EU) 20xx/xx európai parlamenti és tanácsi rendelet[45] [MiCA] 3. cikke (1) bekezdésének u. pontjában meghatározott vezető testület, vagy annak tagjaival egyenértékű személyek csoportja, akik ténylegesen működtetik a szervezetet, vagy abban a vonatkozó uniós vagy nemzeti jogszabályokkal összhangban kulcsfontosságú funkciót látnak el;

23. „hitelintézet”: az 575/2013/EU európai parlamenti és tanácsi rendelet[46] 4. cikke (1) bekezdésének 1. pontjában meghatározott hitelintézet;

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

25. „pénzforgalmi intézmény”: az (EU) 2015/2366 irányelv 1. cikke (1) bekezdésének d) pontjában meghatározott pénzforgalmi intézmény;

26. „elektronikuspénz-kibocsátó intézmény”: a 2009/110/EK európai parlamenti és tanácsi irányelv[47] 2. cikke 1. pontjában meghatározott elektronikuspénz-kibocsátó intézmény;

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

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

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

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

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

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

33. „adatszolgáltató”: a 2014/65/EU irányelv 4. cikke (1) bekezdésének 63. pontjában meghatározott adatszolgáltató;

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

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

---

44 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 és a 2008/48/EK és a 2014/17/EU irányelv és az 596/2014/EU rendelet módosításáról (HL L 171., 2016.6.29., 1. o.).

45 [*Cím és HL-hivatkozás*]

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

47 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.).

36. „biztosításközvetítő”: az (EU) 2016/97 irányelv 2. cikkének 3. pontjában meghatározott biztosításközvetítő;

37. „kiegészítő biztosításközvetítői tevékenységet végző személy”: az (EU) 2016/97 irányelv 2. cikkének 4. pontjában meghatározott kiegészítő biztosításközvetítői tevékenységet végző személy;

38. „viszontbiztosítás-közvetítő”: az (EU) 2016/97 irányelv 2. cikkének 5. pontjában meghatározott viszontbiztosítás-közvetítő;

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

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

41. „jogszabály szerint engedélyezett könyvvizsgáló”: a 2006/43/EK irányelv 2. cikkének 2. pontjában meghatározott jog szerinti könyvvizsgáló;

42. „könyvvizsgáló társaság” a 2006/43/EK irányelv 2. cikkének 3. pontjában meghatározott könyvvizsgáló cég;

43. „kriptoeszköz-szolgáltató”: az (EU) 202x/xx [*KH: a MiCA-rendelet hivatkozása*] rendelet 3. cikke (1) bekezdésének n) pontjában meghatározott kriptoeszköz-szolgáltató;

44. „kriptoeszköz-kibocsátó”: a [*MiCA-rendelet HL-hivatkozása*] rendelet 3. cikke (1) bekezdésének h) pontjában meghatározott kriptoeszköz-kibocsátó;

45. „eszközalapú token kibocsátója”: a [*MiCA-rendelet HL-hivatkozása*] rendelet 3. cikke (1) bekezdésének i) pontjában meghatározott, eszközhöz kötött fizetési token kibocsátója;

46. „jelentős eszközalapú token kibocsátója”: a [*MiCA-rendelet HL-hivatkozása*] rendelet 3. cikke (1) bekezdésének j) pontjában meghatározott, eszközhöz kötött jelentős fizetési token kibocsátója;

47. „kritikus referenciamutató kezelője”: az (EU) 202x/xx rendelet [*a referenciamutató-rendelet HL-hivatkozása*] x. cikkének x) pontjában meghatározott kritikus referenciamutató kezelője;

48. „európai közösségi finanszírozási szolgáltató”: az (EU) 202x/xx rendelet [*a közösségi finanszírozási rendelet HL-hivatkozása*] x. cikkének x. pontjában meghatározott európai közösségi finanszírozási szolgáltató;

49. „értékpapírosítási adattár”: az (EU) 2017/2402 rendelet 2. cikkének 23. pontjában meghatározott értékpapírosítási adattár;

50. „mikrovállalkozás”: a 2003/361/EK ajánlás melléklete 2. cikkének (3) bekezdésében meghatározott mikrovállalkozás.

II. FEJEZET

IKT-KOCKÁZATKEZELÉS

I. SZAKASZ

4. cikk

Irányítás és szervezeti felépítés

(1) A pénzügyi szervezetek belső irányítási és kontrollkerettel rendelkeznek, amelyek biztosítják valamennyi IKT-kockázat eredményes és prudens kezelését.

(2) A pénzügyi szervezet vezető testülete meghatározza, jóváhagyja és ellenőrzi az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszerrel összefüggő intézkedéseket, és elszámoltatható azok végrehajtásáért:

Az első albekezdés alkalmazásában a vezető testület:

a) végső felelősséggel tartozik a pénzügyi szervezet IKT-kockázatainak kezeléséért;

b) egyértelmű feladat- és felelősségi köröket jelöl ki minden IKT-vonatkozású funkcióval összefüggésben;

c) az 5. cikk (9) bekezdésének b) pontjában említett módon meghatározza a pénzügyi szervezet IKT-kockázati toleranciáját;

d) jóváhagyja, ellenőrzi és rendszeresen felülvizsgálja a pénzügyi szervezetnek a 10. cikk (1), illetve (3) bekezdésében említett IKT-vonatkozású üzletmenet-folytonossági szabályait és IKT-vonatkozású katasztrófa utáni helyreállítási tervét;

e) jóváhagyja és rendszeresen felülvizsgálja az IKT-ellenőrzésre vonatkozó terveket, az IKT-ellenőrzéseket és azok jelentős módosításait;

f) megállapítja és rendszeresen felülvizsgálja a pénzügyi szervezet digitális működési rezilienciával kapcsolatos szükségleteinek megfelelő ellátását biztosító költségvetést minden erőforrástípusra kiterjedően, beleértve az érintett személyi állomány IKT-kockázatokkal kapcsolatos képzését és készségfejlesztését is;

g) jóváhagyja és rendszeresen felülvizsgálja a pénzügyi szervezet politikáját a harmadik félnek minősülő IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló megállapodásokra vonatkozóan;

h) megfelelően tájékozódik a harmadik félnek minősülő IKT-szolgáltatókkal az IKT-szolgáltatások igénybevételére vonatkozóan kötött megállapodásokról, a harmadik félnek minősülő IKT-szolgáltatókra vonatkozóan tervezett lényeges változtatásokról, valamint azokról a potenciális hatásokról, amelyeket e változtatások gyakorolhatnak a megállapodásokkal érintett kulcsfontosságú vagy lényeges funkciókra, ezen belül átveszi a változások hatását vizsgáló kockázatelemzés összefoglalóját;

i) megfelelően tájékozódik az IKT-vonatkozású biztonsági eseményekről és azok hatásáról, valamint az elhárítási, helyreállítási és korrekciós intézkedésekről.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek létrehozzák a harmadik félnek minősülő IKT-szolgáltatókkal IKT-szolgáltatások igénybevételére vonatkozóan kötött megállapodások nyomon követésére vonatkozó feladatkört, vagy a kapcsolódó kockázati kitettség és a vonatkozó dokumentáció ellenőrzéséért felelős személyként kinevezik a felső vezetés egy tagját.

(4) A vezető testület tagjai rendszeres speciális képzés keretében megszerzik és naprakészen tartják azokat a megfelelő ismereteket és készségeket, amelyek birtokában megérthetik és értékelhetik az IKT-kockázatokat és azoknak a pénzügyi szervezet működésére gyakorolt hatását.

II. SZAKASZ

5. cikk

IKT-kockázatkezelési keretrendszer

(1) A pénzügyi szervezetek megbízható, átfogó és jól dokumentált IKT-kockázatkezelési keretrendszerrel rendelkeznek, amely lehetővé teszi számukra az IKT-kockázat gyors, hatékony és átfogó kezelését, továbbá a digitális működési reziliencia olyan szintjének biztosítását, amely megfelel üzleti igényeiknek, méretüknek és összetettségüknek.

(2) Az (1) bekezdésben említett IKT-kockázatkezelési keretrendszer magában foglalja azokat a stratégiákat, szabályzatokat, eljárásokat, IKT-protokollokat és eszközöket, amelyek a releváns fizikai összetevők és infrastruktúrák, ezen belül a számítógépes hardvereszközök, kiszolgálók, továbbá a releváns helyszínek, adatközpontok és kijelölt érzékeny területek megfelelő és eredményes védelméhez szükségesek többek között a sérülés, valamint az illetéktelen hozzáférés és használat kockázatával szemben.

(3) A pénzügyi szervezetek az IKT-kockázat csökkentése érdekében bevezetik az IKT-kockázatkezelési keretrendszerben előírt megfelelő stratégiákat, szabályzatokat, eljárásokat, protokollokat és eszközöket. Az IKT-kockázatokkal kapcsolatban átadják az illetékes hatóságok által kért teljes körű és naprakész információkat.

(4) Az (1) bekezdésben említett IKT-kockázatkezelési keretrendszer részeként a mikrovállalkozásnak nem minősülő pénzügyi szervezetek az elismert nemzetközi szabványokra épülő és a felügyeleti iránymutatásoknak megfelelő információbiztonsági irányítási rendszert vezetnek be, amelyet rendszeresen felülvizsgálnak.

(5) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek gondoskodnak az IKT-vonatkozású irányítási funkciók, kontrollfunkciók és belső ellenőrzési funkciók megfelelő különválasztásáról a három védelmi vonalra épülő modellnek, vagy belső kockázatkezelési és kontrollmodellnek megfelelően.

(6) Az (1) bekezdésben említett IKT-kockázatkezelési keretrendszert dokumentálni kell és legalább évente egyszer felül kell vizsgálni, emellett a felülvizsgálatot el kell végezni jelentős IKT-vonatkozású biztonsági esemény bekövetkezésekor, valamint a digitális működési reziliencia tesztelésére vagy ellenőrzésére irányuló releváns folyamatok alapján megfogalmazott felügyeleti utasítások és következtetések nyomán is. A keretrendszert folyamatosan fejleszteni kell a végrehajtás és a nyomon követés során szerzett tapasztalatok alapján.

(7) Az IKT-kockázat területén megfelelő ismeretekkel, készségekkel és szakértelemmel rendelkező IKT-ellenőrök rendszeresen ellenőrzik az (1) bekezdésben említett IKT-kockázatkezelési keretrendszert. Az IKT-ellenőrzések gyakorisága és fókusza arányos a pénzügyi szervezet IKT-kockázataival.

(8) A szervezet az IKT-ellenőrzések legfontosabb megállapításai alapján végzett, időben történő igazolásra és korrekcióra vonatkozó szabályokra is kiterjedő, formális utókövetési folyamatot alakít ki, amely figyelembe veszi a felülvizsgálat következtetéseit, ugyanakkor kellő tekintettel van a pénzügyi szervezet szolgáltatásainak és tevékenységeinek jellegére, nagyságrendjére és összetettségére is.

(9) Az (1) bekezdésben említett IKT-kockázatkezelési keretrendszer a digitális rezilienciára vonatkozó stratégiát is magában foglal, amely meghatározza a keretrendszer végrehajtását. E célból a stratégia a következők révén meghatározza az IKT-kockázatok kezelésének és a konkrét IKT-célkitűzések megvalósításának módszereit:

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

b) megállapítja az IKT-kockázati toleranciát a pénzügyi szervezet kockázatvállalási hajlandóságával összhangban, továbbá elemzi az IKT-zavarok hatásaival kapcsolatos toleranciát;

c) egyértelmű információbiztonsági célkitűzéseket határoz meg;

d) ismerteti az IKT-referenciaarchitektúrákat a meghatározott üzleti célkitűzések eléréséhez szükséges változtatásokkal együtt;

e) vázolja az IKT-vonatkozású biztonsági események észlelését, megelőzését, valamint a hatásaikkal szembeni védelmet szolgáló mechanizmusokat;

f) bizonyítékokkal támasztja alá a bejelentett jelentős IKT-vonatkozású biztonsági események számát és a megelőző intézkedések eredményességét;

g) szervezeti szintű, több beszállítóra épülő holisztikus IKT-stratégiát határoz meg, amely bemutatja a harmadik félnek minősülő IKT-szolgáltatóktól való főbb függőségeket, továbbá kifejti a harmadik félnek minősülő szolgáltatóknál alkalmazott beszerzési mix indokolását;

h) végrehajtja a digitális működési reziliencia tesztelését;

i) vázolja az IKT-vonatkozású biztonsági események bekövetkezésekor alkalmazandó kommunikációs stratégiát.

(10) Az illetékes hatóságok jóváhagyásával a pénzügyi szervezetek a vállalatcsoportjukon belüli vagy külső vállalkozásokhoz delegálhatják az IKT-kockázatkezelési követelményeknek való megfelelés ellenőrzésével kapcsolatos feladatokat.

6. cikk

IKT-rendszerek, -protokollok, -eszközök

(1) A pénzügyi szervezetek naprakész IKT-rendszereket, -protokollokat és -eszközöket alkalmaznak és tartanak fenn, amelyek teljesítik az alábbi feltételeket:

a) a rendszerek és eszközök megfelelnek a szervezet tevékenységének folytatását támogató műveletek jellegének, változatosságának, összetettségének és nagyságrendjének;

b) megbízhatók;

c) kapacitásuk lehetővé teszi az ahhoz szükséges adatok pontos feldolgozását, hogy a szervezet kellő időben elvégezhesse tevékenységeit és nyújthassa szolgáltatásait, továbbá szükség szerint lehetővé teszi a kiugróan magas megbízási, üzenetküldési és ügyleti volumen kezelését többek között új technológia bevezetésekor;

d) technológiai rezilienciájuk lehetővé teszi a piaci stresszhelyzetben vagy egyéb hátrányos helyzetben felmerülő fokozott adatfeldolgozási igények megfelelő ellátását.

(2) A pénzügyi szervezetek az információbiztonságra és a belső IKT-kontrollokra vonatkozó nemzetközileg elismert technikai szabványokat és ágazati bevált módszereket az ezek felhasználására irányadó felügyeleti ajánlásokkal összhangban alkalmazzák.

7. cikk

Azonosítás

(1) Az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek azonosítják, osztályozzák és megfelelően dokumentálják az IKT-vonatkozású üzleti funkciókat, az ezeket támogató információs eszközöket, továbbá az IKT-rendszerek konfigurációit, valamint belső és külső IKT-rendszerekkel való kapcsolatait. A pénzügyi szervezetek szükség szerint, de legalább évente felülvizsgálják az információs eszközök osztályozásának és a vonatkozó dokumentációnak a megfelelőségét.

(2) A pénzügyi szervezetek folyamatosan azonosítják az IKT-kockázat minden forrását, különösen a más pénzügyi szervezetekkel szembeni kölcsönös kockázati kitettséget, továbbá értékelik az IKT-vonatkozású üzleti funkciókhoz és információs eszközökhöz kapcsolódó kiberfenyegetéseket és IKT-sebezhetőségeket. A pénzügyi szervezetek rendszeresen, de legalább évente felülvizsgálják az őket érintő kockázati forgatókönyveket.

(3) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek a hálózati és információs rendszerinfrastruktúra, a funkcióikat érintő folyamatok és eljárások, a támogató folyamatok, valamint az információs eszközök minden jelentős változásakor kockázatértékelést végeznek.

(4) A pénzügyi szervezetek azonosítják az összes IKT-rendszerfiókot, ideértve a távoli helyeken találhatókat is, továbbá a hálózati erőforrásokat és a hardvereszközöket, és feltérképezik a kulcsfontosságúnak minősülő fizikai eszközöket. Feltérképezik az IKT-eszközök konfigurációját, valamint a különböző eszközök kapcsolatait és egymástól való függését.

(5) A pénzügyi szervezetek azonosítják és dokumentálják a harmadik félnek minősülő IKT-szolgáltatóktól függő folyamatokat, valamint a harmadik félnek minősülő IKT-szolgáltatókkal meglévő kapcsolatokat.

(6) Az (1), (4) és (5) bekezdés alkalmazásában a pénzügyi szervezetek fenntartják és rendszeresen frissítik a vonatkozó nyilvántartásokat.

(7) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek rendszeresen, de legalább évente célzottan értékelik a meglévő IKT-rendszerek IKT-kockázatait, különösen a régi és új technológiák, alkalmazások vagy rendszerek összekapcsolása előtt és után.

8. cikk

Védelem és megelőzés

(1) Az IKT-rendszerek megfelelő védelme és a válaszintézkedések megszervezése érdekében a pénzügyi szervezetek gondoskodnak az IKT-rendszerek és -eszközök működésének folyamatos nyomon követéséről és kontrolljáról, és az ezeket érintő kockázatok hatását megfelelő IKT-biztonsági eszközök, szabályzatok és eljárások bevezetésével csökkentik.

(2) A pénzügyi szervezetek megtervezik, illetve beszerzik és végrehajtják azokat az IKT-biztonsági stratégiákat, szabályzatokat, eljárásokat, protokollokat és eszközöket, amelyek elsődleges célja, hogy biztosítsák az IKT-rendszerek rezilienciáját, folytonosságát és rendelkezésre állását, továbbá fenntartsák az adatok biztonságára, bizalmas jellegére és integritására vonatkozó normákat a használaton kívüli, használatban lévő, valamint a továbbítás alatt álló adatok esetében egyaránt.

(3) A (2) bekezdésben említett célkitűzések elérése érdekében a pénzügyi szervezetek a legkorszerűbb IKT-technológiákat és -folyamatokat alkalmazzák, amelyek:

a) garantálják az információk továbbítására használt eszközök biztonságát;

b) minimalizálják az adatsérülés és -veszteség, a jogosulatlan hozzáférés, valamint az üzleti tevékenységet akadályozó technikai hibák kockázatát;

c) megelőzik az információk kiszivárgását;

d) biztosítják az adatok védelmét a nem megfelelő adminisztrációval és feldolgozással, ezen belül a nyilvántartási hiányosságokkal összefüggő kockázatokkal szemben.

(4) Az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek:

a) dokumentált információbiztonsági szabályzatot dolgoznak ki, amely meghatározza a saját szervezetükben és ügyfeleiknél használt IKT-erőforrások, adatok és információs eszközök bizalmas jellegének, integritásának és rendelkezésre állásának védelmét biztosító szabályokat;

b) kockázatalapú megközelítéssel kialakítják a hálózatok és infrastruktúrák megbízható kezelését, amely megfelelő technikákkal, módszerekkel és protokollokkal, többek között automatizált mechanizmusokkal elszigeteli az érintett eszközöket kibertámadás esetén;

c) az IKT-rendszerek erőforrásaihoz és adataihoz való fizikai és virtuális hozzáférést kizárólag a jogszerű és jóváhagyott funkciók és tevékenységek ellátásához szükséges mértékűre korlátozzák, és erre irányuló szabályzatok, eljárások és kontrollok kialakításával kezelik a hozzáférési jogosultságokat és azok megbízható adminisztrációját;

d) szabályzatok és protokollok végrehajtásával erős hitelesítési mechanizmust alakítanak ki a vonatkozó szabványok és az erre irányuló kontrollrendszerek alapján, amely a jóváhagyott adatminősítési és kockázatértékelési folyamatok eredményeinek megfelelően titkosított adatok esetében megakadályozza a kriptográfiai kulcsokhoz való hozzáférést;

e) kockázatértékelési megközelítésen alapuló, a pénzügyi szervezet átfogó változásmenedzsment-folyamatába illeszkedő, IKT-változásmenedzsmentre vonatkozó, szoftver-, hardver- és förmverösszetevőket, rendszert és biztonságot érintő változásokra is kiterjedő szabályzatok, eljárások és kontrollok végrehajtásával biztosítják az IKT-rendszerek valamennyi változásának kontrollált rögzítését, tesztelését, értékelését, jóváhagyását, végrehajtását és ellenőrzését;

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

A b) pont alkalmazásában a pénzügyi szervezetek a hálózati kapcsolati infrastruktúrát azonnali megszakításra alkalmas módon alakítják ki, továbbá az infrastruktúra területi egységekre osztásával és szakaszokra bontásával minimálisra csökkentik, illetve megelőzik az átterjedést, különösen az egymással összekapcsolt pénzügyi folyamatok esetében.

Az e) pont alkalmazásában az IKT-vonatkozású változásmenedzsment-folyamatot a megfelelő vezetői szint hagyja jóvá, emellett a folyamat célzott protokollokat is magában foglal rendkívüli változások esetére.

9. cikk

Észlelés

(1) A pénzügyi szervezetek olyan mechanizmusokkal rendelkeznek, amelyek segítségével a 15. cikknek megfelelően azonnal észlelhetik a rendellenes tevékenységeket, beleértve az IKT-hálózatok teljesítményproblémáit és az IKT-vonatkozású biztonsági eseményeket is, továbbá teljeskörűen azonosíthatják a potenciálisan jelentős egyedi meghibásodási pontokat.

A szervezet a 22. cikkel összhangban rendszeresen teszteli az első albekezdésben említett észlelési mechanizmusokat.

(2) Az (1) bekezdésben említett észlelési mechanizmusok lehetővé teszik a többszintű kontrollt, meghatározzák az IKT-vonatkozású biztonsági események észlelési és válaszfolyamatait kiváltó riasztási értékhatárokat és kritériumokat, továbbá automatikus riasztási mechanizmusokat vezetnek be az IKT-vonatkozású biztonsági eseményekre való reagálásért felelős személyi állomány számára.

(3) A pénzügyi szervezetek a méretükhöz és üzleti, kockázati profiljukhoz mérten elégséges erőforrásokat és képességeket biztosítanak a felhasználói tevékenységek, valamint az IKT-vonatkozású rendellenességek és biztonsági események, különösen a kibertámadások előfordulásának nyomon követéséhez.

(4) A 2. cikk (1) bekezdésének l) pontjában említett pénzügyi szervezetek ezenkívül rendelkeznek olyan rendszerekkel, amelyek hathatósan ellenőrzik a kereskedési jelentéseket azok teljeskörűsége szempontjából, azonosítják a kihagyásokat és a nyilvánvaló hibákat, és kérik az ilyen hibás jelentések újraküldését.

10. cikk

Elhárítás és helyreállítás

(1) Az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként, a 7. cikkben említett azonosítási követelmények alapján a pénzügyi szervezetek célzott és átfogó IKT-vonatkozású üzletmenet-folytonossági szabályokat vezetnek be operatív üzletmenet-folytonossági politikájuk szerves részeként.

(2) A pénzügyi szervezetek az (1) bekezdésben említett IKT-vonatkozású üzletmenet-folytonossági szabályokat célzott, megfelelő és dokumentált intézkedések, tervek, eljárások és mechanizmusok útján hajtják végre, amelyek céljai a következők:

a) az IKT-vonatkozású biztonsági események teljes körű rögzítése;

b) a folytonosság biztosítása a pénzügyi szervezet kulcsfontosságú funkciói kapcsán;

c) az IKT-vonatkozású biztonsági események, különösen – de nem kizárólag – a kibertámadások gyors, megfelelő és eredményes elhárítása és megoldása a kár mérséklésével, a tevékenység újraindítását és a helyreállítási intézkedéseket előtérbe helyezve;

d) célzott tervek haladéktalan aktiválása, amelyek lehetővé teszik az IKT-vonatkozású biztonsági események egyes típusainak megfelelő, elszigetelésre irányuló intézkedések, folyamatok és technológiák alkalmazását, a további károk megelőzését, valamint a 11. cikkel összhangban kialakított célzott elhárítási és helyreállítási intézkedéseket;

e) a hatások, károk, veszteségek előzetes felmérése;

f) kommunikációs és válságkezelési intézkedések meghatározása, amelyek biztosítják a naprakész információk eljuttatását az érintett belső személyi állomány és a külső érdekelt felek részére a 13. cikk, valamint az illetékes hatóságok részére a 17. cikk szerint.

(3) Az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek IKT-vonatkozású katasztrófa utáni helyreállítási tervet vezetnek be, amelyről a mikrovállalkozásnak nem minősülő pénzügyi szervezetek esetében független felülvizsgálat készül.

(4) A pénzügyi szervezetek – különösen a harmadik félnek minősülő IKT-szolgáltatókkal kötött megállapodások keretében kiszervezett vagy megbízásba adott kulcsfontosságú vagy lényeges funkciókra vonatkozóan – megfelelő IKT-vonatkozású üzletmenet-folytonossági tervet vezetnek be és tartanak fenn, amelyet rendszeresen tesztelnek.

(5) Átfogó IKT-kockázatkezelésük keretében a pénzügyi szervezetek:

a) legalább évente, valamint az IKT-rendszereket érintő jelentős változásokat követően tesztelik az IKT-vonatkozású üzletmenet-folytonossági szabályokat és az IKT-vonatkozású katasztrófa utáni helyreállítási tervet;

b) tesztelik a 13. cikknek megfelelően kialakított válsághelyzeti kommunikációs terveket.

Az a) pont alkalmazásában a mikrovállalkozásnak nem minősülő pénzügyi szervezetek a tesztelési terveikben kibertámadásra, továbbá az elsődleges IKT-infrastruktúrájuk és a 11. cikkben meghatározott kötelezettségek teljesítéséhez

szükséges tartalékkapacitás, biztonsági mentések és tartalékeszközök közötti átállásra vonatkozó forgatókönyveket szerepeltetnek.

A pénzügyi szervezetek rendszeresen felülvizsgálják IKT-vonatkozású üzletmenet-folytonossági szabályaikat és IKT-vonatkozású katasztrófa utáni helyreállítási tervüket, figyelembe véve az első albekezdés szerint elvégzett tesztek eredményeit, valamint az ellenőrzések és felügyeleti felülvizsgálatok alapján megfogalmazott ajánlásokat.

(6) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek válságkezelési funkcióval rendelkeznek, amely az IKT-vonatkozású üzletmenet-folytonossági szabályok vagy az IKT-vonatkozású katasztrófa utáni helyreállítási terv aktiválása esetén a 13. cikkel összhangban egyértelmű eljárást határoz meg a belső és külső válsághelyzeti kommunikáció kezelésére vonatkozóan.

(7) Az IKT-vonatkozású üzletmenet-folytonossági szabályok vagy az IKT-vonatkozású katasztrófa utáni helyreállítási terv aktiválása esetén a pénzügyi szervezetek nyilvántartást vezetnek a zavart okozó eseményeket megelőzően és azok időtartama alatt végzett tevékenységekről. A nyilvántartásoknak könnyen elérhetőnek kell lenniük.

(8) A 2. cikk (1) bekezdésének f) pontjában említett pénzügyi szervezetek másolatban átadják az illetékes hatóságoknak a vizsgált időszak alatt végzett IKT-szempontú üzletmenet-folytonossági tesztek vagy azokhoz hasonló műveletek eredményeit.

(9) A mikrovállalkozásnak nem minősülő pénzügyi szervezetek beszámolnak az illetékes hatóságoknak az IKT-zavarokból és az IKT-vonatkozású biztonsági eseményekből eredő költségeikről és veszteségeikről.

11. cikk

Biztonsági mentési szabályzatok és helyreállítási módszerek

(1) Annak érdekében, hogy IKT-rendszereiket minimális leállási időt és zavart követően állíthassák helyre, IKT-kockázatkezelési keretrendszerük részeként a pénzügyi szervezetek kidolgozzák a következőket:

a) a biztonsági mentésre vonatkozó szabályzat, amely az információk kritikus mivolta vagy az adatok érzékenysége alapján meghatározza a biztonsági mentés adatkörét és minimális gyakoriságát;

b) a helyreállítási módszerek.

(2) A készenléti rendszereknek azonnal meg kell kezdeniük az adatfeldolgozást, kivéve akkor, ha az átállás veszélyeztetné a hálózati és információs rendszerek integritását és biztonságát, vagy a bizalmas adatok védelmét.

(3) Az adatok biztonsági mentés alapján, saját rendszerekkel végzett helyreállításához a pénzügyi szervezetek olyan IKT-rendszereket használnak, amelyek az elsődleges rendszertől eltérő környezetben működnek, ahhoz közvetlenül nem kapcsolódnak, és rendelkeznek illetéktelen hozzáférés és IKT-sérülés elleni biztonságos védelemmel.

A 2. cikk (1) bekezdésének g) pontjában említett pénzügyi szervezetek esetében a helyreállítási terv lehetővé teszi 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.

(4) A pénzügyi szervezetek IKT-tartalékkapacitásokat tartanak fenn, amelyek biztosítják az üzleti igények ellátásához elégséges és megfelelő erőforrásokat, képességeket és funkciókat.

(5) A 2. cikk (1) bekezdésének f) pontjában említett pénzügyi szervezetek fenntartanak, illetve gondoskodnak arról, hogy harmadik félnek minősülő IKT-szolgáltatóik fenntartsanak legalább egy másodlagos adatfeldolgozó helyszínt, amely rendelkezik az üzleti igényeik ellátásához elégséges és megfelelő erőforrásokkal, képességekkel, funkciókkal és személyi feltételekkel.

A másodlagos adatfeldolgozási helyszín:

a) olyan földrajzi távolságra helyezkedik el az elsődleges adatfeldolgozási helyszíntől, amely biztosítja attól eltérő kockázati profilját, valamint mentességét az elsődleges helyszínt érintő esemény hatásától;

b) képes biztosítani a kulcsfontosságú szolgáltatásoknak az elsődleges helyszínnel azonos folytonosságát, vagy az ahhoz szükséges szolgáltatási szintet, hogy a pénzügyi szervezet kulcsfontosságú működési folyamatai teljesítsék a helyreállítási célkitűzéseket;

c) azonnal elérhető a pénzügyi szervezet személyi állománya számára, ezáltal biztosítja a kulcsfontosságú szolgáltatások folytonosságát, ha az elsődleges adatfeldolgozási helyszín elérhetetlenné vált.

(6) Az egyes funkciókhoz kapcsolódó helyreállítási időre és pontra vonatkozó célkitűzések megállapításakor a pénzügyi szervezetek figyelembe veszik a piaci hatékonyságra potenciálisan gyakorolt általános hatást. Az időre vonatkozó célkitűzések biztosítják a megállapodás szerinti szolgáltatási szintek teljesítését rendkívüli helyzetekben.

(7) IKT-vonatkozású biztonsági eseményt követő helyreállítás során a pénzügyi szervezetek többszörös ellenőrzés, ezen belül adategyeztetés útján biztosítják az adatok legmagasabb szintű integritását. A szervezetek külső érdekelti forrásból rekonstruált adatok esetében is elvégzik ezeket az ellenőrzéseket, hogy biztosítsák a teljes adatállomány rendszerek közötti egységét.

12. cikk

Tanulás és alkalmazkodás

(1) A pénzügyi szervezetek a méretüknek és üzleti, kockázati profiljuknak megfelelő képességekkel és személyi állománnyal rendelkeznek ahhoz, hogy információt gyűjtsenek a sebezhetőségekről és kiberfenyegetésekről, az IKT-vonatkozású biztonsági eseményekről, ezen belül a kibertámadásokról, és elemezzék azok valószínű hatását a szervezet digitális működési rezilienciájára.

(2) A pénzügyi szervezetek az alaptevékenységeiket érintő IKT-zavarokat okozó IKT-vonatkozású biztonsági eseményeket követő felülvizsgálat keretében elemzik a zavar okait, és megállapítják az IKT-műveletekben vagy a 10. cikkben említett IKT-vonatkozású üzletmenet-folytonossági szabályokban szükséges javításokat.

A mikrovállalkozásnak nem minősülő pénzügyi szervezetek a végrehajtott változtatásokat bejelentik az illetékes hatóságoknak.

Az első albekezdésben említett, IKT-vonatkozású biztonsági eseményeket követő felülvizsgálat az alábbiak kapcsán megállapítja, hogy a kialakított eljárásokat követték-e, és a megtett intézkedések eredményesek voltak-e:

a) gyors reagálás a biztonsági riasztásokra, az IKT-vonatkozású biztonsági események hatásának és súlyosságának gyors megállapítása;

b) 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 23. és 24. cikkel összhangban végzett teszteléséből, a valós IKT-vonatkozású biztonsági eseményekből, ezen belül különösen a kibertámadásokból, továbbá az üzletmenet-folytonossági és helyreállítási tervek aktiválása során felmerült kihívásokból, valamint a partnerekkel cserélt és a felügyeleti felülvizsgálatok során felülvizsgált információkból származó tapasztalatokat a szervezet megfelelően beépíti az IKT-kockázatértékelés folyamatába. A megállapításokat figyelembe kell venni az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer vonatkozó összetevőinek felülvizsgálata során.

(4) A pénzügyi szervezetek nyomon követik az 5. cikk (9) bekezdésében meghatározott, digitális rezilienciára vonatkozó stratégiájuk végrehajtásának eredményességét. Feltérképezik az IKT-kockázatok időbeli alakulását, elemzik az IKT-vonatkozású biztonsági események, különösen a kibertámadások gyakoriságát, típusait, nagyságát, alakulását és mintázatait az IKT-kockázati kitettség mértékének megállapítása, valamint a pénzügyi szervezet kiberbiztonsági érettségének, felkészültségének javítása céljából.

(5) A vezető IKT-munkatársak legalább évente beszámolnak a vezető testületnek a (3) bekezdésben említett megállapításokról, és javaslatokat terjesztenek elő.

(6) A pénzügyi szervezetek IKT-biztonsági tudatosságot elősegítő programokat és a digitális működési rezilienciával kapcsolatos képzéseket dolgoznak ki személyi állományuk képzési rendszerének kötelező moduljaként. Ezeket minden munkavállalónak és a felső vezetés minden tagjának el kell végeznie.

A pénzügyi szervezetek folyamatosan nyomon követik 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. A legkorszerűbb IKT-kockázatkezelési folyamatokkal lépést tartva eredményesen lépnek fel a kibertámadások meglévő és új formáival szemben.

13. cikk

Kommunikáció

(1) Az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek kommunikációs tervvel rendelkeznek, amely lehetővé teszi az ügyfelek, partnerek, valamint adott esetben a nyilvánosság felelős tájékoztatását az IKT-vonatkozású biztonsági eseményekről és a jelentős sebezhetőségekről.

(2) Az 5. cikk (1) bekezdésében említett IKT-kockázatkezelési keretrendszer részeként a pénzügyi szervezetek saját személyi állományukra és a külső érdekeltekre vonatkozó

kommunikációs szabályzatot vezetnek be. A személyi állományra vonatkozó kommunikációs szabályzat figyelembe veszi, hogy különbséget kell tenni az IKT-kockázatkezelésben, ezen belül különösen az elhárításban és helyreállításban részt vevő munkatársak, valamint a tájékoztatást igénylő munkatársak között.

(3) A szervezeten belül legalább egy személy feladata az IKT-vonatkozású biztonsági eseményekre vonatkozó kommunikációs stratégia végrehajtása, aki ennek során a nyilvános és médiaszóvivő szerepét is betölti.

14. cikk

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

Az Európai Bankhatóság (EBH), az Európai Értékpapírpiaci Hatóság (ESMA) és az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság (EIOPA) az Európai Uniós Kiberbiztonsági Ügynökséggel (ENISA) egyeztetve szabályozástechnikai standardtervezeteket dolgoz ki, amelyek keretében:

a) meghatározzák azokat a további elemeket, amelyeket a 8. cikk (2) bekezdésében említett IKT-biztonsági szabályzatoknak, eljárásoknak, protokolloknak és eszközöknek tartalmazniuk kell a hálózatbiztonság, a behatolás és az adatokkal való visszaélés elleni megfelelő védelem, az adatok hitelességének és integritásának többek között kriptográfiai technikákkal történő megóvása, továbbá a garantáltan pontos és gyors, jelentős zavaroktól mentes adattovábbítás érdekében;

b) előírják, hogy a 8. cikk (2) bekezdésében említett IKT-biztonsági szabályzatok, eljárások és eszközök útján miként kapjanak helyet biztonsági kontrollok a rendszerekben a fejlesztés kezdetétől (beépített biztonság), lehetővé teszik a változó fenyegetettségi helyzethez való alkalmazkodást, továbbá előírják a mélységben tagolt védelmi technológia alkalmazását;

c) részletesebben meghatározzák a 8. cikk (4) bekezdésének b) pontjában említett megfelelő technikákat, módszereket és protokollokat;

d) kidolgozzák a felhasználói jogosultságokra vonatkozó, a 8. cikk (4) bekezdésének c) pontjában említett kontrollok további összetevőit, valamint az ezekhez kapcsolódó humánerőforrás-politikát, amely meghatározza a hozzáférési jogosultságokat, a jogosultságok kiosztására és visszavonására vonatkozó eljárásokat, valamint az IKT-kockázatokkal összefüggő rendellenes magatartásformák megfelelő (többek között hálózathasználati mintákra, időbeosztásra, IT-tevékenységekre, ismeretlen eszközökre vonatkozó) mutatók alapján történő nyomon követését;

e) részletesen kidolgozzák a 9. cikk (1) bekezdésében említett, a rendellenes tevékenységek azonnali észlelésére szolgáló elemeket, valamint azokat a 9. cikk (2) bekezdésében említett kritériumokat, amelyek kiváltják az IKT-vonatkozású biztonsági események észlelési és válaszfolyamatait;

f) részletesen meghatározzák a 10. cikk (1) bekezdésében említett IKT-vonatkozású üzletmenet-folytonossági szabályok összetevőit;

g) részletesen meghatározzák az IKT-vonatkozású üzletmenet-folytonossági tervek 10. cikk (5) bekezdésében említett tesztelését, hogy annak során kellő figyelmet kapjanak az olyan helyzetek, amikor egy kulcsfontosságú vagy

lényeges funkció ellátása elfogadhatatlan színvonalon történik vagy meghiúsul, emellett figyelmet kapjanak a harmadik félnek minősülő IKT-szolgáltatók fizetésképtelenség vagy egyéb ok miatti megszűnésének potenciális hatásai, valamint adott esetben az érintett szolgáltatók joghatósági területén fennálló politikai kockázatok;

h) részletesen meghatározzák a 10. cikk (3) bekezdésében említett IKT-vonatkozású katasztrófa utáni helyreállítási terv összetevőit.

Az említett szabályozástechnikai standardtervezeteket az EBA, az ESMA és az EIOPA [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtja a Bizottságnak.

A Bizottság felhatalmazást kap az első albekezdésben említett szabályozástechnikai standardtervezeteknek az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 10–14. cikkével összhangban történő elfogadására.

III. FEJEZET

AZ IKT-VONATKOZÁSÚ BIZTONSÁGI ESEMÉNYEK KEZELÉSE, OSZTÁLYOZÁSA, BEJELENTÉSE

15. cikk

Az IKT-vonatkozású biztonsági események kezelési folyamata

(1) A pénzügyi szervezetek kialakítják és végrehajtják az IKT-vonatkozású biztonsági események észlelésére, kezelésére és bejelentésére szolgáló folyamatot, ezenkívül riasztási célból korai előrejelző mutatókat vezetnek be.

(2) A pénzügyi szervezetek megfelelő folyamatok kialakításával biztosítják az IKT-vonatkozású biztonsági események következetes és integrált nyomon követését, kezelését és utókövetését az ilyen eseményeket kiváltó okoknak az előfordulás megelőzését célzó feltárása és megszüntetése érdekében.

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

a) a 16. cikk (1) bekezdésében említett kritériumok alapján meghatározza az IKT-vonatkozású biztonsági események azonosítását, nyomon követését, naplózását és osztályozását biztosító, az események prioritásának, súlyosságának és az érintett szolgáltatások kritikus mivoltának megfelelő eljárásokat;

b) kijelöli azokat a szerep- és felelősségi köröket, amelyeket az IKT-vonatkozású biztonsági események egyes típusaival és forgatókönyveivel összefüggésben aktiválni kell;

c) meghatározza a személyi állománnyal, a külső érdekelt felekkel és a médiával a 13. cikkel összhangban folytatott kommunikációra, az ügyfelek értesítésére, a belső eszkalációs eljárásokra, beleértve az IKT-vonatkozású ügyfélpanaszok kezelését is, továbbá adott esetben a partner pénzügyi szervezetek tájékoztatására vonatkozó terveket;

d) biztosítja a felső vezetés és a vezető testület tájékoztatását a jelentős IKT-vonatkozású biztonsági eseményekről, amely ismerteti az események hatását, a

megtett válaszlépéseket, valamint azokat a további kontrollokat, amelyeket az IKT-vonatkozású biztonsági események következtében ki kell alakítani;

e) meghatározza az IKT-vonatkozású biztonsági események elhárítására irányuló eljárásokat, amelyek célja a hatások enyhítése, valamint a szolgáltatások működésének és biztonságának mielőbbi helyreállítása.

16. cikk

Az IKT-vonatkozású biztonsági események osztályozása

(1) A pénzügyi szervezetek az alábbi kritériumok alapján osztályozzák az IKT-vonatkozású biztonsági eseményeket, és állapítják meg azok hatását:

a) az IKT-vonatkozású biztonsági esemény által előidézett zavarral érintett felhasználók vagy pénzügyi szerződő felek száma, és az, hogy az IKT-vonatkozású biztonsági eseménynek van-e a hírnevet érintő hatása;

b) az IKT-vonatkozású biztonsági esemény időtartama, beleértve a leállást is;

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

d) az IKT-vonatkozású biztonsági eseménnyel járó adatvesztés jellege, például az integritás, a bizalmas jelleg vagy a rendelkezésre állás sérülése;

e) az IKT-vonatkozású biztonsági esemény által a szervezet IKT-rendszereire gyakorolt hatás súlyossága;

f) az érintett szolgáltatások kritikus mivolta, beleértve a pénzügyi szervezet ügyleteit és működését is;

g) az IKT-vonatkozású biztonsági esemény abszolút és relatív gazdasági hatása.

(2) Az európai felügyeleti hatóságok a vegyes bizottság keretében, az Európai Központi Bankkal (EKB) és az ENISA-val folytatott konzultációt követően közös szabályozástechnikai standardtervezeteket dolgoznak ki, amelyek részletesen meghatározzák az alábbiakat:

a) az (1) bekezdésben említett kritériumok, ezen belül azok a lényegességi küszöbértékek, amelyek alapján megállapíthatók a 17. cikk (1) bekezdésében előírt bejelentési kötelezettség alá tartozó jelentős IKT-vonatkozású biztonsági események;

b) azon kritériumok, amelyek alapján az illetékes hatóságok értékelik a jelentős IKT-vonatkozású biztonsági események relevanciáját a többi tagállam joghatósági területe szempontjából, továbbá az IKT-vonatkozású biztonsági eseményekkel kapcsolatos bejelentések azon részletei, amelyeket a 17. cikk (5) és (6) bekezdésének megfelelően meg kell osztaniuk a többi illetékes hatósággal.

(3) A (2) bekezdésben említett közös szabályozástechnikai standardtervezetek kidolgozása során az EFH-k figyelembe veszik a nemzetközi szabványokat, valamint az ENISA által kidolgozott és közzétett specifikációkat, adott esetben más gazdasági ágazatokra vonatkozóan is.

Az említett közös szabályozástechnikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak.

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 10–14. cikkével összhangban a (2) bekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

17. cikk

A jelentős IKT-vonatkozású biztonsági események bejelentése

(1) A pénzügyi szervezetek a jelentős IKT-vonatkozású biztonsági eseményeket a (3) bekezdésben előírt határidőkön belül bejelentik a 41. cikkben említett illetékes hatóságnak.

Az első albekezdés alkalmazásában a pénzügyi szervezetek a releváns információk összegyűjtését és elemzését követően a 18. cikkben említett mintadokumentum felhasználásával jelentést készítenek az eseményről, amelyet benyújtanak az illetékes hatóságnak.

A jelentés magában foglal minden olyan információt, amelyre az illetékes hatóságnak szüksége van a jelentős IKT-vonatkozású biztonsági esemény mértékének megállapításához és határokon átnyúló hatásainak értékeléséhez.

(2) Ha a jelentős IKT-vonatkozású biztonsági esemény hatással van vagy lehet a szolgáltatást használók és az ügyfelek pénzügyi érdekeire, a pénzügyi szervezetek haladéktalanul tájékoztatják a szolgáltatásaikat használókat és ügyfeleiket a jelentős IKT-vonatkozású biztonsági eseményről, továbbá a lehető leghamarabb tájékoztatják őket az esemény káros hatásainak enyhítésére tett intézkedésekről.

(3) A pénzügyi szervezetek a következőket nyújtják be a 41. cikkben említett illetékes hatóságnak:

a) előzetes bejelentés haladéktalanul, de legkésőbb a munkanap végéig, illetve a munkanap végét megelőző 2 órán belül bekövetkezett jelentős IKT-vonatkozású biztonsági esemény kapcsán a következő munkanap kezdetétől számított 4 órán belül, vagy ha a bejelentési csatornák nem elérhetők, akkor amint elérhetővé válnak;

b) időközi jelentés az a) pontban említett előzetes bejelentést követő egy héten belül, releváns állapotfrissítés esetén és az illetékes hatóság erre irányuló kérésére a bejelentés aktualizálásával;

c) zárójelentés – függetlenül attól, hogy korrekciós intézkedések végrehajtására sor került-e – a kiváltó okok elemzését követően, ha a hatással kapcsolatban a becslések helyettesítésére alkalmas tényadatok rendelkezésre állnak, de legkésőbb az előzetes bejelentés elküldését követően egy hónappal.

(4) A pénzügyi szervezetek az e cikk szerinti bejelentési kötelezettségeket csak a 41. cikkben említett illetékes hatóság jóváhagyásával ruházhatják át harmadik félnek minősülő szolgáltatóra.

(5) Az (1) bekezdésben említett jelentés átvételét követően az illetékes hatóság haladéktalanul tájékoztatja az esemény részleteiről:

a) a helyzetnek megfelelően az EBH-t, az ESMA-t vagy az EIOPA-t;

b) a 2. cikk (1) bekezdésének a), b) és c) pontjában említett pénzügyi szervezetek esetében az EKB-t, ha ez indokolt; valamint

c) az (EU) 2016/1148 irányelv 8. cikke szerint kijelölt egyedüli kapcsolattartó pontot.

(6) Az EBH, az ESMA, illetve az EIOPA, valamint az EKB értékeli a jelentős IKT-vonatkozású biztonsági esemény relevanciáját a többi érintett illetékes hatóság szempontjából, és azokat ennek megfelelően a lehető legkorábbi időpontban értesíti. Az EKB értesítést küld a Központi Bankok Európai Rendszere tagjainak a fizetési rendszer szempontjából releváns kérdésekről. Az értesítés alapján az illetékes hatóságok adott esetben meghoznak minden szükséges intézkedést a pénzügyi rendszer közvetlen stabilitásának megóvása érdekében.

18. cikk

A jelentéstartalom és a mintadokumentumok harmonizációja

(1) Az európai felügyeleti hatóságok a vegyes bizottság keretében, az ENISA-val és az EKB-val folytatott konzultációt követően kidolgozzák az alábbiakat:

a) közös szabályozástechnikai standardtervezetek, amelyek:

1. megállapítják a jelentős IKT-vonatkozású biztonsági eseményekkel kapcsolatos bejelentések tartalmát;

2. részletesen meghatározzák azokat a feltételeket, amelyekkel a pénzügyi szervezetek az illetékes hatóság jóváhagyásával harmadik félnek minősülő szolgáltatóra ruházhatják az e fejezetben előírt bejelentési kötelezettségeket;

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

Az EFH-k az (1) bekezdés a) pontjában említett közös szabályozástechnikai standardtervezeteket és az (1) bekezdés b) pontjában említett közös végrehajtás-technikai standardtervezeteket [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak.

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

A Bizottság felhatalmazást kap arra, hogy az 1093/2010/EU, az 1095/2010/EU és az 1094/2010/EU rendelet 15. cikkével összhangban elfogadja az (1) bekezdés b) pontjában említett közös végrehajtás-technikai standardokat.

19. cikk

A jelentős IKT-vonatkozású biztonsági események központosított bejelentése

(1) Az EFH-k a vegyes bizottság keretében, az EKB-val és az ENISA-val folytatott konzultációt követően közös jelentésben értékelik annak lehetőségét, hogy az eseménybejelentést még nagyobb mértékben központosítsák olyan egységes uniós

központi adatbázis létrehozásával, amelynek segítségével a pénzügyi szervezetek bejelenthetik a jelentős IKT-vonatkozású biztonsági eseményeket. A jelentés megvizsgálja, hogy a felügyeleti konvergencia növelése érdekében milyen lehetőségek vannak az IKT-vonatkozású biztonsági események bejelentésével kapcsolatos információáramlás megkönnyítésére, a járulékos költségek csökkentésére, valamint a tematikus elemzések megalapozására.

(2) Az (1) bekezdésben említett jelentés legalább a következő elemeket foglalja magában:

a) az uniós adatbázis létrehozásának előfeltételei;

b) az előnyök, a korlátok és a lehetséges kockázatok;

c) az üzemeltetési igazgatás elemei;

d) a tagság feltételei;

e) az uniós adatbázishoz való hozzáférés módozatai a pénzügyi szervezetek és az illetékes nemzeti hatóságok számára;

f) az uniós adatbázist támogató működési platform kialakításával, ezen belül a szükséges szakértelem biztosításával összefüggésben felmerülő pénzügyi költségek előzetes értékelése.

(3) Az EFH-k az (1) bekezdésben említett jelentést [*Kiadóhivatal: kérjük, illessze be a dátumot: 3 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak, az Európai Parlamentnek és a Tanácsnak.

20. cikk

Felügyeleti visszajelzés

(1) A 17. cikk (1) bekezdésében említett jelentés átvételekor az illetékes hatóság visszaigazolja a bejelentés fogadását, és a lehető leghamarabb ellátja a pénzügyi szervezetet a szükséges visszajelzéssel és iránymutatásokkal, különösen a szervezeti szintű korrekciós intézkedésekre, valamint a több ágazatot érintő káros hatások enyhítésének módjaira vonatkozóan.

(2) Az EFH-k a vegyes bizottság keretében anonimizált és összesített formában éves beszámolót készítenek az IKT-vonatkozású biztonsági eseményekkel kapcsolatban az illetékes hatóságoktól kapott bejelentésekről, amely közli legalább a jelentős IKT-vonatkozású biztonsági események számát és jellegét, a pénzügyi szervezetek működésére és az ügyfelekre gyakorolt hatását, költségeit, valamint a megtett korrekciós intézkedéseket.

Az EFH-k figyelmeztetések kiadásával és magas szintű statisztikák készítésével hozzájárulnak az IKT-fenyegetések és -sebezhetőségek értékeléséhez.

IV. FEJEZET

A DIGITÁLIS MŰKÖDÉSI REZILIENCIA TESZTELÉSE

21. cikk

A digitális működési reziliencia tesztelésének végrehajtására vonatkozó általános követelmények

(1) Az IKT-vonatkozású biztonsági eseményekre való felkészültség értékelése, a digitális működési reziliencia gyenge pontjainak és hiányosságainak azonosítása, valamint a korrekciós intézkedések gyors végrehajtása érdekében a pénzügyi szervezetek a méretük és üzleti, kockázati profiljuk kellő figyelembevételével megalapozott és átfogó programot alakítanak ki a digitális működési reziliencia tesztelésére az 5. cikkben említett IKT-kockázatkezelési keretrendszer szerves részeként.

(2) A digitális működési reziliencia tesztelését szolgáló program magában foglalja a 22. és 23. cikk rendelkezéseivel összhangban alkalmazandó értékeléseket, teszteket, módszertanokat, gyakorlatokat és eszközöket.

(3) A pénzügyi szervezetek az (1) bekezdésben említett, a digitális működési reziliencia tesztelését szolgáló program végrehajtásakor kockázatalapú megközelítést alkalmaznak, amelynek keretében figyelembe veszik az IKT-kockázatok alakulását, a pénzügyi szervezetet ténylegesen vagy potenciálisan érintő konkrét kockázatokat, az információs eszközök és nyújtott szolgáltatások fontosságát, valamint azokat az egyéb tényezőket, amelyeket a pénzügyi szervezet indokoltnak tart.

(4) A pénzügyi szervezetek biztosítják, hogy a tesztet független belső vagy külső fél hajtsa végre.

(5) A pénzügyi szervezetek eljárásokat és szabályzatokat alakítanak ki a tesztek végrehajtása során feltárt problémák rangsorolása, osztályozása és elhárítása céljából, továbbá kialakítják azokat a belső validálási módszertanokat, amelyekkel megerősíthető, hogy a szervezet teljeskörűen kezelte a feltárt gyenge pontokat és hiányosságokat.

(6) A pénzügyi szervezetek legalább évente tesztelik valamennyi kulcsfontosságú IKT-rendszerüket és alkalmazásukat.

22. cikk

Az IKT-eszközök és -rendszerek tesztelése

(1) A 21. cikkben említett, a digitális működési reziliencia tesztelését szolgáló program biztosítja a megfelelő tesztek teljes körének, ezen belül a sebezhetőségi értékelések és vizsgálatok, nyílt forrású elemzések, hálózatbiztonsági értékelések, hiányelemzések, fizikai biztonsági felülvizsgálatok, kérdőívek, szoftveres megoldások vizsgálata, lehetőség szerint forráskódvizsgálatok, forgatókönyv-alapú tesztek, kompatibilitásvizsgálat, teljesítményvizsgálat, valamint a végpontok közötti tesztek vagy behatolási tesztek végrehajtását.

(2) A 2. cikk (1) bekezdésének f) és g) pontjában említett pénzügyi szervezetek a pénzügyi szervezet kulcsfontosságú funkcióit, alkalmazásait és infrastrukturális

összetevőit támogató új vagy meglévő szolgáltatások elindítása vagy újraindítása előtt sebezhetőségi értékelést végeznek.

23. cikk

Az IKT-eszközök, -rendszerek és - folyamatok fejlett módszerekkel végzett, fenyegetettségi szempontú behatolási tesztelése

(1) A (4) bekezdéssel összhangban azonosított pénzügyi szervezetek legalább háromévente fejlett módszerekkel végzett, fenyegetettségi szempontú behatolási tesztet hajtanak végre.

(2) A fenyegetettségi szempontú behatolási tesztelés kiterjed legalább a pénzügyi szervezet kulcsfontosságú funkcióira és szolgáltatásaira, végrehajtása az e funkciókat támogató éles rendszereken történik. A fenyegetettségi szempontú behatolási tesztelés pontos terjedelmét a kulcsfontosságú funkciók és szolgáltatások értékelése alapján a pénzügyi szervezetek határozzák meg, és az illetékes hatóságok validálják.

Az első albekezdés alkalmazásában a pénzügyi szervezetek a harmadik félnek minősülő IKT-szolgáltatóhoz kiszervezett vagy annak megbízásba adott funkciókra és szolgáltatásokra is kiterjedően azonosítják a kulcsfontosságú funkciókat és szolgáltatásokat támogató releváns IKT-folyamatokat, -rendszereket és -technológiákat.

Ha a fenyegetettségi szempontú behatolási tesztelés harmadik félnek minősülő IKT-szolgáltatókat is érint, a pénzügyi szervezet megteszi az e szolgáltatók közreműködéséhez szükséges intézkedéseket.

A pénzügyi szervezetek eredményes kockázatkezelési kontrollok útján mérsékelik az adatokat érő hatás, az eszközökben keletkező kár és a kulcsfontosságú szolgáltatások, tevékenységek zavarának kockázatát magánál a pénzügyi szervezetnél, annak partnereinél, valamint a pénzügyi ágazat egészében.

A teszt befejezésekor, a jelentések és korrekciós tervek jóváhagyását követően a pénzügyi szervezet a külső tesztelőkkel közösen átadja az illetékes hatóságnak a fenyegetettségi szempontú behatolási tesztelés követelményeknek megfelelő elvégzését igazoló dokumentációt. Az illetékes hatóságok a dokumentáció validálását követően igazolást adnak ki.

(3) A pénzügyi szervezetek a 24. cikknek megfelelően kötnek szerződést a tesztelőkkel a fenyegetettségi szempontú behatolási tesztelés elvégzésére.

Az illetékes hatóságok a következők értékelése alapján választják ki azokat a pénzügyi szervezeteket, amelyeknek a méretükkel, tevékenységük jellegével és mértékével, valamint általános kockázati profiljukkal arányos módon fenyegetettségi szempontú behatolási tesztelést kell végezniük:

a) hatáshoz kapcsolódó tényezők, különösen a pénzügyi szervezet által nyújtott szolgáltatások és végzett tevékenységek kritikus mivolta;

b) esetleges pénzügyi stabilitási megfontolások, ideértve a pénzügyi szervezet nemzeti, illetve uniós léptékű rendszerszintű jellegét;

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

(4) Az EBH, az ESMA és az EIOPA az EKB-val folytatott konzultációt követően, az információkon alapuló behatolási tesztekre vonatkozó uniós keretek

figyelembevételével szabályozástechnikai standardtervezeteket dolgoz ki, amelyek részletesen meghatározzák:

a) az e cikk (6) bekezdése alkalmazásában vizsgált kritériumokat;

b) az alábbiakra vonatkozó követelményeket:

(a) az e cikk (2) bekezdésében említett, fenyegetettségi szempontú behatolási tesztelés terjedelme;

(b) a tesztelési folyamat egyes szakaszaiban követendő tesztelési módszertan és megközelítés;

(c) a tesztelés eredményei, lezárása és korrekciós szakaszai;

c) a több tagállamban működő pénzügyi szervezeteknél végrehajtott, fenyegetettségi szempontú behatolási teszteléssel összefüggő felügyeleti együttműködés típusa a megfelelő szintű felügyeleti részvétel, valamint a pénzügyi alágazatok, illetve a helyi pénzügyi piacok sajátos igényeihez igazodó, rugalmas végrehajtás biztosítása érdekében.

Az említett közös szabályozástechnikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 2 hónappal a hatálybalépést megelőzően*]-jéig/-ig benyújtják a Bizottságnak.

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

24. cikk

A tesztelőkre vonatkozó követelmények

(1) A pénzügyi szervezetek a fenyegetettségi szempontú behatolási tesztelés végrehajtása céljából csak olyan tesztelőt vehetnek igénybe, amely:

a) a feladatra a leginkább alkalmas, és jó szakmai hírnévvel rendelkezik;

b) rendelkezik a megfelelő technikai és szervezeti képességekkel, valamint speciális szakértelemmel a fenyegetettségi információkon alapuló, a behatolási, illetve az érdekütköztetéses elemzőcsoport által végzett tesztelés terén;

c) rendelkezik a tagállamok valamelyikében működő akkreditációs testület tanúsításával, vagy formális magatartási kódex vagy etikai keretrendszer alapján végzi tevékenységét;

d) külső tesztelő esetén független bizonyossági vagy ellenőrzési jelentéssel tudja igazolni a fenyegetettségi szempontú behatolási tesztelés megbízható végrehajtását, ideértve a pénzügyi szervezet bizalmas adatainak megfelelő védelmét és a pénzügyi szervezet üzleti kockázataival kapcsolatos jogorvoslatot is;

e) külső tesztelő esetén megfelelő és teljes körű szakmai felelősségbiztosítással rendelkezik, amely kiterjed a szakmai kötelezettség elmulasztására és a gondatlanságra is.

(2) A pénzügyi szervezetek biztosítják, hogy a külső tesztelőkkel kötött megállapodások előírják a fenyegetettségi szempontú behatolási tesztelés eredményeinek megfelelő

kezelését, továbbá azt, hogy az adatkezelés, ezen belül az adatok előállítása, előkészítése, tárolása, összesítése, 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 MEGFELELŐ KEZELÉSÉNEK ALAPELVEI

25. cikk

Általános elvek

A pénzügyi szervezetek a harmadik féltől eredő IKT-kockázatot IKT-kockázatkezelési keretrendszerükön belül, az IKT-kockázat szerves részeként kezelik az alábbi elvekkel összhangban:

(1) Azok a pénzügyi szervezetek, amelyek üzleti tevékenységük folytatásához IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodást kötöttek, mindenkor teljes felelősséggel tartoznak az e rendeletben és az egyéb alkalmazandó, pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt kötelezettségek teljesítéséért.

(2) A pénzügyi szervezetek a harmadik féltől eredő IKT-kockázat kezelését az arányosság elvének megfelelően, az alábbiak figyelembevételével valósítják meg:

a) az IKT-vonatkozású függőségek nagyságrendje, összetettsége és jelentősége;

b) a harmadik félnek minősülő IKT-szolgáltatókkal kötött, IKT-szolgáltatások igénybevételéről szóló szerződéses megállapodásokból eredő kockázatok, tekintettel az adott szolgáltatás, folyamat vagy funkció kritikus mivoltára vagy lényegességére, valamint arra a hatásra, amely a pénzügyi szolgáltatások és tevékenységek folytonosságát és minőségét érheti az egyedi szervezet és a vállalatcsoport szintjén.

(3) IKT-kockázatkezelési keretrendszerük részeként a pénzügyi szervezetek az 5. cikk (9) bekezdésének g) pontjában említett, több beszállítóra épülő stratégia figyelembevételével a harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát fogadnak el, amelyet rendszeresen felülvizsgálnak. A stratégia, amelyet az egyedi szervezet szintjén, valamint adott esetben szubkonszolidált és konszolidált alapon is alkalmazni kell, magában foglalja a harmadik félnek minősülő IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételére vonatkozó szabályzatot. A vezető testület rendszeresen felülvizsgálja a kulcsfontosságú vagy lényeges funkciók kiszervezése kapcsán azonosított kockázatokat.

(4) IKT-kockázatkezelési keretrendszerük részeként a pénzügyi szervezetek az egyedi szervezet szintjén, valamint szubkonszolidált és konszolidált szinten információ-

nyilvántartást vezetnek a harmadik félnek minősülő IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodásokról.

Az első albekezdésben említett szerződéses megállapodásokat megfelelően dokumentálni kell, megkülönböztetve a kulcsfontosságú vagy lényeges funkciókat érintő és az ilyen funkciót nem érintő megállapodásokat.

A pénzügyi szervezetek legalább évente tájékoztatják az illetékes hatóságokat az IKT-szolgáltatások igénybevételére irányuló új megállapodások számáról, a harmadik félnek minősülő IKT-szolgáltatók kategóriáiról, a szerződéses megállapodások típusairól, valamint a nyújtott szolgáltatásokról és funkciókról.

A pénzügyi szervezetek kérésre az illetékes hatóság rendelkezésére bocsátják a teljes információ-nyilvántartást, illetve a kérésnek megfelelően annak meghatározott részeit, valamint a pénzügyi szervezet eredményes felügyeletéhez szükséges információkat.

A pénzügyi szervezetek időben tájékoztatják az illetékes hatóságot a kulcsfontosságú vagy lényeges funkciók tervezett szerződéses megbízásba adásáról, valamint arról, ha egy funkció kulcsfontosságúvá vagy lényegessé válik.

(5) Az IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodások megkötése előtt a pénzügyi szervezetek:

a) értékelik, hogy a szerződéses megállapodás érint-e kulcsfontosságú vagy lényeges funkciót;

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

c) azonosítják és értékelik a szerződéses megállapodással összefüggő releváns kockázatokat, beleértve annak lehetőségét is, hogy a szerződéses megállapodás hozzájárulhat az IKT-koncentrációs kockázat erősödéséhez;

d) elvégzik a leendő harmadik félnek minősülő IKT-szolgáltató teljes körű átvilágítását, továbbá a kiválasztási és értékelési folyamatok során meggyőződnek a harmadik félnek minősülő IKT-szolgáltató alkalmasságáról;

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

(6) A pénzügyi szervezetek csak azokkal a harmadik félnek minősülő IKT-szolgáltatókkal köthetnek szerződéses megállapodást, amelyek megfelelnek a rájuk vonatkozó mindenkori szigorú információbiztonsági szabványoknak.

(7) A harmadik félnek minősülő IKT-szolgáltató kapcsán a hozzáférési, vizsgálati és ellenőrzési jogok gyakorlásakor a pénzügyi szervezetek kockázatalapú megközelítéssel előzetesen megállapítják az ellenőrzések és vizsgálatok gyakoriságát, valamint azokat a területeket, amelyeket az általánosan elfogadott ellenőrzési standardoknak és az ellenőrzési standardok alkalmazására és beépítésére vonatkozó felügyeleti utasításnak megfelelően ellenőrizni szükséges.

A nagy fokú technológiai összetettségű szerződéses megállapodások esetében a pénzügyi szervezet meggyőződik arról, hogy az ellenőrök – attól függetlenül, hogy belső ellenőrről, ellenőrök csoportjáról vagy külső ellenőrről van szó – rendelkeznek-e az adott ellenőrzések és értékelések eredményes elvégzéséhez szükséges készségekkel és ismeretekkel.

(8) A pénzügyi szervezetek intézkednek az IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodások megszüntetéséről legalább az alábbi körülmények fennállása esetén:

a) a harmadik félnek minősülő IKT-szolgáltató nem tartja be az alkalmazandó jogszabályi, hatósági és szerződéses rendelkezéseket;

b) a harmadik féltől eredő IKT-kockázat nyomon követése olyan körülményeket tár fel, amelyek alkalmasnak tekinthetők arra, hogy befolyásolják a szerződéses megállapodás keretében ellátott funkciók teljesítését, ideértve a megállapodást vagy a harmadik félnek minősülő IKT-szolgáltató helyzetét érintő jelentős módosításokat is;

c) bizonyíthatóan gyenge pontok találhatók a harmadik félnek minősülő IKT-szolgáltató általános IKT-kockázatkezelésében, ezen belül különösen a bizalmas, személyes vagy egyébként érzékeny, nem személyes adatok biztonságát és integritását biztosító módszereiben;

d) az adott szerződéses megállapodás olyan körülményeket eredményez, amelyek között az illetékes hatóság nem tudja eredményesen ellátni a pénzügyi szervezet felügyeletét.

(9) A pénzügyi szervezetek kilépési stratégiák útján fedezik a harmadik félnek minősülő IKT-szolgáltató szintjén esetlegesen felmerülő kockázatokat, így különösen a szolgáltató megszűnését, a nyújtott funkciók minőségének romlását, a szolgáltatások nem megfelelő nyújtása vagy meghiúsulása miatti üzleti zavart, valamint a funkció megfelelő és folyamatos ellátásával összefüggésben felmerülő lényeges kockázatokat.

A pénzügyi szervezetek gondoskodnak arról, hogy képesek legyenek anélkül kilépni a szerződéses megállapodásokból, 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, és azokat dokumentálni, valamint adott esetben megfelelően tesztelni kell.

A pénzügyi szervezetek alternatív megoldásokat határoznak meg és átállási terveket dolgoznak ki, amelyek segítségével a szerződéses megbízásba adott funkciókat és a releváns adatokat leválaszthatják a harmadik félnek minősülő IKT-szolgáltatótól, és azokat biztonságosan és sértetlenségük megőrzésével alternatív szolgáltatókhoz telepíthetik, vagy visszaszervezhetik a saját működésükbe.

A pénzügyi szervezetek megfelelő rendkívüli intézkedésekkel biztosítják az üzletmenet folytonosságát az első albekezdésben említett valamennyi körülmény esetén.

(10) Az EFH-k a vegyes bizottság keretében közös végrehajtás-technikai standardtervezeteket dolgoznak ki, amelyek meghatározzák a (4) bekezdésben említett információ-nyilvántartásban alkalmazandó mintadokumentumokat.

Az említett végrehajtás-technikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak.

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

(11) Az EFH-k a vegyes bizottság keretében szabályozástechnikai standardtervezeteket dolgoznak ki, amelyek részletesen meghatározzák:

a) a (3) bekezdésben említett szabályzat tartalmi elemeit a harmadik félnek minősülő IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodások kapcsán, megemlítve az adott megállapodások életciklusának fő szakaszait;

b) a (4) bekezdésben említett információ-nyilvántartásban szerepeltetendő információtípusokat.

Az említett szabályozástechnikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak.

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

26. cikk

Az IKT-koncentrációs kockázat és a további szinteken kiszervezett tevékenységekről szóló megállapodások előzetes értékelése

(1) Az IKT-koncentrációs kockázat 25. cikk (5) bekezdésének c) pontjában említett azonosítása és értékelése során a pénzügyi szervezetek figyelembe veszik, hogy az IKT-szolgáltatásokkal kapcsolatos szerződéses megállapodás megkötése a következő helyzetek valamelyikét eredményezné-e:

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

b) IKT-szolgáltatások nyújtásával kapcsolatban többszörös szerződéses megállapodás létrejötte ugyanazzal a harmadik félnek minősülő IKT-szolgáltatóval, vagy harmadik félnek minősülő, egymással szoros kapcsolatban álló IKT-szolgáltatókkal.

A pénzügyi szervezetek mérlegelik az alternatív megoldásokkal, többek között más harmadik félnek minősülő IKT-szolgáltatók igénybevételével járó előnyöket és költségeket, ennek során figyelembe veszik, hogy az előirányzott megoldások illeszkednek-e, és ha igen, hogyan, a szervezetek digitális rezilienciára vonatkozó stratégiájában meghatározott üzleti igényekhez és célkitűzésekhez.

(2) Ha egy IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodásban szerepel az a lehetőség, hogy egy harmadik félnek minősülő IKT-szolgáltató egy kulcsfontosságú vagy lényeges funkciót harmadik félnek minősülő más IKT-szolgáltatóknak ad alvállalkozásba, a pénzügyi szervezetek mérlegelik az alvállalkozó igénybevételéből esetlegesen származó előnyöket és kockázatokat, különösen harmadik országban letelepedett IKT-alvállalkozó esetén.

Ha IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodás harmadik országban letelepedett, harmadik félnek minősülő IKT-szolgáltatóval jön létre, a pénzügyi szervezetek adott esetben legalább az alábbi tényezőket mérlegelik:

a) a személyes adatok védelmének tiszteletben tartása;

b) az eredményes jogérvényesítés;

c) a harmadik félnek minősülő IKT-szolgáltató csődje esetén alkalmazandó csődjogi rendelkezések;

d) a pénzügyi szervezet adatainak haladéktalan visszaszerzése kapcsán esetlegesen felmerülő akadályok.

A pénzügyi szervezetek értékelik, hogy az esetlegesen hosszú és összetett alvállalkozói láncok érinthetik-e, és ha igen, hogyan, a szervezet képességét a szerződéses megbízásba adott funkciók teljes körű nyomon követésére, valamint az illetékes hatóság képességét arra, hogy e tekintetben eredményesen ellássa a pénzügyi szervezet felügyeletét.

27. cikk

Főbb szerződéses rendelkezések

(1) A pénzügyi szervezet és a harmadik félnek minősülő IKT-szolgáltató jogait és kötelezettségeit egyértelműen meg kell határozni, és írásban kell rögzíteni. A szolgáltatási szintekre vonatkozó megállapodásokat is magában foglaló teljes szerződést egyetlen, írásba foglalt dokumentumban kell rögzíteni, amely nyomtatott, vagy letölthető és hozzáférhető formátumban áll a felek rendelkezésére.

(2) Az IKT-szolgáltatások igénybevételére irányuló szerződéses megállapodások legalább az alábbiakat foglalják magukban:

a) a harmadik félnek minősülő IKT-szolgáltató által biztosítandó funkciók és szolgáltatások egyértelmű és teljes körű leírása annak feltüntetésével, hogy alkalmazhat-e alvállalkozót valamely kulcsfontosságú vagy lényeges funkció vagy annak érdemi része ellátására, és ha igen, milyen feltételekkel;

b) azon helyszínek, ahol a szerződéses megbízásba vagy alvállalkozásba adott funkciók vagy szolgáltatások nyújtása és az adatkezelés történik, ideértve a tárolás helyét is, továbbá annak előírása, hogy a harmadik félnek minősülő IKT-szolgáltatónak értesítenie kell a pénzügyi szervezetet e helyszínek tervezett megváltoztatásáról;

c) a személyes adatok hozzáférhetőségére, rendelkezésre állására, integritására, biztonságára és védelmére vonatkozó rendelkezések, továbbá azok a rendelkezések, amelyek könnyen hozzáférhető formátumban biztosítják a pénzügyi szervezet által kezelt személyes és nem személyes adatokhoz való hozzáférést, valamint ezen adatok visszaszerzését és visszaszolgáltatását a harmadik félnek minősülő IKT-szolgáltató fizetésképtelensége, szanálása, vagy üzleti tevékenységének megszűnése esetén;

d) a szolgáltatási szintek teljes körű leírása annak frissítéseivel és módosításaival együtt, továbbá az elfogadott szolgáltatási szinteken belüli pontos mennyiségi és minőségi teljesítménycélok, amelyek lehetővé teszik a pénzügyi szervezet számára az eredményes nyomon követést, valamint a megfelelő korrekciós

intézkedések haladéktalan végrehajtását akkor, ha az elfogadott szolgáltatási szintek nem teljesülnek;

e) a harmadik félnek minősülő IKT-szolgáltatóra vonatkozó felmondási idők és a pénzügyi szervezettel szembeni adatszolgáltatási kötelezettségek az olyan fejlemények bejelentésére is kiterjedően, amelyek jelentős hatást gyakorolhatnak a harmadik félnek minősülő IKT-szolgáltató azon képességére, hogy az elfogadott szolgáltatási szinteknek megfelelően eredményesen ellássa a kulcsfontosságú vagy lényeges funkciókat;

f) a harmadik félnek minősülő IKT-szolgáltató azon kötelezettsége, hogy IKT-biztonsági esemény bekövetkezésekor többletköltség nélkül vagy előzetesen megállapított költség mellett támogatást nyújtson;

g) arra vonatkozó követelmény, hogy a harmadik félnek minősülő IKT-szolgáltató vezessen be és teszteljen vészhelyzeti terveket, továbbá rendelkezzen olyan IKT-biztonsági intézkedésekkel, eszközökkel és szabályzatokkal, amelyek megfelelően garantálják, hogy a pénzügyi szervezet a vonatkozó szabályozási kerettel összhangban biztonságosan nyújtsa a szolgáltatásait;

h) a pénzügyi szervezet arra vonatkozó joga, hogy folyamatosan nyomon kövesse a harmadik félnek minősülő IKT-szolgáltató teljesítményét; ez a jog kiterjed a következőkre:

   i. a pénzügyi szervezet vagy az általa kijelölt harmadik fél hozzáférési, vizsgálati és ellenőrzési joga és a releváns dokumentumokról való másolatkészítés joga, amelynek eredményes gyakorlását nem akadályozza vagy korlátozza más szerződéses megállapodás vagy végrehajtási szabályzat;

   ii. az alternatív bizonyossági szint megállapításának joga, ha más ügyfelek jogai érintettek;

   iii. a szolgáltató arra vonatkozó kötelezettségvállalása, hogy teljeskörűen együttműködik a pénzügyi szervezet által végzett helyszíni vizsgálatokban, továbbá a távellenőrzések terjedelmének, módozatainak és gyakoriságának részleteit;

i) a harmadik félnek minősülő IKT-szolgáltató arra vonatkozó kötelezettsége, hogy teljeskörűen együttműködjön a pénzügyi szervezet illetékes hatóságaival és szanálási hatóságaival, valamint az általuk kijelölt személyekkel;

j) a szerződés megszüntetésére vonatkozó felmondási jogok és az azokhoz kapcsolódó minimális felmondási idők az illetékes hatóságok elvárásainak megfelelően;

k) kilépési stratégiák, ezen belül különösen a megfelelő kötelező átmeneti időszak meghatározása:

   (a) amelynek során a harmadik félnek minősülő IKT-szolgáltató folytatja az érintett funkciók és szolgáltatások nyújtását annak érdekében, hogy csökkentse a pénzügyi szervezetnél keletkező zavar kockázatát; továbbá

   (b) amely lehetővé teszi a pénzügyi szervezet számára, hogy válthasson a harmadik félnek minősülő IKT-szolgáltatók között, illetve helyszíni

megoldásokra állhasson át a nyújtott szolgáltatás összetettségének megfelelően.

(3) A szerződéses megállapodásokat előkészítő tárgyalások során a pénzügyi szervezetek és a harmadik félnek minősülő IKT-szolgáltatók mérlegelik az egyes szolgáltatásokra kidolgozott általános szerződéses rendelkezések alkalmazását.

(4) Az EFH-k a vegyes bizottság keretében szabályozástechnikai standardtervezeteket dolgoznak ki, amelyek részletesen meghatározzák azokat az elemeket, amelyeket a pénzügyi szervezetnek kulcsfontosságú vagy lényeges funkciók alvállalkozásba adásakor meg kell állapítania és értékelnie kell annak érdekében, hogy érvényesítse a (2) bekezdés a) pontjában foglalt rendelkezéseket.

Az említett szabályozástechnikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak.

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

II. SZAKASZ

A HARMADIK FÉLNEK MINŐSÜLŐ KULCSFONTOSSÁGÚ IKT-SZOLGÁLTATÓKRA VONATKOZÓ FELVIGYÁZÁSI KERET

28. cikk

A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók kijelölése

(1) Az EFH-k a vegyes bizottság keretében, a 29. cikk (1) bekezdése alapján létrehozott felvigyázási fórum ajánlásával:

a) a (2) bekezdésben meghatározott kritériumok figyelembevételével kijelölik azokat a harmadik félnek minősülő IKT-szolgáltatókat, amelyek a pénzügyi szervezetek szempontjából kulcsfontosságúak;

b) a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók mindegyikére vonatkozóan vezető felvigyázóként kijelölik az EBH-t, az ESMA-t vagy az EIOPA-t attól függően, hogy az érintett pénzügyi szervezetek konszolidált mérlege, illetve a konszolidáció körébe nem tartozó vállalkozások egyedi mérlege alapján az adott harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató szolgáltatásait igénybe vevő, az 1093/2010/EU, az 1094/2010/EU vagy az 1095/2010/EU rendelet hatálya alá tartozó pénzügyi szervezetek teljes eszközértéke meghaladja-e a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató szolgáltatásait igénybe vevő összes vállalkozás teljes eszközértékének felét.

(2) Az (1) bekezdés a) pontjában említett kijelölés során az alábbi kritériumok mindegyikét figyelembe kell venni:

a) az a rendszerszintű hatás, amely a pénzügyi szolgáltatások nyújtásának stabilitását, folytonosságát vagy minőségét érné akkor, ha az adott harmadik félnek minősülő IKT-szolgáltató kiterjedt üzemzavar miatt nem képes nyújtani a szolgáltatásait, figyelembe véve azon pénzügyi szervezetek számát, amelyek részére a harmadik félnek minősülő IKT-szolgáltató szolgáltatásokat nyújt;

b) az adott harmadik félnek minősülő IKT-szolgáltató szolgáltatásait igénybe vevő pénzügyi szervezetek rendszerszintű jellege vagy jelentősége az alábbi paraméterek alapján:

i. az adott harmadik félnek minősülő IKT-szolgáltató szolgáltatásait igénybe vevő, globálisan rendszerszinten jelentős intézmények vagy egyéb rendszerszinten jelentős intézmények száma;

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

(c) az adott harmadik félnek minősülő IKT-szolgáltató által nyújtott szolgáltatások igénybevétele a pénzügyi szervezetek olyan kulcsfontosságú vagy lényeges funkciói kapcsán, amelyek ellátására végső soron ugyanezen harmadik félnek minősülő IKT-szolgáltató közreműködésével kerül sor attól függetlenül, hogy a pénzügyi szervezetek e szolgáltatásokat közvetlenül vagy közvetetten, alvállalkozási megállapodások útján veszik igénybe;

(d) a harmadik félnek minősülő IKT-szolgáltató helyettesíthetőségének mértéke az alábbi paraméterek alapján:

i. valós – legalább részleges – alternatívák hiánya, amely az adott piacon működő harmadik félnek minősülő IKT-szolgáltatók korlátozott számának, az adott harmadik félnek minősülő IKT-szolgáltató piaci részesedésének, vagy a megoldás technikai összetettségének vagy fejlettségének tulajdonítható, többek között szabadalmaztatott technológiának, vagy a harmadik félnek minősülő IKT-szolgáltató szervezeti felépítésének, tevékenységének egyedi jellemzői kapcsán;

ii. az érintett adatok és munkamennyiség adott harmadik félnek minősülő IKT-szolgáltatótól másik szolgáltatóhoz történő részleges vagy teljes migrálásával járó nehézségek, amelyek oka lehet egyrészt a migrálási folyamat jelentős pénzügyi költsége, valamint idő- és egyéb erőforrásigénye, másrészt pedig azoknak az IKT-kockázatoknak vagy egyéb működési kockázatoknak a megnövekedett mértéke, amelyeknek a migrálás kitenné a pénzügyi szervezetet;

e) azoknak a tagállamoknak a száma, amelyekben az adott harmadik félnek minősülő IKT-szolgáltató szolgáltatást nyújt;

f) azoknak a tagállamoknak a száma, amelyekben az adott harmadik félnek minősülő IKT-szolgáltató szolgáltatását igénybe vevő pénzügyi szervezetek tevékenységet folytatnak.

(3) A Bizottság felhatalmazást kap arra, hogy az 50. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el a (2) bekezdésben említett kritériumok kiegészítése céljából.

(4) Az (1) bekezdés a) pontjában említett kijelölési mechanizmus csak azt követően alkalmazható, hogy a Bizottság a (3) bekezdésnek megfelelően felhatalmazáson alapuló jogi aktust fogadott el.

(5) Az (1) bekezdés a) pontjában említett kijelölési mechanizmus nem alkalmazható azon harmadik félnek minősülő IKT-szolgáltatók tekintetében, amelyek az Európai

Unió működéséről szóló szerződés 127. cikkének (2) bekezdésében említett feladatok ellátásának támogatására létrehozott felvigyázási keret hatálya alá tartoznak.

(6) Az EFH-k a vegyes bizottság keretében összeállítják, közzéteszik és évente frissítik a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók uniós szintű jegyzékét.

(7) Az (1) bekezdés a) pontjának alkalmazásában az illetékes hatóságok összesített formában évente átadják a 29. cikk alapján létrehozott felvigyázási fórumnak a 25. cikk (4) bekezdésében említett jelentéseket. A felvigyázási fórum az illetékes hatóságoktól kapott információk alapján értékeli a pénzügyi szervezetek harmadik féltől való IKT-függőségét.

(8) A harmadik félnek minősülő IKT-szolgáltatók közül azok is kérhetik felvételüket a (6) bekezdésben említett jegyzékbe, amelyek eredetileg nem szerepeltek benne.

Az első albekezdés alkalmazásában a harmadik félnek minősülő IKT-szolgáltató indokolással ellátott kérelmet nyújt be az EBH, az ESMA vagy az EIOPA részére, a felügyeleti hatóságok pedig a vegyes bizottság keretében határoznak arról, hogy a harmadik félnek minősülő IKT-szolgáltatót az (1) bekezdés a) pontjának megfelelően felvegyék-e a jegyzékbe.

Az európai felügyeleti hatóságok a kérelem beérkezésétől számított 6 hónapon belül elfogadják a második albekezdésben említett határozatot, és arról értesítik a harmadik félnek minősülő IKT-szolgáltatót.

(9) A pénzügyi szervezetek nem veszik igénybe azt a harmadik országban letelepedett, harmadik félnek minősülő IKT-szolgáltatót, amely az Unión belüli letelepedése esetén az (1) bekezdés a) pontja szerint kulcsfontosságúnak minősülne.

29. cikk

A felvigyázási keret felépítése

(1) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 57. cikkével összhangban a vegyes bizottság albizottságként hozza létre a felvigyázási fórumot, amelynek célja, hogy támogassa a vegyes bizottság és a 28. cikk (1) bekezdésének b) pontjában említett vezető felvigyázó munkáját a pénzügyi ágazatok harmadik féltől eredő IKT-kockázatai terén. A felvigyázási fórum előkészíti a vegyes bizottság e területet érintő közös álláspontjainak és közös intézkedéseinek tervezeteit.

A felvigyázási fórum rendszeresen megvitatja az IKT-kockázatok és -sebezhetőségek releváns fejleményeit, és előmozdítja a harmadik féltől eredő IKT-kockázat uniós léptékű nyomon követését.

(2) A felvigyázási fórum évente együttesen értékeli a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó felvigyázási tevékenységek eredményeit és megállapításait, és koordinációs intézkedéseket mozdít elő, amelyek célja a pénzügyi szervezetek digitális működési rezilienciájának növelése, az IKT-koncentrációs kockázat kezelésében bevált módszerek támogatása, továbbá a kockázat ágazatok közötti átterjedését mérséklő eszközök vizsgálata.

(3) A felvigyázási fórum a harmadik félnek minősülő kulcsfontosságú 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 az EFH-k elnökeiből és az egyes tagállamok releváns illetékes hatósága mindenkori személyzetének egy magas rangú képviselőjéből áll. Az egyes EFH-k ügyvezető igazgatója, valamint az Európai Bizottság, az ERKT, az EKB és az ENISA egy-egy képviselője megfigyelőként vesz részt a felvigyázási fórum munkájában.

(5) Az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 16. cikkével összhangban az EFH-k iránymutatásokat adnak ki a köztük és az illetékes hatóságok között az e szakasz alkalmazásában folytatandó együttműködésről, az EFH-k és az illetékes hatóságok közötti feladatellátáshoz kapcsolódó részletes eljárásokról és feltételekről, valamint az ahhoz szükséges információátadás részleteiről, hogy az illetékes hatóságok biztosíthassák a vezető felvigyázók által a 31. cikk (1) bekezdésének d) pontja alapján a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozóan megfogalmazott ajánlásokhoz kapcsolódó intézkedéseket.

(6) Az e szakaszban meghatározott követelmények nem érintik az (EU) 2016/1148 irányelv, valamint a felhőszolgáltatók felvigyázásával kapcsolatos egyéb uniós szabályok alkalmazását.

(7) Az EFH-k a vegyes bizottság keretében a felvigyázási fórum előkészítő munkája alapján évente jelentést nyújtanak be a az Európai Parlamentnek, a Tanácsnak és a Bizottságnak.

30. cikk

A vezető felvigyázó feladatai

(1) A vezető felvigyázó értékeli, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók mindegyike rendelkezik-e átfogó, megbízható és hatékony szabályokkal, eljárásokkal, mechanizmusokkal és rendszerekkel azoknak a tőle eredő IKT-kockázatoknak a kezeléséhez, amelyekkel a pénzügyi szervezetek szembesülhetnek.

(2) Az (1) bekezdésben említett értékelés kiterjed:

a) azokra az IKT-vonatkozású követelményekre, amelyek biztosítják különösen a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által a pénzügyi szervezeteknek nyújtott szolgáltatások biztonságát, rendelkezésre állását, folytonosságát, skálázhatóságát és minőségét, valamint az adatok biztonságával, bizalmas jellegével és integritásával kapcsolatos szigorú normák folyamatos érvényesítését;

b) az IKT-biztonságot elősegítő fizikai biztonságra, ezen belül a helyszínek, létesítmények, adatközpontok biztonságára;

c) a kockázatkezelési folyamatokra, ezen belül az IKT-vonatkozású üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervekre;

d) az irányítási rendszerre, ezen belül az olyan szervezeti felépítésre, amelyben az egyértelmű, átlátható és következetes felelősségi körök és elszámoltathatósági szabályok lehetővé teszik az IKT-kockázatok eredményes kezelését;

e) a pénzügyi szervezeteket érő IKT-vonatkozású biztonsági események azonosítására, nyomon követésére és haladéktalan bejelentésére és az ilyen események, különösen a kiberbiztonsági események kezelésére és elhárítására;

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

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

h) az IKT-ellenőrzésekre;

i) a pénzügyi szervezetek részére nyújtott IKT-szolgáltatásokra vonatkozó releváns nemzeti és nemzetközi előírásokat.

(3) Az (1) bekezdésben említett értékelés alapján a vezető felvigyázó egyértelmű, részletes és indokolással ellátott egyedi felvigyázási tervet fogad el a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók mindegyikére vonatkozóan. A tervről minden évben értesíti a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatót.

(4) A (3) bekezdésben említett éves felvigyázási terv elfogadását, valamint arról a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók értesítését követően az illetékes hatóságok kizárólag a vezető felvigyázó egyetértésével hozhatnak a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókat érintő intézkedéseket.

31. cikk

A vezető felvigyázó hatáskörei

(1) Az e szakaszban meghatározott feladatok elvégzéséhez a vezető felvigyázó az alábbi hatáskörökkel rendelkezik:

a) a 32. cikknek megfelelően releváns információkat és dokumentumokat kérhet be;

b) a 33. és a 34. cikknek megfelelően általános vizsgálatot és ellenőrzést folytathat;

c) a felvigyázási tevékenységek elvégzését követően jelentést kérhet arról, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató milyen korrekciós és egyéb intézkedéseket hajtott végre az e bekezdés d) pontjában említett ajánlások kapcsán;

d) ajánlásokat fogalmazhat meg a 30. cikk (2) bekezdésében említett területekre, ezen belül különösen az alábbiakra vonatkozóan:

i. egyes IKT-biztonsági és minőségi követelmények vagy folyamatok alkalmazása, kiemelten 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 harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók által a pénzügyi szervezetek részére nyújtott szolgáltatásokra vonatkozó feltételek közül azoknak az alkalmazása, amelyek a vezető felvigyázó megítélése szerint relevánsak az egyedi meghibásodási pontok kialakulása vagy az ezzel kapcsolatos

kockázat felerősödése, valamint az IKT-koncentrációs kockázat esetében az uniós pénzügyi ágazat egészére kiterjedő esetleges rendszerszintű hatás csökkentése szempontjából;

iii. a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók által más harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókkal vagy harmadik országban letelepedett IKT-alvállalkozókkal megkötni tervezett alvállalkozói megállapodások, ezen belül a további szinteken kiszervezett tevékenységekről szóló megállapodások 32. és 33. cikkel összhangban végzett vizsgálata keretében azok a tervezett alvállalkozói és további szinteken kiszervezett tevékenységek, amelyek esetében a vezető felvigyázó megítélése szerint az alvállalkozásba adás kockázatokat eredményezhet a pénzügyi szervezet szolgáltatásnyújtására vagy a pénzügyi stabilitására nézve;

iv. az alvállalkozási megállapodástól való tartózkodás az alábbi feltételek teljesülése esetén:

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

– az alvállalkozó bevonása a pénzügyi szervezet kulcsfontosságú vagy lényeges funkciójának ellátására irányul.

(2) A vezető felvigyázó az (1) bekezdésben említett hatáskörök gyakorlását megelőzően egyeztet a felvigyázási fórummal.

(3) A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók jóhiszeműen együttműködnek a vezető felvigyázóval, és segítik a vezető felvigyázót a feladatai ellátásában.

(4) A vezető felvigyázó kényszerítő bírság kiszabásával kényszerítheti a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatót az (1) bekezdés a), b) és c) pontjának betartására.

(5) A (4) bekezdésben említett kényszerítő bírság naponta alkalmazandó a követelmények teljesítéséig, a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató értékesítését követő legfeljebb féléves időszakban.

(6) A kényszerítő bírság összege a bírság kiszabásáról szóló határozatban megjelölt naptól számítandó, mértéke a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató előző üzleti évben elért átlagos napi világpiaci forgalmának 1 %-a.

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

(8) Az EFH-k nyilvánosságra hoznak minden kiszabott kényszerítő bírságot, kivéve, ha az ilyen nyilvánosságra hozatal súlyosan veszélyeztetné a pénzügyi piacokat, vagy aránytalan károkat okozna az érintett feleknek.

(9) A kényszerítő bírság (4) bekezdés alapján történő kiszabása előtt a vezető felvigyázó a megállapítások kapcsán meghallgatási lehetőséget biztosít az eljárás alá vont harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató képviselői számára, és a

határozathozatal során kizárólag azokat a megállapításokat veszi figyelembe, amelyek kapcsán a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató lehetőséget kapott észrevételei megtételére. Az eljárás alá vont személyek védekezéshez való jogát az eljárás során teljes mértékben tiszteletben kell tartani. E személyeknek jogukban 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.

32. cikk

Információkérés

(1) A vezető felvigyázó egyszerű kérés vagy határozat útján előírhatja a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók számára, hogy adják át a részére az e rendelet szerinti feladatainak elvégzéséhez szükséges információkat, ideértve a releváns üzleti vagy működési dokumentumokat, a szerződéseket, a szabályzatok dokumentációját, az IKT-biztonsági ellenőrzésekről készült jelentéseket. az IKT-vonatkozású biztonsági eseményekről készült jelentéseket, valamint az olyan felekkel kapcsolatos információkat, amelyekhez az adott harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató működési funkciót vagy tevékenységet szervezett ki.

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

a) a kérés jogalapjaként e cikket jelöli meg;

b) meghatározza a kérés célját;

c) részletesen meghatározza a kért információt;

d) meghatározza az információnyújtás határidejét;

e) tájékoztatja a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató azon képviselőjét, akitől az információt kéri, hogy nem köteles megadni az információt, viszont amennyiben önkéntesen válaszol a kérésre, a nyújtott információ nem lehet a valóságnak nem megfelelő vagy félrevezető.

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

a) a kérés jogalapjaként e cikket jelöli meg;

b) meghatározza a kérés célját;

c) részletesen meghatározza a kért információt;

d) meghatározza az információnyújtás határidejét;

e) felhívja a figyelmet a 31. cikk (4) bekezdésében arra az esetre előírt kényszerítő bírságra, ha a nyújtott információ hiányos;

f) felhívja a figyelmet arra, hogy az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 60. és 61. cikke értelmében a határozat ellen fellebbezni lehet az EFH fellebbezési tanácsa előtt, és a határozat felülvizsgáltatható az Európai Unió Bíróságával.

(4) A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók képviselőjük útján nyújtják be a kért információkat. A megfelelően meghatalmazott ügyvédek szintén

jogosultak az ügyfelük nevében az információk benyújtására. A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók teljes felelősséggel tartoznak, ha a szolgáltatott információ hiányos, a valóságnak nem megfelelő vagy félrevezető.

(5) A vezető felvigyázó a határozat példányának haladéktalan megküldésével tájékoztatja a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságait.

33. cikk
Általános vizsgálatok

(1) Az e rendelet szerinti feladatainak elvégzése érdekében a vezető felvigyázó a 34. cikk (1) bekezdésében említett vizsgálócsoport támogatásával lefolytathatja a harmadik félnek minősülő IKT-szolgáltatók szükséges vizsgálatait:

(2) A vezető felvigyázó az alábbi hatáskörökkel rendelkezik:

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

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

c) a harmadik félnek minősülő IKT-szolgáltató képviselőjének 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 tisztviselők és más személyek hatáskörüket a vizsgálat tárgyát és célját feltüntető írásbeli felhatalmazás alapján gyakorolják.

A felhatalmazásban fel kell tüntetni továbbá a 31. cikk (4) bekezdése értelmében abban az esetben kiszabandó kényszerítő bírságot, ha a kért nyilvántartásokat, adatokat, eljárásokat vagy egyéb anyagokat nem vagy hiányosan nyújtják be, vagy ha a harmadik félnek minősülő IKT-szolgáltató képviselői a feltett kérdésekre nem vagy hiányosan válaszolnak.

(4) A harmadik félnek minősülő IKT-szolgáltatók képviselői kötelesek alávetni magukat a vezető felvigyázó határozata alapján elrendelt vizsgálatoknak. A határozatban fel kell tüntetni a vizsgálat tárgyát és célját, a 31. cikk (4) bekezdésében előírt kényszerítő bírságokat, az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet értelmében igénybe vehető jogorvoslati lehetőségeket, valamint azt a jogot, hogy a határozat az Európai Unió Bíróságával felülvizsgáltatható.

(5) A vezető felvigyázó a vizsgálat előtt kellő időben értesítést küld a vizsgálatról és a felhatalmazott személyek személyazonosságáról az adott harmadik félnek minősülő IKT-szolgáltatót igénybe vevő pénzügyi szervezetek illetékes hatóságainak.

34. cikk

Helyszíni ellenőrzések

(1) Az e rendelet szerinti feladatainak elvégzése érdekében a vezető felvigyázó a 35. cikk (1) bekezdésében említett vizsgálócsoportok támogatásával helyszíni ellenőrzés céljából beléphet a harmadik félnek minősülő IKT-szolgáltató bármely helyiségébe, területére és ingatlanára, beleértve a szolgáltató székhelyét, tevékenységének központi helyét, telephelyét is, emellett külső ellenőrzést végezhet.

(2) A vezető felvigyázó által helyszíni ellenőrzés lefolytatására felhatalmazott tisztviselők és más személyek beléphetnek a szolgáltató helyiségébe, területére és ingatlanára, és hatáskörükben eljárva az ellenőrzés időtartamára, az ahhoz szükséges mértékben zár alá vehetnek helyiségeket és nyilvántartásokat.

Az említett személyek hatáskörüket az ellenőrzés tárgyát és célját feltüntető írásbeli felhatalmazás felmutatásával gyakorolják, amelyben fel kell tüntetni a 31. cikk (4) bekezdése értelmében abban az esetben kivetendő kényszerítő bírságot, ha az érintett harmadik félnek minősülő IKT-szolgáltatók képviselői nem vetik alá magukat az ellenőrzésnek.

(3) A vezető felvigyázó az ellenőrzés előtt kellő időben értesítést küld az adott harmadik félnek minősülő IKT-szolgáltatót igénybe vevő pénzügyi szervezetek illetékes hatóságainak.

(4) Az ellenőrzés kiterjed a pénzügyi szervezeteknek nyújtott szolgáltatások teljesítéséhez felhasznált vagy ahhoz hozzájáruló releváns IKT-rendszerek, -hálózatok, -eszközök, valamint információk és adatok teljes körére.

(5) A tervezett helyszíni ellenőrzést megelőzően a vezető felvigyázó megfelelően értesíti a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatót, kivéve akkor, ha az értesítés veszélyhelyzet vagy válsághelyzet miatt nem lehetséges, vagy ha meghiúsítaná az eredményes vizsgálatot vagy ellenőrzést.

(6) A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató köteles alávetni magát a vezető felvigyázó határozata alapján elrendelt helyszíni ellenőrzéseknek. A határozatban fel kell tüntetni az ellenőrzés tárgyát és célját, meg kell határozni az ellenőrzés megkezdésének időpontját, valamint utalni kell a 31. cikk (4) bekezdésében előírt kényszerítő bírságokra, az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet értelmében igénybe vehető jogorvoslati lehetőségekre és arra a jogra, hogy a határozat az Európai Unió Bíróságával felülvizsgáltatható.

(7) Ha a vezető felvigyázó által felhatalmazott tisztviselők és más személyek azt állapítják meg, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató megtagadja az e cikk alapján elrendelt ellenőrzést, a vezető felvigyázó tájékoztatja a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatót ennek következményeiről, többek között arról, hogy az érintett pénzügyi szervezetek illetékes hatóságai megszüntethetik az adott harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóval létrejött szerződéses megállapodásokat.

35. cikk

Folyamatos felvigyázás

(1) A vezető felvigyázót az általános vizsgálat vagy helyszíni ellenőrzés lefolytatásában az adott harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóhoz létrehozott vizsgálócsoport támogatja.

(2) Az (1) bekezdésben említett közös vizsgálócsoport a vezető felvigyázó, valamint a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató szolgáltatásait igénybe vevő pénzügyi szervezeteket felügyelő illetékes hatóságok személyzetének tagjaiból áll, akik legfeljebb 10 fővel részt vesznek a felvigyázási tevékenységek előkészítésében és végrehajtásában. A közös vizsgálócsoport minden tagja tapasztalattal rendelkezik az IKT- és működési kockázat terén. A közös vizsgálócsoport munkáját az EFH személyzetének kijelölt tagja (a vezető felvigyázó koordinátora) koordinálja.

(3) Az EFH-k a vegyes bizottság keretében közös szabályozástechnikai standardtervezeteket dolgoznak ki, amelyek részletesen meghatározzák a releváns illetékes hatóságok által a közös vizsgálócsoportba delegált tagok kijelölését, valamint a vizsgálócsoport feladatait és munkarendjét. Az említett szabályozástechnikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják a Bizottságnak.

A Bizottság felhatalmazást kap az első albekezdésben említett szabályozástechnikai standardtervezeteknek az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 10–14. cikkével összhangban történő elfogadására.

(4) A vizsgálat vagy helyszíni ellenőrzés befejezését követő 3 hónapon belül a vezető felvigyázó a felvigyázási fórummal történt egyeztetés után a 31. cikkben említett hatáskörében ajánlásokat fogalmaz meg a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató számára.

(5) A vezető felvigyázó haladéktalanul közli a (4) bekezdésben említett ajánlásokat a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóval és az annak szolgáltatásait igénybe vevő pénzügyi szervezetek illetékes hatóságaival.

Felvigyázási tevékenysége keretében a vezető felvigyázó figyelembe veheti a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által rendelkezésére bocsátott külső tanúsítványokat, valamint a harmadik félnek minősülő IKT-szolgáltatónál végzett belső és külső ellenőrzési jelentéseket.

36. cikk

A felvigyázási előfeltételek harmonizálása

(1) Az EFH-k a vegyes bizottság keretében szabályozástechnikai standardtervezeteket dolgoznak ki, amelyek részletesen meghatározzák:

a) a 28. cikk (8) bekezdése szerinti önkéntes jegyzékbe vételét kérő harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által benyújtandó információkat;

b) a 31. cikk (1) bekezdése c) pontjának alkalmazásában bekérhető jelentések tartalmi és formai elemeit;

c) a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által a 31. cikk (1) bekezdése alapján benyújtandó, közzéteendő vagy bejelentendő információk megjelenítését annak felépítésére, formátumára és módjára kiterjedően;

d) a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által a vezető felvigyázó ajánlásai alapján végrehajtott intézkedések kapcsán a 37. cikk (2) bekezdése alapján végzendő illetékes hatósági értékelés részleteit.

(2) Az említett szabályozástechnikai standardtervezeteket az EFH-k [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig benyújtják 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 első albekezdésben említett szabályozástechnikai standardok elfogadása útján kiegészítse ezt a rendeletet.

37. cikk

Illetékes hatósági utókövetés

(1) A vezető felvigyázó által a 31. cikk (1) bekezdésének d) pontja alapján kiadott ajánlások kézhezvételét követő 30 naptári napon belül a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató értesíti a vezető felvigyázót arról, hogy végre kívánja-e hajtani az ajánlásokat. A vezető felvigyázó a kapott tájékoztatást haladéktalanul továbbítja az illetékes hatóságoknak.

(2) Az illetékes hatóságok nyomon követik, hogy a pénzügyi szervezetek figyelembe veszik-e a vezető felvigyázó által a 31. cikk (1) bekezdésének d) pontjával összhangban megfogalmazott, a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók számára tett ajánlásokban azonosított kockázatokat.

(3) Az illetékes hatóságok a 44. cikkel összhangban előírhatják a pénzügyi szervezetek számára a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által nyújtott szolgáltatás igénybevételének vagy bevezetésének átmeneti – részleges vagy teljes – felfüggesztését a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató részére megfogalmazott ajánlásokban azonosított kockázatok kezeléséig. Az illetékes hatóságok szükség esetén előírhatják a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóval kötött vonatkozó szerződéses megállapodások részleges vagy teljes megszüntetését.

(4) A (3) bekezdésben említett határozatok meghozatala során az illetékes hatóságok figyelembe veszik a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató által nem kezelt kockázat jellegét és nagyságát, továbbá a meg nem felelés alábbi kritériumok szerinti jelentőségét:

a) a meg nem felelés súlyossága és időtartama;

b) a meg nem felelés jelez-e súlyos hiányosságot a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató eljárásaiban, irányítási rendszereiben, kockázatkezelésében és belső kontrolljaiban;

c) a meg nem felelés megkönnyítette-e pénzügyi bűncselekmény elkövetését, előidézte-e azt, vagy a pénzügyi bűncselekmény más módon a meg nem felelésnek tulajdonítható-e;

d) a meg nem felelés szándékos cselekmény vagy gondatlanság eredménye.

(5) Az illetékes hatóságok rendszeresen tájékoztatják a vezető felvigyázót a pénzügyi szervezetekkel kapcsolatos felügyeleti feladataik ellátása során alkalmazott megközelítésekről és intézkedésekről, valamint a pénzügyi szervezetek által azokban

az esetekben alkalmazott szerződéses intézkedésekről, amikor a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltató részben vagy egészben nem fogadta el a vezető felvigyázó ajánlásait.

38. cikk

Felvigyázási díjak

(1) Az EFH-k a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókkal szemben díjat számítanak fel, amely teljes mértékben fedezi az EFH-knál az e rendelet alapján végzett felvigyázási tevékenységekkel kapcsolatban felmerült szükséges kiadásokat, beleértve azoknak a költségeknek a megtérítését is, amelyek a 35. cikkel összhangban a felvigyázási tevékenységekbe bekapcsolódó illetékes hatóságok munkájával összefüggésben merülhetnek fel.

A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatónak felszámított díj teljeskörűen fedezi az igazgatási költségeket, ugyanakkor összege arányos a szolgáltató forgalmával.

(2) A Bizottság felhatalmazást kap arra, hogy az 50. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el, amelyek a díj összegének és a díjfizetés módjának meghatározásával kiegészítik ezt a rendeletet.

39. cikk

Nemzetközi együttműködés

(1) Az EBH, az ESMA és az EIOPA az 1093/2010/EU rendelet, az 1094/2010/EU rendelet és az 1095/2010/EU rendelet 33. cikkével összhangban harmadik országbeli szabályozó és felügyeleti hatóságokkal kötött igazgatási megállapodások útján, ezen belül különösen az IKT-kockázatkezelési módszerek és kontrollok, a korrekciós intézkedések és az IKT-biztonsági események elhárítására irányuló intézkedések fejlesztésével mozdíthatja elő a több pénzügyi ágazatra kiterjedő, harmadik féltől eredő IKT-kockázat kezelésével kapcsolatos nemzetközi együttműködést.

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

VI. FEJEZET

INFORMÁCIÓMEGOSZTÁSRA VONATKOZÓ MEGÁLLAPODÁSOK

40. cikk

A kiberfenyegetésekkel kapcsolatos adatok és információk megosztására vonatkozó megállapodások

(1) A pénzügyi szervezetek kiberfenyegetésekkel kapcsolatban többek között az illetéktelen hozzáférésre utaló körülményekre, taktikákra, módszerekre, eljárásokra,

kiberfenyegetettségi riasztásokra és konfigurációs eszközökre is kiterjedő adatokat és információkat adhatnak át egymásnak, amennyiben az adatok és információk átadása:

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 pénzügyi szervezeteknél meglévő védelmi képességek, fenyegetésészlelési módszerek, mérséklési stratégiák, valamint elhárítási és helyreállítási megoldások körének bővítéséhez nyújtott támogatással;

b) megbízható közösségeken vagy pénzügyi szervezeteken 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 adatok védelme[48], valamint a versenypolitikára vonatkozó iránymutatások[49] maradéktalan betartását.

(2) Az (1) bekezdés c) pontjának alkalmazásában az információmegosztási megállapodások meghatározzák a részvétel feltételeit, valamint adott esetben részletesen rögzítik a közigazgatási szervek szerepvállalásának körülményeit és azt, hogy e szervek milyen minőségben kapcsolódhatnak az információmegosztási megállapodásokhoz, valamint a műveleti elemeket, ideértve az e célból kialakított informatikai platformok alkalmazását.

(3) A pénzügyi szervezetek értesítik az illetékes hatóságokat az (1) bekezdésben említett információmegosztási megállapodásban való részvételükről tagságuk érvényesítésekor, illetve adott esetben tagságuk megszűnéséről annak hatálybalépésekor.

VII. FEJEZET

ILLETÉKES HATÓSÁGOK

41. cikk

Illetékes hatóságok

A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó, e rendelet V. fejezetének II. szakaszában említett felvigyázási keret rendelkezéseinek sérelme nélkül az e rendeletben meghatározott kötelezettségek teljesítését a vonatkozó jogi aktusokban rájuk ruházott hatásköröknek megfelelően az alábbi illetékes hatóságok biztosítják:

a) hitelintézetek esetében a 2013/36/EU irányelv 4. cikkével összhangban kijelölt illetékes hatóság, az 1024/2013/EU rendelettel az EKB-ra ruházott egyedi feladatok sérelme nélkül;

[48] 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 szóló 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelettel (az általános adatvédelmi rendelettel) összhangban (HL L 119., 2016.5.4., 1. o.).

[49] A Bizottság közleménye – Iránymutatás az Európai Unió működéséről szóló szerződés 101. cikkének a horizontális együttműködési megállapodásokra való alkalmazhatóságáról (HL C 11., 2011.1.14., 1. o.).

b) pénzforgalmi szolgáltatók esetében az (EU) 2015/2366 irányelv 22. cikkével összhangban kijelölt illetékes hatóság;

c) elektronikus pénzforgalmi intézmények esetében a 2009/110/EK irányelv 37. cikkével összhangban kijelölt illetékes hatóság;

d) befektetési vállalkozások esetében az (EU) 2019/2034 irányelv 4. cikkével összhangban kijelölt illetékes hatóság;

e) kriptoeszköz-szolgáltatók, kriptoeszköz-kibocsátók, eszközalapú token kibocsátói és jelentős eszközalapú token kibocsátói esetében az [*(EU) 20xx MiCA-rendelet*] 3. cikke (1) bekezdése ee) pontjának első franciabekezdésével összhangban kijelölt illetékes hatóság;

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

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

h) kereskedési helyszínek és adatszolgáltatók esetében a 2014/65/EU irányelv 67. cikkével összhangban kijelölt illetékes hatóság;

i) kereskedési adattárak esetében a 648/2012/EU rendelet 55. cikkével összhangban kijelölt illetékes hatóság;

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

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

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

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

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

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

p) jogszabály szerint engedélyezett könyvvizsgálók és könyvvizsgáló társaságok esetében a 2006/43/EK irányelv 3. cikkének (2) bekezdésével és 32. cikkével összhangban kijelölt illetékes hatóság;

q) kritikus referenciamutatók kezelői esetében az *(EU) 20xx/xx rendelet* 40. és 41. cikkével összhangban kijelölt illetékes hatóság;

r) európai közösségi finanszírozási szolgáltatók esetében az *(EU) 20xx/xx rendelet x. cikkével* összhangban kijelölt illetékes hatóság;

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

42. cikk

Együttműködés az (EU) 2016/1148 irányelvvel létrehozott struktúrákkal és hatóságokkal

(1) Az együttműködés elősegítése, valamint az e rendelet alapján kijelölt illetékes hatóságok és az (EU) 2016/1148 irányelv 11. cikkével létrehozott együttműködési csoport közötti felügyeleti kapcsolattartás lehetővé tétele érdekében az EFH-k és az illetékes hatóságok kezdeményezhetik részvételüket az együttműködési csoport munkájában.

(2) Az illetékes hatóságok indokolt esetben egyeztethetnek az (EU) 2016/1148 irányelv 8., illetve 9. cikkében említett egyedüli kapcsolattartó ponttal és a számítógép-biztonsági eseményekre reagáló nemzeti csoportokkal.

43. cikk

Több pénzügyi ágazatra kiterjedő műveletek, kommunikáció és együttműködés

(1) Az EFH-k a vegyes bizottság keretében, az EKB-val és az ERKT-val együttműködve mechanizmusokat alakíthatnak ki, amelyek lehetővé teszik az eredményes módszerek pénzügyi ágazatok közötti megosztását a helyzetismeret javítása, valamint a pénzügyi ágazatok számára közös kibersebezhetőségek és -kockázatok azonosítása céljából.

Kibertámadási forgatókönyveket alkalmazó válságkezelési és vészhelyzeti műveleteket dolgozhatnak ki kommunikációs csatornák kialakítása, valamint az eredményes, koordinált uniós szintű elhárítás fokozatos lehetővé tétele érdekében, hogy kezelhessék a jelentős, határokon átnyúló IKT-vonatkozású biztonsági eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazat egészére.

E műveletek keretében adott esetben tesztelhetők a pénzügyi ágazat más ágazatoktól való függőségei is.

(2) Az illetékes hatóságok, az EBH, az ESMA és az EIOPA, valamint az EKB szorosan együttműködnek és információkat cserélnek egymással a 42–48. cikk szerinti feladataik ellátása céljából. Felügyeleti tevékenységüket szorosan összehangolva kell végezniük annak érdekében, hogy feltárják 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.

44. cikk

Közigazgatási szankciók és korrekciós intézkedések

(1) Az illetékes hatóságok rendelkeznek 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 arról másolat beszerzése vagy készítése;

b) helyszíni ellenőrzések, vizsgálatok elvégzése;

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

(3) A tagállamok azon jogának sérelme nélkül, hogy a 46. cikkel összhangban büntetőjogi szankciókat alkalmazzanak, a tagállamok meghatározzák az e rendelet megsértése esetén alkalmazandó megfelelő közigazgatási szankciók és korrekciós intézkedések megállapításának szabályait, és gondoskodnak azok eredményes végrehajtásáról.

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 az alábbi közigazgatási szankciókat vagy korrekciós intézkedéseket alkalmazzák:

a) végzés meghozatala, amely előírja a természetes vagy jogi személy számára, hogy hagyjon fel az adott 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 szolgáltató birtokában lévő adatforgalmi nyilvántartások bekérése, amennyiben észszerűen feltételezhető e rendelet megsértése, és amennyiben ezen nyilvántartások relevánsak lehetnek e rendelet megsértésének kivizsgálása szempontjából; valamint

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 elrendelő határozatokat kellően megindokolják, és azokkal szemben jogorvoslattal lehessen élni.

45. cikk

A közigazgatási szankciók és korrekciós intézkedések előírására vonatkozó hatáskörök gyakorlása

(1) Az illetékes hatóságoknak a 44. cikkben említett közigazgatási szankciók és korrekciós intézkedések kiszabására vonatkozó hatáskörüket a nemzeti jogi keretrendszerükkel összhangban kell gyakorolniuk adott esetben:

a) közvetlenül;

b) más hatóságokkal együttműködve;

c) saját felelősségi körükön belül, más hatóságokra történő hatáskör-átruházás útján;

d) az illetékes igazságügyi hatóságok megkeresése útján.

(2) Az illetékes hatóságoknak az e rendelet 44. cikke alapján kiszabott közigazgatási szankciók vagy korrekciós intézkedések típusának és szintjének meghatározása során figyelembe kell venniük, hogy a jogsértés mennyiben volt szándékos vagy mennyiben származott gondatlanságból, továbbá figyelembe kell venniük minden egyéb lényeges 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 ereje;

d) a felelős természetes vagy jogi személy által elért nyereség vagy elkerült veszteség jelentősége, amennyiben ezek meghatározhatók;

e) a jogsértés által harmadik feleknek okozott veszteség, amennyiben meghatározható;

f) a felelős természetes vagy jogi személy illetékes hatósággal való együttműködésének mértéke, amelytől függetlenül gondoskodni kell az adott személy által – nyereség elérésével vagy veszteség elkerülésével – szerzett haszon visszaszolgáltatásáról;

g) a felelős természetes vagy jogi személy által elkövetett korábbi jogsértések.

46. 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) Ha 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 joghatósági területükön belül kapcsolatba lépjenek az igazságügyi, büntetőeljárást lefolytató, illetve 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 és az EIOPA-nak, hogy teljesíthessék az együttműködésre vonatkozó, e rendelet szerinti kötelezettségüket.

47. cikk

Értesítési kötelezettség

A tagállamok [*Kiadóhivatal: kérjük, illessze be a dátumot: 1 évvel a hatálybalépést követően*]-jéig/-ig értesítik a Bizottságot, az ESMA-t, az EBH-t és az EIOPA-t az e fejezetet végrehajtó törvényi, rendeleti és közigazgatási rendelkezésekről, a vonatkozó büntetőjogi rendelkezéseket is beleértve. 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.

48. cikk

A közigazgatási szankciók nyilvánosságra hozatala

(1) Az illetékes hatóságok a hivatalos honlapjukon a címzett előzetes értesítését követően haladéktalanul közzéteszik azokat a közigazgatási szankciókat elrendelő határozatokat, amelyekkel szemben fellebbezésnek nincs helye.

(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) Ha 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, 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 hatóság a közigazgatási szankciót elrendelő határozat kapcsán az alábbi megoldások valamelyikét alkalmazza:

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 a közzététel nem állna arányban az előírt szankció engedékenységével.

(4) A közigazgatási szankció anonim közzétételéről szóló, a (3) bekezdés b) pontja szerinti határozat esetében az érintett 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 hatóság köteles a hivatalos honlapján haladéktalanul közzétenni ezt az információt, valamint az eljárás későbbi szakaszaiban a fellebbezés eredményével kapcsolatban keletkező információkat is. A közigazgatási szankciót elrendelő határozatot megsemmisítő bírósági határozatokat ugyancsak közzé kell tenni.

(6) Az illetékes hatóságoknak biztosítaniuk kell, hogy az e cikk (1)–(4) bekezdésében említett bármely közzététel a közzétételt követően legalább öt évig elérhető legyen a hivatalos honlapjukon. A nyilvánosságra hozott személyes adatokat csak annyi ideig

lehet az illetékes hatóság honlapján megjelentetni, ameddig ez az alkalmazandó adatvédelmi szabályok alapján szükséges.

49. cikk

Szakmai titoktartás

(1) A szakmai titoktartás (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 semmilyen más személlyel vagy hatósággal nem közölhetők, kivéve, ha ezt az uniós vagy tagállami jogban foglalt rendelkezés írja elő.

(4) Az e rendelet alapján az illetékes hatóságok között folytatott bármilyen, üzleti vagy működési feltételekkel, illetve 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 a szóban forgó információ nyilvánosságra hozható, vagy ha e nyilvánosságra hozatalt bírósági eljárás teszi szükségessé.

VIII. FEJEZET

FELHATALMAZÁSON ALAPULÓ JOGI AKTUSOK

50. 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 28. cikk (3) bekezdésében és a 38. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása öt éves időtartamra szól [*Kiadóhivatal: kérjük, illessze be a dátumot: 5 évvel e rendelet hatálybalépését követően*-án/-én] kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 28. cikk (3) bekezdésében és a 38. 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 foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul, egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 28. cikk (3) bekezdése és a 38. 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 két 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 két hónappal meghosszabbodik.

IX. FEJEZET

ÁTMENETI ÉS ZÁRÓ RENDELKEZÉSEK

I. SZAKASZ

51. cikk

Felülvizsgálatra vonatkozó rendelkezés

A Bizottság [*Kiadóhivatal: kérjük, illessze be a dátumot: 5 évvel e rendelet hatálybalépését követően*-jéig/-ig] – adott esetben az EBH, az ESMA, az EIOPA, valamint az ERKT bevonásával folytatott konzultációt követően – felülvizsgálatot végez és – indokolt esetben jogalkotási javaslattal együtt – jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók 28. cikk (2) bekezdése szerinti kijelölésére vonatkozó kritériumokról.

II. SZAKASZ

MÓDOSÍTÁSOK

52. cikk

Az 1060/2009/EK rendelet módosításai

Az 1060/2009/EK rendelet I. mellékletében az A. szakasz 4. pontjának első albekezdése helyébe a következő szöveg lép:

„A hitelminősítő intézet hatékony és eredményes adminisztratív és számviteli eljárásokkal, belső ellenőrzési mechanizmusokkal, célravezető kockázatelemzési eljárásokkal és az IKT-rendszerek kezelésére vonatkozó hatékony ellenőrzési és védelmi szabályozással kell rendelkeznie az (EU) 2021/xx európai parlamenti és tanácsi rendelettel* [DORA] összhangban.

* Az Európai Parlament és a Tanács (EU) 2021/xx rendelete […] (HL L XX, ÉÉÉÉ.HH.NN., X. o.).”.

53. 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) 2021/xx európai parlamenti és tanácsi rendelettel* [DORA] összhangban kezelt IKT-rendszereket kell alkalmaznia.

   * Az Európai Parlament és a Tanács (EU) 2021/xx rendelete […] (HL L XX, ÉÉÉÉ.H.N., X. 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 vészhelyzet esetére helyreállítási tervet, ezen belül az (EU) 2021/xx európai parlamenti és tanácsi rendelettel* [DORA] összhangban kialakított IKT-vonatkozású üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervet dolgoz ki, hajt végre és tart fenn, amelynek célja a központi szerződő fél funkcióinak megőrzése, a műveletek időben történő helyreállítása, valamint kötelezettségeinek teljesítése.”;

   (b) a (3) bekezdés első albekezdése helyébe a következő szöveg lép:

   „E cikk következetes alkalmazása érdekében az EÉPH a KBER tagjaival folytatott konzultációt követően kidolgozza az üzletmenet-folytonossági terv, valamint a vészhelyzeti helyreállítási terv minimális tartalmát és előírásait meghatározó szabályozástechnikai standardok tervezetét, az IKT-vonatkozású üzletmenet-folytonossági és katasztrófa utáni helyreállítási terv kivételével.”;

3. az 56. cikk (3) bekezdése első albekezdésének helyébe a következő szöveg lép:

   „(3) E cikk következetes alkalmazása érdekében az EÉPH 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) bekezdése 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, ideértve az (EU) 2021/xx európai parlamenti és tanácsi rendelettel [*DORA*] összhangban kezelt IKT-rendszereket is.

   (2) A kereskedési adattár megfelelő üzletmenet-folytonossági politikát és vészhelyzet esetére helyreállítási tervet, ezen belül az (EU) 2021/xx

európai parlamenti és tanácsi rendelettel [*DORA*] összhangban kialakított IKT-vonatkozású üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervet dolgoz ki, hajt végre és tart fenn, amelynek célja a kereskedési adattár funkcióinak megőrzése, a műveletek időben történő helyreállítása, valamint kötelezettségeinek teljesítése.”;

5. a 80. cikk (1) bekezdését el kell hagyni.

54. 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 csökkentenie kell azok hatását egyrészt az (EU) 2021/xx európai parlamenti és tanácsi rendelettel* [*DORA*] összhangban kialakított és kezelt IKT-eszközök, eljárások és politikák, a működési kockázat más típusai esetében pedig egyéb megfelelő eszközök, ellenőrzések és eljárások alkalmazásával, többek között az általa üzemeltetett valamennyi értékpapír-kiegyenlítési rendszer tekintetében.

* Az Európai Parlament és a Tanács (EU) 2021/xx rendelete […] (HL L XX, ÉÉÉÉ.H.N., X. 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 és katasztrófa utáni helyreállítási tervet, ezen belül az (EU) 2021/xx európai parlamenti és tanácsi rendelettel [*DORA*] összhangban kialakított IKT-vonatkozású üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervet kell kidolgoznia, végrehajtania és fenntartania, amellyel biztosítja a folyamatos szolgáltatásnyújtást, a működés mielőbbi helyreállítását, valamint kötelezettségeinek teljesítését olyan események bekövetkeztekor, amikor komolyan fennáll a működési zavar veszélye.

(4) A (3) bekezdésben említett tervnek – többek közt annak biztosításával, hogy a kulcsfontosságú informatikai rendszerek működését a leállást követően az (EU) 2021/xx európai parlamenti és tanácsi rendelet [DORA] 11. cikkének (5) és (7) bekezdésében előírt módon helyre lehessen állítani – lehetővé kell tennie az üzemzavar bekövetkeztekor folyamatban lévő összes 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 első albekezdésének helyébe a következő szöveg lép:

„A központi értéktár köteles meghatározni, nyomon követni és kezelni azokat a kockázatokat, amelyeket az általa üzemeltetett értékpapír-kiegyenlítési rendszerek fő résztvevői, valamint a szolgáltatók és közműszolgáltatók, illetve más központi értéktárak és piaci infrastruktúrák jelenthetnek a működésére. Kérésre az illetékes és érintett hatóságok rendelkezésére kell bocsátania a feltárt kockázatokkal kapcsolatos

információkat. Ezenfelül haladéktalanul tájékoztatnia kell az illetékes hatóságot és az érintett hatóságokat az ilyen kockázatokból eredő működési zavarokról, kivéve azokat, amelyek IKT-kockázattal összefüggésben következnek be.”;

5. a (7) bekezdés első albekezdésének helyébe a következő szöveg lép:

„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 a katasztrófa utáni helyreállítási tervet, valamint az ezekhez kapcsolódó értékelési módszereket.”.

55. cikk

A 600/2014/EU rendelet módosításai

A 600/2014/EU rendelet a következőképpen módosul:

1. a 27g. cikk a következőképpen módosul:

(a) a (4) bekezdést el kell hagyni;

(b) a (8) bekezdés c) pontja helyébe a következő szöveg lép:

(c) „c) a (3) és (5) bekezdésben megállapított konkrét szervezeti követelményeket.”;

2. A 27h. cikk a következőképpen módosul:

(a) az (5) bekezdést el kell hagyni;

(b) a (8) bekezdés e) pontja helyébe a következő szöveg lép:

„e) a (4) bekezdésben megállapított konkrét szervezeti követelményeket.”;

3. A 27i. cikk a következőképpen módosul:

(a) a (3) bekezdést el kell hagyni;

(b) az (5) bekezdés b) pontja helyébe a következő szöveg lép:

„b) a (2) és (4) bekezdésben megállapított konkrét szervezeti követelményeket.”;

56. cikk

Hatálybalépés és alkalmazás

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

Rendelkezéseit *[a hatálybalépést 12 hónappal követő dátum]-tól/-től* kell alkalmazni.

A 23. és 24. cikket azonban *[a hatálybalépést 36 hónappal követő dátum]-tól/-től* kell alkalmazni.

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

Kelt Brüsszelben, -án/-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

1.2. Érintett szakpolitikai terület(ek)

1.3. A javaslat/kezdeményezés típusa

1.4. Célkitűzés(ek)

1.5. A javaslat/kezdeményezés indoklása

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

1.7. Tervezett irányítási módszer(ek)

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

2.2. Irányítási és kontrollrendszer(ek)

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási tétele/tételei

3.2. A kiadásokra gyakorolt becsült hatás

3.2.1. A kiadásokra gyakorolt becsült hatás összegzése

3.2.2. Az előirányzatokra gyakorolt becsült hatás

3.2.3. A humánerőforrásra gyakorolt becsült hatás

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

3.2.5. Harmadik felek részvétele a finanszírozásban

3.3. A bevételre gyakorolt becsült hatás

Melléklet

Általános feltételezések

Felvigyázási hatáskörök

PÉNZÜGYI KIMUTATÁS – „ÜGYNÖKSÉGEK”

(1) A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

Javaslat – az Európai Parlament és a Tanács rendelete a pénzügyi ágazat digitális működési rezilienciájáról

1.2. Érintett szakpolitikai terület(ek)

Szakpolitikai terület: Pénzügyi stabilitás, pénzügyi szolgáltatások és tőkepiaci unió

Tevékenység: Digitális működési reziliencia

1.3. A javaslat a következőre irányul:

☑ **új intézkedés**

☐ **kísérleti projektet/előkészítő intézkedést követő új intézkedés**[50]

☐ **jelenlegi intézkedés meghosszabbítása**

☐ **egy vagy több intézkedés összevonása egy másik/új intézkedéssé**

1.4. Célkitűzés(ek)

1.4.1. Általános célkitűzés(ek)

A kezdeményezés általános célkitűzése az uniós pénzügyi ágazathoz tartozó szervezetek digitális működési rezilienciájának erősítése a meglévő szabályok észszerűsítésével és korszerűsítésével, hiányosság esetén új követelmények bevezetésével. Ez az egységes szabálykönyv digitális dimenzióját is erősítené.

Az átfogó célkitűzés három általános célkitűzésre bontható: 1. a pénzügyi rendszerben keletkező zavar és instabilitás kockázatának csökkentése; 2. az adminisztratív teher enyhítése és a felügyeleti eredményesség javítása; 3. a fogyasztók és a befektetők védelmének erősítése.

1.4.2. Konkrét célkitűzés(ek)

A javaslat konkrét célkitűzései a következők:

az információs és kommunikációs technológiákkal (IKT) összefüggő kockázatok átfogóbb kezelése, a digitális reziliencia általános szintjének növelése a pénzügyi ágazatban;

az IKT-vonatkozású biztonsági események bejelentésének észszerűsítése, a bejelentési követelmények közötti átfedések megszüntetése;

a pénzügyi felügyeletek számára az IKT-vonatkozású biztonsági eseményekkel kapcsolatos információk hozzáférhetővé tétele;

annak biztosítása, hogy a pénzügyi vállalkozások értékeljék a megelőző és a rezilienciára irányuló intézkedéseiket, és azonosítsák az IKT-vonatkozású sebezhetőségeket;

az egységes piac széttagoltságának csökkentése, a teszteredmények országok közötti kölcsönös elismerésének lehetővé tétele;

[50] A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint.

az IKT-szolgáltatást igénybe vevő pénzügyi szervezeteket védő, ezen belül a harmadik félnek minősülő IKT-szolgáltatók nyomon követésére irányadó kiszervezési szabályokra vonatkozó szerződéses biztosítékok megerősítése;

a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázásának lehetővé tétele;

a fenyegetettségi információk cseréjének ösztönzése a pénzügyi ágazaton belül.

1.4.3. Várható eredmény(ek) és hatás(ok)

Tüntesse fel a javaslat/kezdeményezés várt hatásait a kedvezményezettekre/célcsoportokra.

A pénzügyi ágazat digitális működési rezilienciájára vonatkozó jogszabály a digitális működési reziliencia valamennyi szempontjára kiterjedő átfogó keret létrehozásával eredményesen javítaná a pénzügyi ágazat általános digitális működési rezilienciáját. Óvná az egységes szabálykönyv érthetőségét és belső koherenciáját.

Egyértelműbbé és koherensebbé tenné a kiberbiztonsági irányelvvel és annak felülvizsgálatával való kölcsönhatást. Egyértelművé tenné a pénzügyi szervezetek számára az általuk a digitális működési rezilienciára vonatkozóan betartandó különböző szabályokat, különösen azon pénzügyi szervezetek számára, amelyek több engedéllyel is rendelkeznek, és az Unión belül több piacon is folytatnak tevékenységet.

1.4.4. Teljesítménymutatók

Határozza meg az előrehaladás és az eredmények nyomon követésére szolgáló mutatókat.

Lehetséges mutatók:

Az uniós pénzügyi ágazatban bekövetkezett IKT-vonatkozású biztonsági események száma és hatása

A prudenciális felügyeleti hatóságoknál bejelentett jelentős IKT-vonatkozású biztonsági események száma

Fenyegetettségi szempontú behatolási teszt végzésére kötelezett pénzügyi szervezetek száma

Harmadik félnek minősülő IKT-szolgáltatóval szerződéses megállapodást kötő, általános szerződéses rendelkezéseket alkalmazó pénzügyi szervezetek száma

A prudenciális felügyeleti hatóságok/európai felügyeleti hatóságok által felvigyázott, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók száma

A fenyegetettségi információk megosztásában részt vevő pénzügyi szervezetek száma

Egy adott IKT-vonatkozású biztonsági eseményről kötelezően bejelentést fogadó hatóságok száma

Határon átnyúló fenyegetettségi szempontú behatolási tesztek száma

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével

A pénzügyi ágazat nagymértékben támaszkodik az információs és kommunikációs technológiákra (IKT). A tagállami és európai szintű célzott szakpolitikai és jogalkotási kezdeményezések révén elért jelentős előrehaladás ellenére az IKT-kockázatok továbbra is kihívást jelentenek az uniós pénzügyi rendszer digitális működési rezilienciája, teljesítménye és stabilitása szempontjából. A 2008. évi pénzügyi válságot követő reform elsősorban az uniós pénzügyi ágazat pénzügyi rezilienciáját erősítette meg, és arra irányult, hogy megóvja az Unió versenyképességét, valamint gazdasági, prudenciális és a piaci magatartás szempontjából vett stabilitását. Bár az IKT-biztonság és az általános digitális működési reziliencia a működési kockázat kezelésének része, a válság utáni szabályozási menetrendben kisebb hangsúlyt kapott, és fejlesztésére az uniós pénzügyi piacot érintő szakpolitikai és szabályozási területek

közül csak egyeseken, vagy csak néhány tagállamban került sor. Ez a következő kihívásokkal járt, amelyeket a javaslatnak kezelnie kell:

A pénzügyi ágazat IKT-kockázatára és digitális működési rezilienciájára vonatkozó uniós jogi keret széttagolt, összhangja nem teljes.

Az IKT-vonatkozású biztonsági események bejelentésére vonatkozó egységes követelmények hiányában a felügyeletek nem alkothatnak teljes képet a biztonsági események jellegéről, gyakoriságáról, jelentőségéről és hatásáról.

Egyes pénzügyi szervezetekre összetett, egymást átfedő és adott esetben egymással össze nem hangolt bejelentési követelmények vonatkoznak ugyanazon IKT-vonatkozású biztonsági esemény kapcsán.

A kiberfenyegetettségi információk megosztásának és a kapcsolódó stratégiai, taktikai és operatív együttműködésnek az elégtelensége megakadályozza a pénzügyi szervezeteket abban, hogy megfelelően értékeljék, nyomon kövessék, kivédjék és kezeljék a kiberfenyegetéseket.

Egyes pénzügyi szolgáltatási alágazatokban egymással párhuzamos, össze nem hangolt penetrációs és rezilienciatesztelési keretek lehetnek érvényben az eredmények országok közötti kölcsönös elismerése nélkül, míg más alágazatokban egyáltalán nincsenek ilyen keretek.

Az, hogy a felügyeleteknek nincs betekintésük a pénzügyi szervezetek harmadik félnek minősülő IKT-szolgáltatók által végzett tevékenységeibe, az egyes pénzügyi szervezeteket és a teljes pénzügyi rendszert egyaránt működési kockázatoknak teszi ki.

A pénzügyi felügyeletek sem megfelelő felhatalmazással, sem eszközökkel nem rendelkeznek az abból eredő koncentrációs és rendszerszintű kockázatok nyomon követésére és kezelésére, hogy a pénzügyi szervezetek harmadik félnek minősülő IKT-szolgáltatók szolgáltatásait veszik igénybe.

1.5.2. Az Unió részvételéből származó hozzáadott érték (adódhat többek között a koordinációból eredő előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pontban „az Unió részvételéből származó hozzáadott érték” azt az uniós részvételből adódó értéket jelenti, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.

Az európai szintű fellépés indokai (előzetes):

A digitális működési reziliencia közös érdekű kérdés az uniós pénzügyi piacok számára. Az uniós szintű fellépés több előnnyel és nagyobb hozzáadott értékkel járna, mint az egyes tagállamok külön intézkedései. Az IKT-kockázatra vonatkozó operatív rendelkezésekkel való kiegészítés nélkül az egységes szabálykönyv biztosítaná az eszközöket valamennyi egyéb kockázattípus európai szintű kezeléséhez, azonban ezekben a digitális működési reziliencia szempontjai nem, vagy csak széttagolt és össze nem hangolt nemzeti kezdeményezések szintjén kapnának szerepet. A javaslat egyértelmű jogi helyzetet teremtene azt illetően, hogy a digitális működési rezilienciára vonatkozó rendelkezések alkalmazandók-e, és ha igen, hogyan, különösen a határokon átnyúló tevékenységet végző pénzügyi szervezetek esetében; emellett az alól is mentesítené a tagállamokat, hogy az uniós szabályok jelenlegi korlátozott alkalmazási körére és a kiberbiztonsági irányelv általános jellegére tekintettel önállóan fejlesszék tovább a digitális működési rezilienciára és a kiberbiztonságra vonatkozó szabályokat, szabványokat és elvárásokat.

A várható uniós hozzáadott érték (utólagos):

Az uniós beavatkozás jelentősen javítaná a szakpolitikai intézkedés eredményességét, emellett csökkentené az összetettséget, és valamennyi pénzügyi szervezet számára csökkentené a pénzügyi és adminisztratív terheket. A gazdaság egy szorosan integrálódott és összekapcsolt területét harmonizálna, amelyre már egységes szabályrendszer és felügyelet vonatkozik. Az olyan kérdésekben, mint az IKT-vonatkozású biztonsági események bejelentése, kizárólag harmonizált uniós szabályokkal mérsékelhetők az azzal összefüggő adminisztratív terhek és pénzügyi költségek, hogy ugyanazt az IKT-vonatkozású biztonsági eseményt különböző uniós és/vagy nemzeti hatóságoknál kell bejelenteni. A beavatkozás emellett megkönnyíti a teszteredmények kölcsönös elismertetését és elfogadtatását az olyan határokon átnyúló tevékenységet végző szervezetek számára, amelyek különböző tagállamokban eltérő tesztelési keretek hatálya alá tartoznak.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

Új kezdeményezés

1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák

E javaslat célkitűzése összhangban áll több más uniós szakpolitikával és folyamatban lévő kezdeményezéssel, különösen a hálózati és információs rendszerek biztonságáról szóló (kiberbiztonsági) irányelvvel és az európai kritikus infrastruktúrákról szóló irányelvvel. A javaslat megtartaná a horizontális kiberbiztonsági kerethez köthető előnyöket azáltal, hogy a kiberbiztonsági irányelv hatálya változatlanul kiterjedne a pénzügyi szolgáltatási alágazatra. A kiberbiztonsági irányelv ökoszisztémájával meglévő kapcsolódásai pontok megtartása lehetővé tenné a pénzügyi felügyeletek számára a releváns információk cseréjét a kiberbiztonsági hatóságokkal, valamint a részvételt a Kiberbiztonsági Együttműködési Csoportban. A javaslat nem lenne hatással a kiberbiztonsági irányelvre, inkább építene arra, az esetleges átfedéseket *lex specialis* mentesség keretében kezelné. A pénzügyi szolgáltatások szabályozása és a kiberbiztonsági irányelv közötti kölcsönhatásra továbbra is *lex specialis* záradék vonatkozna, amely érdemben mentesítené a pénzügyi szervezeteket a kiberbiztonsági irányelvben foglalt követelmények alól, és kiküszöbölné a két jogi aktus átfedéseit. Emellett a javaslat összhangban áll az európai kritikus infrastruktúrákról szóló irányelvvel, amelynek folyamatban lévő felülvizsgálata erősíteni kívánja a kritikus infrastruktúrák védelmét és rezilienciáját a kibertéren kívül megjelenő fenyegetésekkel szemben.

A javaslatnak nem lenne hatása a többéves pénzügyi keretre. Egyrészt a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók felvigyázási keretének finanszírozására teljes egészében az érintett szolgáltatóktól beszedett díjakból kerül majd sor; másrészt pedig az EFH-k a digitális működési rezilienciával kapcsolatos új szabályozási feladataikat a meglévő személyi állományuk belső átcsoportosításával látják el.

Ennek megfelelően a javaslat a hivatal engedélyezett személyi állományának bővítésesét is tartalmazza a soron következő éves költségvetési eljárás keretében. A hivatal továbbra is törekedni fog a minél nagyobb szinergiára és hatékonyságnövelésre (többek között informatikai rendszerek útján), és szoros figyelemmel kíséri a javaslattal összefüggő többlet-munkamennyiséget, ami megjelenik a hivatal által az éves költségvetési eljárás keretében igényelt engedélyezett létszámban is.

1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is

A Bizottság több finanszírozási alternatívát mérlegelt:

A járulékos költségek egyrészt fedezhetők az EFH-k szokásos finanszírozási mechanizmusának keretében. Ez azonban jelentősen megnövelné az EFH-k pénzügyi erőforrásaihoz való uniós hozzájárulást.

A javaslathoz kapcsolódó felügyeleti feladatokkal összefüggő költségek esetében ez a választott alternatíva. Az EFH-k felkérést kapnak meglévő munkatársaik átcsoportosítására technikai szabványok kidolgozása céljából. A harmadik félnek minősülő kulcsfontosságú szolgáltatók felvigyázásához kapcsolódó járulékos költségek azonban nem fedezhetők az EFH-k belső erőforrás-átcsoportosításával, mivel a hatóságoknak az e rendeletben foglaltakon kívül más uniós jogszabályokban meghatározott feladataik is vannak. Ezenfelül a digitális működési rezilienciához kapcsolódó felügyeleti feladatok speciális szakmai ismereteket és tapasztalatokat kívánnak meg. Mivel az EFH-k jelenleg nem rendelkeznek elegendő ilyen erőforrással, további erőforrásokra van szükségük.

Végül pedig a javaslat szerint a felvigyázás alá vont, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóknak díjfizetési kötelezettsége keletkezne. A javaslat értelmében a beszedett díj fedezné azokat a kiegészítő erőforrásokat, amelyeket az EFH-k az új feladatok és hatáskörök ellátásához igényelnek.

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

☐ **határozott időtartam**

☐ A javaslat/kezdeményezés időtartama: ÉÉÉÉ [HH/NN]-tól/-től ÉÉÉÉ [HH/NN]-ig

☐ Pénzügyi hatás: ÉÉÉÉ-tól/-től ÉÉÉÉ-ig

☑ **határozatlan időtartam**

Beindítási időszak: 2021-től;

azt követően: rendes ütem.

1.7. Tervezett irányítási módszer(ek)[51]

Bizottság általi **közvetlen irányítás**

☐ végrehajtó ügynökségeken keresztül

☐ **Megosztott irányítás** a tagállamokkal

☑ **Közvetett irányítás** a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

☐ nemzetközi szervezetek és ügynökségeik (nevezze meg);

☐ az EBB és az Európai Beruházási Alap;

☑ a 70. és 71. cikkben említett szervek;

☐ közjogi szervek;

☐ magánjog alapján működő, közfeladatot ellátó szervek, olyan mértékben, amennyiben megfelelő pénzügyi garanciákat nyújtanak;

☐ a valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek;

☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek.

Megjegyzések

N.a.

[51] Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a Költségvetési Főigazgatóság honlapján: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Gyakoriság és feltételek.

A már meglévő szabályoknak megfelelően az európai felügyeleti hatóságok rendszeresen tevékenységi jelentést készítenek (ideértve a felső vezetés felé irányuló belső jelentéstételt, a testületeknek tett jelentést és az éves jelentés elkészítését), és a Számvevőszék, valamint a Bizottság Belső Ellenőrzési Szolgálata ellenőrzést végez az erőforrások felhasználására és a teljesítményükre vonatkozóan. A javaslatban szereplő tevékenységek nyomon követése és az azokra vonatkozó jelentéstétel megfelel a meglévő követelményeknek és az e javaslatból eredő új követelményeknek.

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása

Az irányítás közvetetten, az európai felügyeleti hatóságokon keresztül történik. A finanszírozási mechanizmus végrehajtása az érintett, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóktól beszedett díjakból történik.

2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk

A javaslatból eredő előirányzatok jogszerű, gazdaságos, hatékony és eredményes felhasználása terén a javaslat várhatóan nem teremt olyan jelentős új kockázatokat, amelyekre ne terjedne ki a meglévő belső ellenőrzési keretrendszer. Mindazonáltal új kihívás is felmerülhet a díjaknak az érintett harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóktól megfelelő időben történő beszedése kapcsán.

2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)

Az európai felügyeleti hatóságokról szóló rendeletekben előírtaknak megfelelő irányítási és kontrollrendszereket már végrehajtották. Az európai felügyeleti hatóságok szorosan együttműködnek a Bizottság Belső Ellenőrzési Szolgálatával annak biztosítása érdekében, hogy a belső kontroll keretrendszerének valamennyi területén eleget tegyenek a megfelelő előírásoknak. E rendelkezések az e javaslatban az európai felügyeleti hatóságok számára előírt feladatkörök tekintetében is alkalmazandók lesznek. Emellett az Európai Parlament – a Tanács ajánlása alapján – minden pénzügyi évben megadja az egyes európai felügyeleti hatóságok számára a felmentést költségvetésük végrehajtására vonatkozóan.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket, pl. a csalás elleni stratégiából.

A csalás, a korrupció és bármely egyéb jogellenes tevékenység elleni fellépés érdekében az európai felügyeleti hatóságok vonatkozásában is megszorítások nélkül alkalmazandók az Európai Csalás Elleni Hivatal (OLAF) által lefolytatott vizsgálatokról szóló, 2013. szeptember 11-i 883/2013/EU, Euratom európai parlamenti és tanácsi rendelet előírásai.

Az európai felügyeleti hatóságok saját csalás elleni stratégiával és ebből következő cselekvési tervvel rendelkeznek. Az európai felügyeleti hatóságok által a csalás elleni küzdelem terén hozott megerősített intézkedések összhangban állnak majd a költségvetési rendeletben (csalás elleni intézkedések a hatékony és eredményes pénzgazdálkodás részeként), az OLAF csalásmegelőzési politikáiban, a Bizottság csalás elleni stratégiájában (COM(2011)376), valamint az uniós decentralizált ügynökségekre vonatkozó, 2012. júliusi közös megközelítésben és a kapcsolódó ütemtervben előírt rendelkezésekkel és útmutatásokkal.

Emellett az európai felügyeleti hatóságok létrehozásáról szóló rendeletek és az európai felügyeleti hatóságok költségvetésére vonatkozó rendeletek megállapítják az európai felügyeleti hatóságok költségvetésének végrehajtására és ellenőrzésére, valamint az alkalmazandó pénzügyi szabályokra vonatkozó rendelkezéseket, ideértve a csalás és más szabálytalanságok megelőzésére irányuló rendelkezéseket is.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási tétele/tételei

Jelenlegi költségvetési sorok

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési sorok sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	Type of kiadás	Hozzájárulás			
	Szám	Diff./nem diff.[52]	EFTA-országokt ól[53]	tagjelölt országoktól[54]	harmadik országokt ól	a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében

Létrehozandó új költségvetési sorok

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési sorok sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	Type of kiadás	Hozzájárulás			
	Szám	diff./nem diff.	EFTA-országokt ól	tagjelölt országoktól	harmadik országokt ól	a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében

[52] Diff. = Differenciált előirányzatok / Nem diff. = Nem differenciált előirányzatok.

[53] EFTA: Európai Szabadkereskedelmi Társulás.

[54] Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelöltek.

3.2. A kiadásokra gyakorolt becsült hatás

3.3. A kiadásokra gyakorolt becsült hatás összegzése

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret fejezete	Szám	Megnevezés

Főigazgatóság: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**ÖSSZESEN**
	Kötelezettségvállalási előirányzatok	(1)									
	Kifizetési előirányzatok	(2)									
Előirányzatok ÖSSZESEN <…> Főigazgatóság	Kötelezettségvállalási előirányzatok										
	Kifizetési előirányzatok										

A többéves pénzügyi keret fejezete		

millió EUR (három tizedesjegyig)

		2022	2023	2024	2025	2026	2027	ÖSSZESEN
Főigazgatóságok:								
• Humánerőforrás								
• Egyéb igazgatási kiadások <>								
Főigazgatóságok ÖSSZESEN	Előirányzatok							

Előirányzatok ÖSSZESEN (FEJEZET) többéves pénzügyi keret	(Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat)							

millió EUR (három tizedesjegyig) állandó árakon

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**ÖSSZESEN**
Előirányzatok ÖSSZESEN (1. FEJEZET) többéves pénzügyi keret	Kötelezettségvállalási előirányzatok							
	Kifizetési előirányzatok							

3.3.1. Az előirányzatokra gyakorolt becsült hatás

☑ A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását

☐ A javaslat/kezdeményezés az alábbi operatív előirányzatok felhasználását vonja maga után:

Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig) állandó árakon

Tüntesse fel a célkitűzéseket és a teljesítéseket ⇩			2022		2023		2024		2025		2026		2027		**ÖSSZESEN**	
	TELJESÍTÉSEK															
	Típus[55]	Átlagos költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Összesített szám	Teljes költség
1. KONKRÉT CÉLKITŰZÉS[56]…																
- Teljesítés																
1. konkrét célkitűzés részösszege																
2. KONKRÉT CÉLKITŰZÉS …																
- Teljesítés																
2. konkrét célkitűzés részösszege																
TELJES KÖLTSÉG																

55 A teljesítés a nyújtandó termékekre és szolgáltatásokra vonatkozik (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

56 Az 1.4.2. pontban leírtak szerint („Konkrét célkitűzés(ek)…”)

3.3.2. A humánerőforrásra gyakorolt becsült hatás

3.3.2.1. Összefoglalás

☐ A javaslat/kezdeményezés nem vonja maga után igazgatási előirányzatok felhasználását

☑ A javaslat/kezdeményezés az alábbi igazgatási előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig) állandó árakon

EBH, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**ÖSSZESEN**
Ideiglenes alkalmazottak (AD besorolási fokozat)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Ideiglenes alkalmazottak (AST besorolási fokozat)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Szerződéses munkatársak							
Kirendelt nemzeti szakértők							
ÖSSZESEN	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Személyzettel kapcsolatos követelmények (teljes munkaidős egyenérték):

EBH, EIOPA, ESMA és EEA	2022	2023	2024	2025	2026	2027	**ÖSSZESEN**
Ideiglenes alkalmazottak (AD besorolási fokozat) EBH=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Ideiglenes alkalmazottak (AST besorolási fokozat) EBH=1, EIOPA=1, EEA=1	3	3	3	3	3	3	3
Szerződéses munkatársak							
Kirendelt nemzeti szakértők							

ÖSSZESEN	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. A (felügyeletet ellátó) főigazgatóságoknál felmerülő, becsült humánerőforrás-szükségletek

☑ A javaslat/kezdeményezés nem igényel humánerőforrást.

☐ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

A becsléseket egész számmal (vagy legfeljebb egy tizedesjeggyel) kell kifejezni

		2022	2023	2024	2025	2026	2027
• **A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)**							
• **Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve**[57]							
XX 01 02 01 (AC, END, INT a teljes keretből)							
XX 01 02 02 (AC, AL, END, INT és JPD a küldöttségeknél)							
XX 01 04 ***éé***[58]	- a központban[59]						
	- a küldöttségeknél						
XX 01 05 02 (AC, END, INT – közvetett kutatás)							
10 01 05 02 (AC, END, INT – közvetlen kutatás)							
Egyéb költségvetési sor (kérjük megnevezni)							
ÖSSZESEN							

XX az érintett szakpolitikai terület vagy költségvetési cím.

A humánerőforrás-igényeknek az adott főigazgatóságok rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságokon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további juttatásokkal.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	
Külső munkatársak	

[57] AC = szerződéses alkalmazott; AL = helyi alkalmazott; END=kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

[58] Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

[59] Elsősorban a strukturális alapok, az Európai Mezőgazdasági Vidékfejlesztési Alap (EMVA) és az Európai Halászati Alap (EHA) esetében.

A teljes munkaidős egyenértékre jutó költség kiszámításának leírását bele kell foglalni az V. melléklet 3. szakaszába.

3.3.3. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

☑ A javaslat/kezdeményezés összeegyeztethető a jelenlegi többéves pénzügyi kerettel.

☐ A javaslat/kezdeményezés miatt szükséges a többéves pénzügyi keret vonatkozó fejezetének átprogramozása.

☐ A javaslat/kezdeményezés miatt szükség van a rugalmassági eszköz alkalmazására vagy a többéves pénzügyi keret felülvizsgálatára.[60]

Fejtse ki a szükségleteket: tüntesse fel az érintett fejezeteket és költségvetési sorokat és a megfelelő összegeket. […]

3.3.4. Harmadik felek részvétele a finanszírozásban

☐ A javaslat/kezdeményezés nem irányoz elő harmadik felek általi társfinanszírozást.

☑ A javaslat/kezdeményezés az alábbi becsült társfinanszírozást irányozza elő:

millió EUR (három tizedesjegyig)

EBH

	2022	2023	2024	2025	2026	2027	Összesen
A költségeket 100 %-ban a felügyelet alá vont szervezetektől beszedett díjak fedezik[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Társfinanszírozott előirányzatok ÖSSZESEN	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Összesen
A költségeket 100 %-ban a felügyelet alá vont szervezetektől beszedett díjak fedezik[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Társfinanszírozott előirányzatok ÖSSZESEN	1,305	1,811	1,611	1,611	1,611	1,611	9,560

[60] Lásd a 2014–2020-as időszakra vonatkozó többéves pénzügyi keretről szóló 1311/2013/EU, Euratom tanácsi rendelet 11. és 17. cikkét.

[61] A teljes becsült költség 100 %-a és a munkáltatói nyugdíjjárulék teljes összege.

[62] A teljes becsült költség 100 %-a és a munkáltatói nyugdíjjárulék teljes összege.

ESMA

	2022	2023	2024	2025	2026	2027	Összesen
A költségeket 100 %-ban a felügyelet alá vont szervezetektől beszedett díjak fedezik[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Társfinanszírozott előirányzatok ÖSSZESEN	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. A bevételre gyakorolt becsült hatás

☑ A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre.

☐ A javaslatnak/kezdeményezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:

- ☐ a saját forrásokra gyakorol hatást
- ☐ más bevételre gyakorol hatást
- ☐ kérjük, adja meg, hogy a bevétel kiadási sorhoz van-e rendelve

millió EUR (három tizedesjegyig)

Bevételi költségvetési sor:	A folyó pénzügyi évben rendelkezésre álló előirányzatok	A javaslat/kezdeményezés hatása[64]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető		
… jogcímcsoport								

Az egyéb címzett bevételek esetében tüntesse fel az érintett kiadáshoz tartozó költségvetési sort vagy sorokat.

[…]

Ismertesse a bevételre gyakorolt hatás számításának módszerét.

[…]

63 A teljes becsült költség 100 %-a és a munkáltatói nyugdíjjárulék teljes összege.

64 A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összeget kell megadni, amely a 20 %-kal (beszedési költségek) csökkentett bruttó összegnek felel meg.

MELLÉKLET

Általános feltételezések

I. cím – Személyzeti kiadások

Az azonosított munkaerőigényen alapuló személyzeti kiadások számításában alábbi konkrét feltételezések érvényesültek:

- Az új személyzet 2022. évi felvételével kapcsolatos költségtervezés a felvétel feltételezett időigényére tekintettel 6 hónapra szól
- Egy ideiglenes alkalmazott átlagos éves költsége 150 000 EUR, amely 25 000 EUR „kiigazítási” költséget (épület, IT stb.) is magában foglal
- A személyzeti illetményre alkalmazandó korrekciós szorzó Párizs (EBH, ESMA) esetében 117,7, Frankfurt (EIOPA) esetében 99,4
- Az ideiglenes alkalmazottak után fizetendő munkáltatói nyugdíjjárulék alapja az átlagos éves standard költségben foglalt általános alapilletmény, 95 660 EUR
- A további ideiglenes alkalmazottak besorolása AD5 és AST

II. cím – Infrastrukturális és működési kiadások

A költségek számítása a létszám, a foglalkoztatás éven belüli időaránya, valamint az általános „kiigazítási” költség (25 000 EUR) szorzatán alapul.

III. cím – Operatív kiadások

A költségek becslése az alábbi feltételezéseken alapul:

- A tervezett fordítási költségek mindegyik EFH esetében évente 350 000 EUR-t tesznek ki
- Az egyes EFH-k egyszeri 500 000 EUR összegű informatikai költsége a feltételezés szerint a 2022. és a 2023. év között oszlik meg 50-50 % arányban. 2024-től az éves fenntartási költségek becsült összege az EFH-k mindegyike esetében 50 000 EUR
- A helyszíni felügyeleti tevékenységek költségének becsült éves összege az EFH-k mindegyike esetében 200 000 EUR

A fent közölt becslésekből az alábbi éves költségek adódnak:

A többéves pénzügyi keret fejezete	Szám	

Állandó árak

EBH:			2022	2023	2024	2025	2026	2027	ÖSSZESEN
1. cím:	Kötelezettségvállalási előirányzatok	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Kifizetési előirányzatok	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
2. cím:	Kötelezettségvállalási előirányzatok	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Kifizetési előirányzatok	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3. cím:	Kötelezettségvállalási előirányzatok	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Kifizetési előirányzatok	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Előirányzatok ÖSSZESEN az EBH számára:	Kötelezettségvállalási előirányzatok	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Kifizetési előirányzatok	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	ÖSSZESEN
1. cím:	Kötelezettségvállalási előirányzatok	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Kifizetési előirányzatok	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
2. cím:	Kötelezettségvállalási előirányzatok	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825

	Kifizetési előirányzatok	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3. cím:	Kötelezettségvállalási előirányzatok	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Kifizetési előirányzatok	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Előirányzatok ÖSSZESEN az EIOPA számára:	Kötelezettségvállalási előirányzatok	=1+1a+3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Kifizetési előirányzatok	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**ÖSSZESEN**
1. cím:	Kötelezettségvállalási előirányzatok	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Kifizetési előirányzatok	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
2. cím:	Kötelezettségvállalási előirányzatok	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Kifizetési előirányzatok	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3. cím:	Kötelezettségvállalási előirányzatok	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Kifizetési előirányzatok	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Előirányzatok ÖSSZESEN az ESMA számára:	Kötelezettségvállalási előirányzatok	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Kifizetési előirányzatok	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

A javaslat az alábbi operatív előirányzatok felhasználását vonja maga után:

Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig) állandó árakon

EBH

Tüntesse fel a célkitűzéseket és a teljesítéseket ⇩			2022		2023		2024		2025		2026		2027			
	TELJESÍTÉSEK															
	Típus[65]	Átlagos költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Összesített szám	Teljes költség
1. KONKRÉT CÉLKITŰZÉS[66] Harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók közvetlen felvigyázása																
- Teljesítés				0,800		0,800		0,600		0,600		0,600		0,600		4,000
1. konkrét célkitűzés részösszege																
2. KONKRÉT CÉLKITŰZÉS …																
- Teljesítés																
2. konkrét célkitűzés részösszege																
TELJES KÖLTSÉG				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Tüntesse fel a célkitűzéseket és a teljesítéseket ⇩			2022		2023		2024		2025		2026		2027			
	TELJESÍTÉSEK															
	Típus[67]	Átlagos költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Összesített szám	Teljes költség
1. KONKRÉT CÉLKITŰZÉS[68] Harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók közvetlen felvigyázása																

[65] A teljesítés a nyújtandó termékekre és szolgáltatásokra vonatkozik (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

[66] Az 1.4.2. pontban leírtak szerint („Konkrét célkitűzés(ek)…”).

[67] A teljesítés a nyújtandó termékekre és szolgáltatásokra vonatkozik (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

[68] Az 1.4.2. pontban leírtak szerint („Konkrét célkitűzés(ek)…”).

- Teljesítés				0,800		0,800		0,600		0,600		0,600		0,600		4,000
1. konkrét célkitűzés részösszege																
2. KONKRÉT CÉLKITŰZÉS …																
- Teljesítés																
2. konkrét célkitűzés részösszege																
TELJES KÖLTSÉG				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Tüntesse fel a célkitűzéseket és a teljesítéseket ⇩			2022		2023		2024		2025		2026		2027			
	TELJESÍTÉSEK															
	Típus[69]	Átlagos költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Összesített szám	Teljes költség
1. KONKRÉT CÉLKITŰZÉS[70] Harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók közvetlen felvigyázása																
- Teljesítés				0,800		0,800		0,600		0,600		0,600		0,600		4,000
1. konkrét célkitűzés részösszege																
2. KONKRÉT CÉLKITŰZÉS …																
- Teljesítés																
2. konkrét célkitűzés részösszege																
TELJES KÖLTSÉG				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

A felvigyázási tevékenységek finanszírozása teljes mértékben a felvigyázás alá vont szervezetektől beszedett díjakból történik az alábbiak szerint:

EBH

[69] A teljesítés a nyújtandó termékekre és szolgáltatásokra vonatkozik (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

[70] Az 1.4.2. pontban leírtak szerint („Konkrét célkitűzés(ek)…”).

	2022	2023	2024	2025	2026	2027	Összesen
A költségeket 100 %-ban a felvigyázás alá vont szervezetektől beszedett díjak fedezik[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Társfinanszírozott előirányzatok ÖSSZESEN	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Összesen
A költségeket 100 %-ban a felvigyázás alá vont szervezetektől beszedett díjak fedezik[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Társfinanszírozott előirányzatok ÖSSZESEN	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Összesen
A költségeket 100 %-ban a felvigyázás alá vont szervezetektől beszedett díjak fedezik[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Társfinanszírozott előirányzatok ÖSSZESEN	1,373	1,948	1,748	1,748	1,748	1,748	10,313

RÉSZLETES INFORMÁCIÓK

Közvetlen felvigyázási hatáskörök

Bevezetésként újból kiemelendő, hogy az ESMA közvetlen felügyelete alatt álló szervezetek kötelesek az ESMA számára díjakat fizetni (egyszeri nyilvántartásba vételi díjat és rendszeres díjakat a folyamatos felügyeletért). Ez vonatkozik a hitelminősítő intézetekre (lásd: 272/2012/EU felhatalmazáson alapuló bizottsági rendelet) és a kereskedési adattárakra (1003/2013/EU felhatalmazáson alapuló bizottsági rendelet).

A jogalkotási javaslat szerint az EFH-k új feladatkört kapnak, amelynek célja, hogy előmozdítsa a pénzügyi ágazat harmadik féltől eredő IKT-kockázatával kapcsolatos

[71] A teljes becsült költség 100 %-a és a munkáltatói nyugdíjjárulék teljes összege.
[72] A teljes becsült költség 100 %-a és a munkáltatói nyugdíjjárulék teljes összege.
[73] A teljes becsült költség 100 %-a és a munkáltatói nyugdíjjárulék teljes összege.

felügyeleti megközelítések konvergenciáját azáltal, hogy a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra is kiterjeszti az uniós felvigyázási keret hatályát.

Az e javaslatban meghatározott felvigyázási keret a pénzügyi szolgáltatások területén meglévő intézményi struktúrára épít úgy, hogy az EFH-k vegyes bizottsága – a kiberbiztonsággal kapcsolatos feladataival összhangban – biztosítja az ágazatközi koordinációt az IKT-kockázatot érintő valamennyi kérdésben, ennek során pedig a harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatókra vonatkozó egyedi döntéseket és a részükre megfogalmazott kollektív ajánlásokat előkészítő releváns albizottság (felvigyázási fórum) munkájára támaszkodik.

E keretben az egyes harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók vezető felvigyázójaként kijelölt EFH olyan hatásköröket kap, amelyeket gyakorolva biztosíthatja a pénzügyi ágazat működésében kulcsfontosságú szerepet betöltő technológiai szolgáltatók megfelelő, páneurópai léptékű figyelemmel kísérését. A javaslatban meghatározott felvigyázási feladatokat az indokolás pontosítja. Ezek közé a következők tartoznak: az általános vizsgálat és ellenőrzés lefolytatásához szükséges releváns információk és dokumentumok bekérésére, az ajánlások megfogalmazására, majd az ajánlások kapcsán végrehajtott korrekciós és egyéb intézkedésekkel kapcsolatos jelentések benyújtására vonatkozó jogosultságok.

Az e javaslatban előirányzott új feladatok ellátása érdekében az EFH-k az IKT-kockázatra szakosodott, a harmadik felektől való függőségeket értékelő új munkatársakat vesznek fel.

A hatóságonként becsült humánerőforrás-igény 6 teljes munkaidős alkalmazott (5 AD és az őket támogató 1 AST). Az EFH-knál emellett járulékos informatikai költségek is felmerülnek, amelyek becsült mértéke 500 000 EUR egyszeri költség, valamint a három EFH mindegyike esetében 50 000 EUR éves fenntartási költség. Az új feladatok ellátásának lényeges elemét adják a helyszíni vizsgálatok és ellenőrzések elvégzésére szóló megbízások, amelyek becsült költsége mindegyik EFH esetében évente 200 000 EUR. A harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatók által az EFH-knak átadott különféle dokumentumok tervezett éves fordítási költsége 350 000 EUR, amelyet az operatív kiadások sora tartalmaz.

A felsorolt igazgatási költségeket teljes mértékben az EFH-k által a felvigyázás alá vont, harmadik félnek minősülő kulcsfontosságú IKT-szolgáltatóktól beszedett éves díjak fedezik (nincsenek hatással az uniós költségvetésre).