Iránymutatások

EBA/GL/2019/04

2019. november 28.

Az IKT- és biztonsági kockázatok kezelésére vonatkozó EBH iránymutatások

Megfelelőségi és jelentéstételi kötelezettségek

Az iránymutatások jogállása

1. Az e dokumentumban szereplő iránymutatásokat az 1093/2010/EU rendelet[1] 16. cikkének rendelkezéseivel összhangban adták ki. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése szerint az illetékes hatóságok és pénzügyi intézmények minden erőfeszítést megtesznek azért, hogy megfeleljenek az iránymutatásoknak.

2. Az iránymutatások az EBH azzal kapcsolatos álláspontját ismertetik, hogy mi a megfelelő felügyeleti gyakorlat a Pénzügyi Felügyeletek Európai Rendszerében, és miként kell alkalmazni az Európai Unió jogát egy adott területen belül. Az 1093/2010/EU rendelet 4. cikkének (2) bekezdésében meghatározott, az iránymutatások hatálya alá tartozó illetékes hatóságok azzal tesznek eleget az iránymutatásoknak, hogy megfelelően beépítik azt saját felügyeleti gyakorlataikba (pl. saját jogi kereteik vagy felügyeleti folyamataik módosításával), beleértve azokat az eseteket is, ahol az iránymutatások elsősorban intézményekre vonatkoznak.

Jelentéstételi követelmények

3. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése értelmében az egyes illetékes hatóságok éééé.hh.nn-ig kötelesek értesíteni az EBH-t arról, hogy megfelelnek-e, vagy meg kívánnak-e felelni ezeknek az iránymutatásoknak, és ha nem, úgy tájékoztatniuk kell az EBH-t a meg nem felelés indokairól. Amennyiben a fenti határidőig ilyen értesítés nem érkezik, az EBH úgy tekinti, hogy a szóban forgó hatáskörrel rendelkező hatóság nem felel meg az iránymutatásoknak. Az értesítéseket „EBA/GL/2019/04” hivatkozással az EBH honlapján szereplő formanyomtatványon kell megküldeni a compliance@eba.europa.eu címre. Az értesítést olyan személynek kell benyújtania, aki megfelelő felhatalmazással rendelkezik arra, hogy a felügyeletet ellátó hatósága nevében nyilatkozzon annak megfeleléséről. Az EBH-nak megfeleléssel kapcsolatban bekövetkező bármely változást is be kell jelenteni.

4. Az értesítéseket a 16. cikk (3) bekezdésével összhangban közzéteszik az EBH honlapján.

[1] Az Európai Parlament és a Tanács 1093/2010/EU rendelete (2010. november 24.) az európai felügyeleti hatóság (Európai Bankhatóság) létrehozásáról, a 716/2009/EK határozat módosításáról és a 2009/78/EK bizottsági határozat hatályon kívül helyezéséről (HL L 331., 2010.12.15., 12. o.).

Tárgy, alkalmazási kör és fogalommeghatározások

Tárgy

5. Ezek az iránymutatások a belső irányítás tekintetében a 2013/36/EU irányelv (tőkekövetelmény-irányelv) 74. cikkében foglalt rendelkezésekre épülnek, és az (EU) 2015/2366 irányelv (második pénzforgalmi szolgáltatási irányelv) 95. cikkének (3) bekezdésében meghatározott, iránymutatások közzétételére irányuló megbízatásból erednek.

6. Az iránymutatások meghatározzák azokat a kockázatkezelési intézkedéseket, amelyeket a (9. bekezdésben meghatározott) pénzügyi intézményeknek meg kell tenniük a tőkekövetelmény-irányelv 74. cikkével összhangban annak érdekében, hogy kezeljék az IKT- és a biztonsági kockázataikat valamennyi tevékenységük esetében, továbbá azokat, amelyeket a (9. bekezdésben meghatározott) pénzforgalmi szolgáltatóknak a második pénzforgalmi szolgáltatási irányelv 95. cikkének (1) bekezdésével összhangban meg kell tenniük az általuk nyújtott pénzforgalmi szolgáltatásokkal kapcsolatos működési és biztonsági kockázatok kezelése érdekében. Az iránymutatások tartalmazzák az információbiztonság követelményeit, beleértve a kiberbiztonságot is, amennyiben az információkat IKT-rendszerekben tárolják.

Alkalmazási kör

7. Az iránymutatások a (9. bekezdésben meghatározottak szerinti) pénzügyi intézményeken belüli IKT- és biztonsági kockázatok kezelésére vonatkoznak. Az iránymutatások alkalmazásában az IKT- és biztonsági kockázat kifejezés a fizetési szolgáltatások nyújtásának a második pénzforgalmi szolgáltatási irányelv 95. cikkében foglalt működési és biztonsági kockázatait jelenti.

8. A (9. bekezdésben meghatározottak szerinti) pénzforgalmi szolgáltatók esetében az iránymutatások a fizetési szolgáltatások nyújtására vonatkoznak a második pénzforgalmi szolgáltatási irányelv 95 cikkének hatályával és az abban foglalt megbízatással összhangban. A (9. bekezdésben meghatározottak szerinti) intézmények esetében az iránymutatások az általuk végzett összes tevékenységre vonatkoznak.

Címzettek

9. Ezen iránymutatások címzettjei a pénzügyi intézmények, amelyek ezen iránymutatások alkalmazásában (1) a második pénzforgalmi szolgáltatási irányelv 4. cikke (11) bekezdésében meghatározott pénzforgalmi szolgáltatók, és (2) intézmények, azaz a 2013/575/EU rendelet 4. cikke (1) bekezdésének 3. pontjában meghatározott hitelintézetek és befektetési vállalkozások. Az iránymutatások vonatkoznak továbbá a 2013/575/EU rendelet 4. cikke (1) bekezdésének 40. pontjában meghatározott illetékes hatóságokra – beleértve az Európai

Központi Bankot – az 1024/2013/EU rendelet által rájuk ruházott feladatokkal kapcsolatos kérdések vonatkozásában, valamint a második pénzforgalmi szolgáltatási irányelv szerinti hatáskörrel rendelkező hatóságokra, az 1093/2010/EU rendelet 4. cikke (2) bekezdésének ii. pontjában említettek szerint.

Fogalommeghatározások

10. Eltérő rendelkezés hiányában a 2013/36/EU irányelvben (a tőkekövetelmény-irányelv), a 575/2013/EU rendeletben (a tőkekövetelmény-rendelet) és a 2015/2366/EU irányelvben (második pénzforgalmi szolgáltatási irányelv) használt és meghatározott fogalmak ebben az iránymutatásban is az említett rendeletben, illetve irányelvekben használt jelentéssel bírnak. Ezen túlmenően az iránymutatások alkalmazásában a következő fogalmak az alábbi jelentéssel bírnak:

IKT- és biztonsági kockázat	A bizalmasság megsértéséből, a rendszerek és adatok sértetlenségének sérüléséből, a rendszerek és adatok nem megfelelőségéből vagy elérhetetlenségéből, illetve a környezeti vagy üzleti követelmények változása esetén az információs technológia (IT) észszerű időn belül és költségekkel járó megváltoztatására való (agilitás) képtelenségből adódó veszteség kockázata[2]. Ide tartoznak a nem megfelelő vagy rosszul működő belső folyamatokból vagy külső eseményekből eredő biztonsági kockázatok, beleértve a kibertámadásokat vagy a nem megfelelő fizikai biztonságot is.
Vezető testület	(a) Hitelintézetek és befektetési vállalkozások esetében ez a kifejezés a 2013/36/EU irányelv 3. cikke (1) bekezdésének 7. pontjában foglalt fogalommeghatározással megegyező jelentéssel bír. (b) A pénzforgalmi intézmények vagy elektronikuspénz-kibocsátó intézmények esetében ez a kifejezés a pénzforgalmi intézmények vagy elektronikuspénz-kibocsátó intézmények vezető tisztségviselőit vagy az irányításért felelős tisztségviselőket, valamint adott esetben a pénzforgalmi intézmények vagy elektronikuspénz-kibocsátó intézmények pénzforgalmi szolgáltatási tevékenységeinek irányításáért felelős tisztségviselőket jelenti. (c) Az (EU) 2015/2366 irányelv 1. cikke (1) bekezdésének c), e) és f) pontjában említett pénzforgalmi szolgáltatók tekintetében ez a kifejezés az alkalmazandó uniós vagy nemzeti jogban az e kifejezéshez rendelt jelentéssel bír.

[2] Az EBH 2014. december 19-i, „Iránymutatás a felügyeleti felülvizsgálati és értékelési folyamat közös eljárásairól és módszertanairól” című, az EBA/GL/2018/03 dokumentummal módosított iránymutatásából (EBA/GL/2014/13) származó fogalommeghatározás.

Működési vagy biztonsági incidens	A pénzügyi intézmény által előre nem tervezett olyan egyedi esemény vagy egymáshoz kapcsolódó események olyan sorozata, amelynek negatív hatása van vagy lehet a szolgáltatások sértetlenségére, rendelkezésre állására, bizalmasságára és/vagy hitelességére.
Felső vezetés	(a) Hitelintézetek és befektetési vállalkozások esetében ez a kifejezés a 2013/36/EU irányelv 3. cikke (1) bekezdésének 9. pontjában foglalt fogalommeghatározással megegyező jelentéssel bír. (b) A pénzforgalmi intézmények vagy elektronikuspénz-kibocsátó intézmények esetében, ez a kifejezés az intézménynél vezetői feladatot ellátó természetes személyeket jelenti, akik felelősek és elszámoltathatók a vezető testület előtt az intézmény mindennapi vezetéséért; (c) Az (EU) 2015/2366 irányelv 1. cikke (1) bekezdésének c), e) és f) pontjában említett pénzforgalmi szolgáltatók tekintetében ez a kifejezés az alkalmazandó uniós vagy nemzeti jogban az e kifejezéshez rendelt jelentéssel bír.
Kockázati étvágy	A kockázat azon aggregált szintje és típusai, amelyeket a pénzforgalmi szolgáltatók és intézmények stratégiai céljaik megvalósítása érdekében, kockázatvállalási képességük keretein belül, üzleti modelljükkel összhangban hajlandók vállalni.
Ellenőrzési funkció	(a) Hitelintézetek és befektetési vállalkozások esetében az EBH belső irányításról szóló iránymutatásának (EBA/GL/2017/11) 22. pontjában említett ellenőrzési (audit) funkció. (b) Azon pénzforgalmi szolgáltatók esetében, amelyek nem hitelintézetek, az ellenőrzési funkciónak függetlennek kell lennie a pénzforgalmi szolgáltatón belül vagy magától a szolgáltatótól, és lehet belső és/vagy külső ellenőrzési funkció.
IKT-projektek	Minden olyan projekt vagy annak egy része, amely keretében IKT-rendszereket és szolgáltatásokat módosítanak, cserélnek le, szüntetnek meg vagy vezetnek be. Az IKT-projektek szélesebb körű IKT- vagy vállalatátalakítási programok részét is képezhetik.
Harmadik fél	Egy olyan szervezet, amely termék vagy szolgáltatás nyújtása céljából üzleti kapcsolatot létesített vagy szerződést kötött egy pénzügyi intézménnyel [3].
Információs vagyonelem	Olyan, kézzelfogható vagy nem kézzelfogható információhalmaz, amelyet érdemes megvédeni.
IKT-eszköz	Olyan szoftver vagy hardver eszköz, amely megtalálható az üzleti környezetben.

[3] A G7-ek „Harmadik felek kiberkockázat-kezelésének alapvető elemei a pénzügyi ágazatban” című dokumentumából származó fogalommeghatározás.

IKT-rendszerek[4]	Egy pénzügyi intézmény működését támogató mechanizmus vagy összekapcsolt hálózat részét képező információs és kommunikációs technológiai eszközök
IKT-szolgáltatások[5]	Az IKT-rendszerek által egy vagy több belső vagy külső felhasználónak nyújtott szolgáltatások. Erre példaként szolgálnak az adatbeviteli, adattárolási, adatfeldolgozási és jelentésszolgálati szolgáltatások, de ide tartoznak a monitorozási-, valamint üzleti és döntéstámogatási szolgáltatások is.

Végrehajtás

Alkalmazás időpontja

11. A jelen iránymutatások 2020. június 30. napjától hatályosak.

Hatályon kívül helyezés

12. Ez az iránymutatás az alkalmazandóvá válásának időpontjában hatályon kívül helyezi a működési és biztonsági kockázatokkal kapcsolatos biztonsági intézkedésekről szóló, 2017-ben közzétett iránymutatásokat (EBA/GL/2017/17).

Az IKT- és biztonsági kockázatok kezelésére vonatkozó iránymutatás

1.1. Arányosság

1. Az összes pénzügyi intézménynek úgy kell megfelelnie a jelen iránymutatásban meghatározott rendelkezéseknek, hogy az figyelembe vegye és arányos legyen a pénzügyi intézmény méretével, belső szervezetével, a pénzügyi intézmény által nyújtott vagy nyújtani tervezett szolgáltatások és termékek jellegével, körével, összetettségével és kockázatosságával.

1.2. Irányítás és stratégia

1.2.1. Irányítás

2. A vezető testületnek biztosítania kell, hogy a pénzügyi intézmény az IKT- és biztonsági kockázatai tekintetében megfelelő belső irányítási és belső ellenőrzési keretrendszerrel rendelkezzen. A vezető testületnek világos szerep- és felelősségi köröket kell meghatároznia az

[4] Az IKT-kockázatok felügyeleti felülvizsgálati és értékelési eljárás (EBH SREP) keretében történő értékeléséről szóló iránymutatásokból (EBA/GL/ 2017/05) származó fogalommeghatározás.
[5] ugyanott.

IKT-funkciók, az információbiztonsági kockázatok kezelése és üzletmenet-folytonosság vonatkozásában, beleértve a vezető testület és bizottságainak szerep- és felelősségi köreit is.

3. A vezető testületnek biztosítania kell, hogy a pénzügyi intézmény személyzetének létszáma és szakértelme megfelelő legyen az IKT működési szükségleteinek, valamint az IKT- és biztonsági kockázatkezelési folyamatainak folyamatos támogatásához, továbbá az IKT-stratégiája megvalósításának biztosításához. A vezető testületnek biztosítania kell, hogy az előirányzott költségkeret megfelelő legyen a fentiek megvalósításához. Ezenfelül a pénzügyi intézménynek biztosítania kell, hogy személyzetének összes tagja, beleértve a kulcsfontosságú feladatot ellátó személyeket, évente, vagy szükség szerint gyakrabban, megfelelő képzésben részesüljenek az IKT- és biztonsági kockázatokról, beleértve az információbiztonságot is (lásd még 1.4.7. pontot).
4. A vezető testület általánosan elszámoltatható a pénzügyi intézmény általános üzleti stratégiájának részét képező IKT-stratégiájának kidolgozásáért, jóváhagyásáért és végrehajtásának felügyeletéért, valamint az IKT- és biztonsági kockázatok hatékony kockázatkezelési keretrendszerének kidolgozásáért.

1.2.2. Stratégia

5. Az IKT-stratégiát össze kell hangolni a pénzügyi intézmény általános üzleti stratégiájával, és a stratégiának a következőket kell meghatároznia:
    a) a pénzügyi intézmény IKT-jának fejlesztési szükségleteit annak érdekében, hogy az hatékonyan támogassa és részt vegyen az üzleti stratégia megvalósításában, ideértve a szervezeti felépítés fejlesztését, az IKT-rendszer változtatásait és a harmadik felekkel szembeni fő függőségeket;
    b) az IKT architektúrájának tervezett stratégiáját és fejlesztését, beleértve a harmadik felekkel szembeni függőségeket is;
    c) világos információbiztonsági célkitűzéseket, amelyek az IKT-rendszerekre és IKT-szolgáltatásokra, továbbá az alkalmazottakra és a folyamatokra irányulnak.
6. A pénzügyi intézményeknek cselekvési terveket kell kidolgozniuk, amelyek tartalmazzák az IKT-stratégia céljának elérése érdekében meghozandó intézkedéseket. Ezeket közölni kell az összes érintett alkalmazottal (ideértve a vállalkozókat és harmadik fél szolgáltatókat is, amennyiben ez értelmezhető és releváns). A cselekvési terveket rendszeresen felül kell vizsgálni naprakészségük és megfelelőségük biztosítása érdekében. Továbbá a pénzügyi intézményeknek folyamatokat kell kidolgozniuk az IKT-stratégiájuk végrehajtási hatékonyságának nyomon követésére és mérésére.

1.2.3. Harmadik fél szolgáltatók igénybevétele

7. A kiszervezésről szóló EBH iránymutatás (EBA/GL/2019/02) és a második pénzforgalmi szolgáltatási irányelv 19. cikkének sérelme nélkül, a pénzügyi intézményeknek biztosítaniuk kell a kockázatkezelési keretrendszerükben meghatározottak szerinti kockázatcsökkentő intézkedések hatékonyságát, beleértve a jelen irányelvekben meghatározott intézkedéseket, amikor a fizetési szolgáltatások és/vagy IKT-szolgáltatások, vagy bármely tevékenység IKT-

rendszereinek működési tevékenységeit kiszervezik, ideértve a csoporthoz tartozó szervezethez történő kiszervezést, vagy harmadik felek igénybe vételét.

8. Az IKT-szolgáltatások és IKT-rendszerek folytonosságának biztosítása érdekében a pénzügyi intézményeknek gondoskodniuk kell arról, hogy a szolgáltatókkal (kiszervezést végző szolgáltatókkal, csoporthoz tartozó szervezetekkel vagy harmadik fél szolgáltatókkal) kötött szerződések és szolgáltatási szint megállapodások (mind a rendes körülményekre, mind a szolgáltatás zavarára vonatkozóan – lásd még a 1.7.2. pontot) tartalmazzák a következőket:

   a) megfelelő és arányos információbiztonsággal kapcsolatos célok és intézkedések, beleértve olyan követelményeket, mint például kiberbiztonsági minimumkövetelmények; a pénzügyi intézmény adatainak életciklusára vonatkozó specifikációk; az adatok titkosításával, a hálózatbiztonsággal és a biztonsági monitorozási folyamatokkal, valamint az adatközpontok elhelyezkedésével kapcsolatos követelmények;
   b) működési és biztonsági incidensek kezelésének eljárásai, beleértve az eszkalációt és a jelentéstételt.

9. A pénzügyi intézményeknek nyomon kell követniük és bizonyosságot kell szerezniük arról, hogy az említett szolgáltatók mennyire felelnek meg a pénzügyi intézmény biztonsági céljainak, intézkedéseinek és teljesítménycéljainak.

1.3. IKT- és biztonsági kockázatkezelési keretrendszer

1.3.1. Szervezet és célkitűzések

10. A pénzügyi intézményeknek azonosítaniuk és kezelniük kell az IKT- és biztonsági kockázataikat. Az IKT-rendszerekért, folyamatokért és biztonsági műveletekért felelős IKT-funkció(k)nak megfelelő folyamatokkal és kontrollokkal kell rendelkezniük, melyek biztosítják, hogy minden kockázatot azonosítsanak, elemezzenek, mérjenek, nyomon kövessenek, kezeljenek, jelentsenek és a pénzügyi intézmény kockázati étvágyának keretein belül tartsanak, továbbá, hogy az általuk kezelt projektek és rendszerek, valamint az általuk végrehajtott tevékenységek összhangban legyenek a külső és belső követelményekkel.

11. A pénzügyi intézményeknek az IKT- és a biztonsági kockázatok kezelésének és felügyeletének felelősségét egy ellenőrző funkcióra kell bízniuk, betartva az EBH belső irányításról szóló iránymutatásának (EBA/GL/2017/11) 19. pontjában foglalt követelményeket. A pénzügyi intézményeknek biztosítaniuk kell az ellenőrző funkció függetlenségét és objektivitását az IKT működési folyamataitól történő megfelelő elkülönítéssel. Ennek az ellenőrző funkciónak közvetlenül a vezető testület felé kell elszámoltathatónak lennie, továbbá felelősnek kell lennie az IKT- és biztonsági kockázatkezelési keretrendszer betartásának nyomon követéséért és ellenőrzéséért. Biztosítania kell az IKT-kockázatok és a biztonsági kockázatok azonosítását, mérését, értékelését, kezelését, nyomon követését és jelentését. A pénzügyi intézményeknek biztosítaniuk kell, hogy ez az ellenőrző funkció ne legyen felelős semmilyen belső ellenőrzésért.

    A belső ellenőrzési funkciónak kockázatalapú megközelítés alapján képesnek kell lennie arra, hogy függetlenül megvizsgálja a pénzügyi intézmény IKT-val és biztonsággal kapcsolatos összes

tevékenységének és egységének a pénzügyi intézmény szabályzatainak és eljárásainak, valamint a külső követelményeknek való megfelelését, és erre vonatkozóan objektív bizonyosságot nyújtson, betartva az EBH belső irányításról szóló iránymutatása (EBA/GL/2017/11) 22. pontjának követelményeit.

12. A pénzügyi intézményeknek meg kell határozniuk és ki kell osztaniuk a kulcsfontosságú szerepeket és felelősségeket, valamint a vonatkozó jelentési útvonalakat annak érdekében, hogy az IKT- és biztonsági kockázatkezelési keretrendszer hatékony legyen. Ezt a keretrendszert teljes mértékben be kell építeni a pénzügyi intézmények általános kockázatkezelési folyamataiba és össze kell hangolni azokkal.

13. Az IKT- és biztonsági kockázatkezelési keretrendszernek a következőket biztosító folyamatokat kell tartalmaznia:

    a) a kockázati étvágy meghatározása az IKT- és biztonsági kockázatok vonatkozásában, a pénzügyi intézmény kockázati étvágyával összhangban;
    b) azon IKT- és biztonsági kockázatok azonosítása és értékelése, amelyeknek a pénzügyi intézmény ki van téve;
    c) az IKT- és biztonsági kockázatok mérséklését célzó kockázatcsökkentő intézkedések meghatározása, ideértve az ellenőrzéseket is;
    d) ezen intézkedések hatékonyságának, valamint a bejelentett incidensek számának nyomon követése, ideértve a pénzforgalmi szolgáltatók esetében a második pénzforgalmi szolgáltatási irányelv 96. cikkével összhangban bejelentett, és az IKT-val kapcsolatos tevékenységeket érintő incidenseket, továbbá szükség esetén az intézkedések helyesbítését szolgáló lépések megtétele;
    e) jelentéstétel a vezető testületnek az IKT- és biztonsági kockázatokról és ellenőrzésekről;
    f) annak azonosítása és felmérése, hogy vannak-e IKT- és biztonsági kockázatok az IKT-rendszerben vagy az IKT-szolgáltatásokban, a folyamatokban vagy eljárásokban bekövetkezett bármilyen jelentős változás eredményeként és/vagy bármilyen jelentős működési vagy biztonsági incidenst követően.

14. A pénzügyi intézményeknek biztosítaniuk kell, hogy az IKT- és biztonsági kockázatkezelési keretrendszert dokumentálják és folyamatosan fejlesszék a bevezetése és nyomon követése során szerzett tapasztalatok alapján. Az IKT- és biztonsági kockázatkezelési keretrendszert a vezető testületnek jóvá kell hagynia és legalább évente egyszer felül kell vizsgálnia.

1.3.2. A funkciók, a folyamatok és az eszközök meghatározása

15. A pénzügyi intézményeknek meg kell határozniuk, létre kell hozniuk és folyamatosan frissíteniük kell üzleti funkcióik, szerepköreik és támogató folyamataik kapcsolati térképét, hogy azonosítsák ezek fontosságát és összefüggéseiket az IKT- és biztonsági kockázatok kapcsán.

16. Ezen kívül a pénzügyi intézményeknek meg kell határozniuk, létre kell hozniuk és folyamatosan frissíteniük kell az üzleti funkcióikat és támogató folyamataikat kiszolgáló információs eszközök kapcsolati térképét, mint például az IKT-rendszereket, az alkalmazottakat, a vállalkozókat, a harmadik feleket és más belső és külső rendszerektől és folyamatoktól való függőségeket annak

érdekében, hogy legalább azokat az információs eszközöket kezelni tudják, amelyek a kritikus üzleti funkcióikat és folyamataikat támogatják.

1.3.3. Besorolás és kockázatértékelés

17. A pénzügyi intézményeknek kritikusság szerint osztályozniuk kell a 15. és 16. bekezdésekben azonosított üzleti funkciókat, támogató folyamatokat és információs eszközöket.

18. Ezen azonosított üzleti funkciók, támogató folyamatok és információs eszközök kritikusságának meghatározása érdekében a pénzügyi intézményeknek figyelembe kell venniük legalább a bizalmasság, sértetlenség és rendelkezésre állás követelményeit. Az információs eszközökre vonatkozó elszámoltathatóságot és felelősséget egyértelműen meg kell határozni.

19. A pénzügyi intézményeknek a kockázatértékelés során felül kell vizsgálniuk az információs eszközök besorolásának és a vonatkozó dokumentációnak a megfelelőségét.

20. A pénzügyi intézményeknek meg kell határozniuk az azonosított és osztályokba sorolt üzleti funkciókra, a támogató folyamatokra és információs eszközökre ható IKT- és biztonsági kockázatokat és azok kritikusságát. Ezt a kockázatértékelést évente vagy szükség esetén rövidebb időközönként el kell végezni és dokumentálni kell. Az említett kockázatértékeléseket el kell végezni az üzleti funkciókat, támogató folyamatokat vagy az információs eszközöket érintő, az infrastruktúrában, folyamatokban vagy eljárásokban bekövetkező bármilyen jelentős változás esetén is, és következésképpen frissíteni kell a pénzügyi intézmények aktuális kockázatértékelését.

21. A pénzügyi intézményeknek biztosítaniuk kell, hogy folyamatosan nyomon kövessék az üzleti folyamataikkal, támogató funkcióikkal és információs eszközeikkel kapcsolatos fenyegetéseket és sérülékenységeket, és rendszeresen felül kell vizsgálniuk az ezeket érintő kockázati forgatókönyveket.

1.3.4. Kockázatcsökkentés

22. A kockázatértékelések alapján a pénzügyi intézményeknek meg kell határozniuk, hogy milyen intézkedések szükségesek az azonosított IKT- és biztonsági kockázatok elfogadható szintre történő csökkentéséhez, és hogy szükség van-e változtatásra a meglévő üzleti folyamatok, ellenőrzési intézkedések, IKT-rendszerek és IKT-szolgáltatások kapcsán. A pénzügyi intézményeknek figyelembe kell venniük az említett változtatások és a megfelelő ideiglenes kockázatcsökkentő intézkedések végrehajtásához szükséges időt, hogy az IKT- és biztonsági kockázatoka pénzügyi intézmény kockázati étvágyán belül maradjanak.

23. A pénzügyi intézményeknek meg kell határozniuk és végre kell hajtaniuk az azonosított IKT- és biztonsági kockázatok mérséklésére és az információs eszközök – besorolásuknak megfelelő – védelmére irányuló intézkedéseket.

1.3.5. Jelentéstétel

24. A pénzügyi intézményeknek a vezető testület felé egyértelműen és kellő időben jelentést kell tenniük a kockázatértékelés eredményeiről. Az említett jelentéstétel nem érinti a pénzforgalmi

szolgáltatók azon kötelezettségét, hogy az (EU) 2015/2366 irányelv 95. cikkének (2) bekezdésében foglaltaknak megfelelően aktualizált és átfogó kockázatértékelést nyújtsanak be az illetékes hatóságoknak.

1.3.6. Ellenőrzés

25. A pénzügyi intézmény IKT- és biztonsági kockázatait érintő irányítását, rendszereit és folyamatait rendszeresen ellenőrizniük kell az IKT- és biztonsági kockázatok, valamint (pénzforgalmi szolgáltatók esetén) a pénzforgalom terén megfelelő ismertekkel, jártassággal és szakértelemmel rendelkező auditoroknak, hogy a vezető testület számára független bizonyosságot nyújtsanak azok hatékonyságáról. Az auditoroknak függetlennek kell lenniük a pénzügyi intézménytől vagy azon belül. Az ilyen ellenőrzések gyakoriságának és hatókörének arányosnak kell lennie a vonatkozó IKT- és biztonsági kockázatokkal.

26. A pénzügyi intézmény vezető testületének jóvá kell hagynia az ellenőrzési tervet, beleértve az IKT-ellenőrzéseket és azok minden lényeges módosítását. Az ellenőrzési tervnek és végrehajtásának, beleértve az ellenőrzés gyakoriságát, tükröznie kell a pénzügyi intézmény IKT- és biztonsági kockázatait, és azokkal arányosnak kell lennie, továbbá az ellenőrzési terveket rendszeresen aktualizálni kell.

27. Ki kell alakítani egy hivatalos nyomonkövetési folyamatot, beleértve a kritikus IKT-ellenőrzési megállapítások időszerű igazolását és javítását biztosító rendelkezéseket.

1.4. Információbiztonság

1.4.1. Információbiztonsági politika

28. A pénzügyi intézményeknek ki kell dolgozniuk és dokumentálniuk kell információbiztonsági politikájukat, amely meghatározza a pénzügyi intézmények és ügyfeleik adatai és információi bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére vonatkozó magas szintű elveket és szabályokat. A pénzforgalmi szolgáltatók esetében ezt a politikát az (EU) 2015/2366 irányelv 5. cikke (1) bekezdésének j) pontjával összhangban elfogadásra kerülő biztonságpolitikai dokumentumban kell meghatározni. Az információbiztonsági politikának összhangban kell lennie a pénzügyi intézmény információbiztonsági célkitűzéseivel, és a kockázatértékelési folyamat vonatkozó eredményein kell alapulnia. A politikát a vezető testületnek jóvá kell hagynia.

29. A politikának tartalmaznia kell az információbiztonsági irányítás legfontosabb szerepköreinek és felelősségi köreinek a leírását, és meg kell határoznia az alkalmazottakkal és vállalkozókkal, az eljárásokkal és a technológiával kapcsolatos információbiztonsági követelményeket, figyelembe véve, hogy az alkalmazottak és a vállalkozók minden szinten felelősek a pénzügyi intézmény információbiztonságának biztosításáért. A politikának biztosítania kell a pénzügyi intézmények alapvető logikai és fizikai eszközeinek, erőforrásainak és érzékeny adatainak bizalmasságát, sértetlenségét és rendelkezésre állását, tárolás, továbbítás és használat során egyaránt. Az információbiztonsági politikáról a pénzügyi intézmény minden alkalmazottját és vállalkozóját tájékoztatni kell.

30. Az információbiztonsági politika alapján a pénzügyi intézményeknek biztonsági intézkedéseket kell kidolgozniuk és végrehajtaniuk annak érdekében, hogy mérsékeljék azokat az IKT- és biztonsági kockázatokat, amelyeknek ki vannak téve. Ezeknek az eljárásoknak ki kell terjedniük a következőkre:

    a) szervezet és irányítás a 10. és 11. bekezdésnek megfelelően;
    b) logikai biztonság (1.4.2. pont);
    c) fizikai biztonság (1.4.3. pont);
    d) IKT-üzemeltetési biztonság (1.4.4. pont);
    e) biztonsági monitorozás (1.4.5. pont);
    f) információbiztonsági felülvizsgálatok, értékelés és tesztelés (1.4.6. pont);
    g) információbiztonsági képzés és tudatosítás (1.4.7. pont);

1.4.2. Logikai biztonság

31. A pénzügyi intézményeknek meg kell meghatározniuk, dokumentálniuk kell és végre kell hajtaniuk a logikai hozzáférés kezelésének (személyazonosság- és hozzáféréskezelés) eljárásait. Ezeket az eljárásokat be kell vezetni, be kell tartatni, nyomon kell követni és rendszeresen felül kell vizsgálni. Az eljárásoknak a rendellenességek nyomon követését biztosító kontrollokat is tartalmazniuk kell. Ezeknek az eljárásoknak legalább a következő követelményeket is meg kell valósítaniuk, ahol a „felhasználó” kifejezés magában foglalja a technikai felhasználókat is:

    (a) **A szükséges ismeret, a legkisebb jogosultság és a feladatok elkülönítésének elve:** a pénzügyi intézményeknek az információs eszközökhöz és az azokat támogató rendszerekhez való hozzáféréseket a „szükséges ismeret” elve alapján kell kezelniük, ideértve a távoli hozzáférést is. A felhasználók számára a feladataik ellátásához szükséges, legszűkebb körű hozzáférési jogokat kell biztosítani (a „legkisebb jogosultság” elve), vagyis, hogy megakadályozzák azadatok széles köréhez való indokolatlan hozzáférést vagy megakadályozzák a hozzáférési jogok olyan kombinációinak kiosztását, amelyek a kontrollok megkerülésére használhatók (a „feladatok elkülönítésének” elve).
    (b) **A felhasználó elszámoltathatósága:** a pénzügyi intézményeknek a lehető legnagyobb mértékben korlátozniuk kell az általános és a megosztott felhasználói fiókok használatát, és biztosítaniuk kell, hogy a felhasználók azonosíthatók legyenek az IKT-rendszerekben végrehajtott tevékenységek tekintetében.
    (c) **Kiemelt hozzáférési jogok:** a pénzügyi intézményeknek szigorúan ellenőrizniük kell a rendszerekhez való kiemelt hozzáférést az emelt szintű rendszerhozzáférési jogosultságokkal rendelkező fiókok szigorú korlátozása és szoros felügyelete révén (például rendszergazdai fiókok). A biztonságos kommunikáció biztosítása és a kockázat csökkentése érdekében a kritikus IKT-rendszerekhez távoli rendszergazdai hozzáférést csak a szükséges ismeret elve alapján szabad adni, és csak erős hitelesítési megoldások használata esetén.
    (d) **A felhasználói tevékenységek naplózása:** legalább a kiemelt felhasználók összes tevékenységét naplózni és ellenőrizni kell. Biztosítani kell a hozzáférési naplók védelmét az illetéktelen módosítás vagy törlés ellen és meg kell őrizni azokat a meghatározott

üzleti funkciók, támogató folyamatok és információs eszközök kritikusságának megfelelően, az iránymutatások 1.3.3. pontja alapján, az uniós és nemzeti jogszabályban előírt megőrzési követelmények sérelme nélkül. A pénzügyi intézménynek ezt az információt fel kell használnia a szolgáltatások nyújtása során azonosított rendellenes tevékenységek felmérésére és kivizsgálására.

(e) **Hozzáféréskezelés:** a hozzáférési jogokat kellő időben kell megadni, visszavonni vagy módosítani, az előre meghatározott jóváhagyási munkafolyamatoknak megfelelően, amelyekbe be kell vonni a hozzáféréssel érintett információk üzleti tulajdonosát (az információs vagyon tulajdonosát). A munkaviszony megszűnése esetén a hozzáférési jogokat haladéktalanul vissza kell vonni.

(f) **A hozzáférések felülvizsgálata:** a hozzáférési jogokat rendszeres időközönként felül kell vizsgálni annak biztosítása érdekében, hogy a felhasználók ne rendelkezzenek túlzott kiváltságokkal, és hogy a hozzáférési jogokat visszavonják, amikor már nincs azokra szükség.

(g) **Azonosítási módszerek:** a pénzügyi intézményeknek hatásos azonosítási módszereket kell hatályba léptetniük, amelyek megfelelően és hatékonyan biztosítják a hozzáférési követelmények és eljárások betartását. Az azonosítási módszereknek arányosnak kell lenniük az IKT-rendszerek, az információk vagy a hozzáféréssel érintett folyamat kritikusságával. Ennek – a vonatkozó kockázat alapján – legalább az összetett jelszavakat vagy erősebb azonosítási módszereket (mint a kétfaktoros azonosítás) tartalmaznia kell.

32. Az alkalmazásoknak az adatokhoz és IKT-rendszerekhez való elektronikus hozzáférését az adott szolgáltatás nyújtásához szükséges minimumra kell korlátozni.

1.4.3. Fizikai biztonság

33. A pénzügyi intézményeknek fizikai biztonsági intézkedéseket kell meghatározniuk, dokumentálniuk és végrehajtaniuk annak érdekében, hogy megvédjék telephelyüket, adatközpontjaikat és érzékeny területeiket az illetéktelen hozzáféréssel és a környezeti veszélyekkel szemben.

34. Az IKT-rendszerekhez való fizikai hozzáférést csak a feljogosított személyeknek szabad lehetővé tenni. A feljogosítást a személy feladataival és felelősségi köreivel összhangban, valamint a megfelelően képzett és ellenőrzött személyekre korlátozva kell kiosztani. A fizikai hozzáférést rendszeresen felül kell vizsgálni, hogy biztosítsák a felesleges hozzáférési jogok haladéktalan visszavonását, amikor azokra már nincs szükség.

35. A környezeti veszélyekkel szembeni védelmet szolgáló megfelelő intézkedéseknek arányosnak kell lenniük az épületek fontosságával és az érintett épületekben található műveletek vagy IKT-rendszerek kritikusságával.

1.4.4. IKT üzemeltetés biztonsága

36. A pénzügyi intézményeknek olyan eljárásokat kell bevezetniük, amelyek megakadályozzák, hogy biztonsági problémák forduljanak elő az IKT-rendszerekben és az IKT-szolgáltatásokban,

és minimalizálják a biztonsági problémáknak az IKT-szolgáltatások nyújtására gyakorolt hatásait. Ezeknek az eljárásoknak a következő intézkedésekre kell kiterjedniük:

a) a lehetséges sérülékenységek azonosítására, amelyeket ki kell értékelni és javítani kell a szoftver és a firmware naprakész állapotának biztosításával – ideértve a pénzügyi intézmények által a belső és külső felhasználóik számára biztosított szoftvert is –, kritikus biztonsági javítások telepítésével vagy kompenzáló kontrollok megvalósításával;
b) az összes hálózati eszköz biztonságos alapkonfigurációinak kialakítására;
c) a hálózati szegmentálás megvalósítására, adatvesztés-megelőző rendszerekre és a hálózati forgalom titkosítására (az adatok osztályozásának megfelelően);
d) a végpontok védelmének megvalósítására, beleértve a szervereket, munkaállomásokat és mobil eszközöket; a pénzügyi intézményeknek meg kell vizsgálniuk, hogy a végpontok megfelelnek-e az általuk meghatározott biztonsági előírásoknak, mielőtt azok hozzáférést kapnak a vállalati hálózathoz;
e) a szoftverek, a firmware és az adatok sértetlenségének ellenőrzésére szolgáló mechanizmusok bevezetésére;
f) az adatok titkosítására tárolás és továbbítás során (az adatok osztályozásának megfelelően).

37. Ezenkívül a pénzügyi intézményeknek folyamatosan meg kell határozniuk, hogy a meglévő üzemeltetési környezetben végrehajtott változtatások befolyásolják-e a meglévő biztonsági intézkedéseket, vagy szükségessé teszik-e további intézkedések elfogadását a felmerülő kockázatok megfelelő mérséklése érdekében. Ezeknek a változtatásoknak a pénzügyi intézmény formális változáskezelési folyamatának részét kell képezniük, ami biztosítja a változtatások megfelelő megtervezését, tesztelését, dokumentálását, engedélyezését és telepítését.

1.4.5. Biztonsági monitorozás

38. A pénzügyi intézményeknek szabályzatokat és eljárásokat kell kidolgozniuk és bevezetniük annak érdekében, hogy a pénzügyi intézmények információbiztonságát esetlegesen befolyásoló rendellenes tevékenységeket észleljék és megfelelően reagáljanak azokra. A Pénzügyi intézményeknek ezen folyamatos nyomon követés részeként megfelelő és hatékony mechanizmusokat kell kialakítaniuk a fizikai vagy logikai behatolás, valamint az információs eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának sérülésének észlelésére és jelentésére. A folyamatos monitorozási és észlelési folyamatoknak ki kell terjedniük a következőkre:

a) a releváns belső és külső tényezőkre, beleértve az üzleti és IKT adminisztratív funkciókat;
b) tranzakciókra, a harmadik felek vagy más szervezetek általi hozzáféréssel és a belső hozzáféréssel való visszaélések észlelése érdekében;
c) a potenciális belső és külső fenyegetésekre.

39. A pénzügyi intézményeknek folyamatokat és szervezeti struktúrákat kell kialakítaniuk és bevezetniük, hogy felismerjék és folyamatosan monitorozzák azon biztonsági fenyegetéseket,

amelyek érdemben befolyásolhatják a szolgáltatások nyújtására való képességüket. A pénzügyi intézményeknek aktívan nyomon kell követniük a technológia fejlődését, ezzel biztosítva, hogy tisztában legyenek a biztonsági kockázatokkal. A pénzügyi intézményeknek észlelési intézkedéseket kell bevezetniük, például, hogy felismerjék az esetleges információszivárgást, a kártékonykódokat és más biztonsági fenyegetéseket, valamint, hogy azonosítsák a szoftverek és hardverek közismert sérülékenységeit, és ellenőrizniük kell az ezen sérülékenységekre megfelelő új biztonsági frissítések elérhetőségét.

40. A biztonsági monitorozás folyamatnak segítenie kell a pénzügyi intézményt a működési vagy biztonsági incidensek természetének megértésben, a tendenciák azonosításában, valamint támogatnia kell az intézmény vizsgálatait is.

1.4.6. Információbiztonsági vizsgálatok, értékelés és tesztelés

41. A pénzügyi intézményeknek különféle információbiztonsági vizsgálatokat, értékeléseket és teszteket kell elvégezniük az IKT-rendszereik és IKT-szolgáltatásaik sérülékenységeinek hatékony azonosítása érdekében. A pénzügyi intézmények végezhetnek például eltéréselemzést (gap-elemzés) információbiztonsági szabványok, megfelelőségi vizsgálatok, az információs rendszerek belső és külső ellenőrzése vagy fizikai biztonsági vizsgálatok alapján. Ezenkívül az intézménynek mérlegelnie kell a bevált gyakorlatok alkalmazását is, mint a forráskód felülvizsgálatokat, a sérülékenységvizsgálatokat, behatolási teszteket és a saját támadóerős ún. Red team gyakorlatokat.

42. A pénzügyi intézményeknek ki kell dolgozniuk és be kell vezetniük egy információbiztonsági tesztelési keretrendszert, amely ellenőrzi az információbiztonsági intézkedéseik megbízhatóságát és hatékonyságát, továbbá biztosítja, hogy ez a keretrendszer figyelembe veszi a fenyegetés nyomonkövetési, valamint az IKT- és biztonsági kockázatértékelési folyamaton keresztül azonosított fenyegetéseket és sérülékenységeket.

43. Az információbiztonsági tesztelési keretrendszernek biztosítania kell, hogy:

    a) a teszteket olyan független, tesztelők végezzék, akik megfelelő ismeretekkel, készségekkel és szakértelemmel rendelkeznek az információbiztonsági intézkedések tesztelésében, és akik nem vesznek részt az információbiztonsági intézkedések kidolgozásában;
    b) a tesztek között legyenek az üzleti folyamatok és rendszerek azonosított kockázati szintjével arányos sérülékenységi vizsgálatok és behatolási tesztek (ideértve a fenyegetés alapú behatolásvizsgálatokat, ahol szükséges és megfelelő).

44. A pénzügyi intézményeknek folyamatos és ismételt teszteket kell végezniük a biztonsági intézkedéseikre vonatkozóan. Az összes kritikus IKT-rendszer (17. bekezdés) esetében ezeket a teszteket legalább évente el kell végezni, a pénzforgalmi szolgáltatók esetében pedig ezen tesztek a második pénzforgalmi szolgáltatási irányelv 95. cikkének (2) bekezdésével összhangban az általuk nyújtott pénzforgalmi szolgáltatásokkal kapcsolatos biztonsági kockázatok átfogó értékelésének részét képezik. A nem kritikus rendszereket rendszeresen, de legalább háromévente tesztelni kell a kockázati alapú megközelítést alkalmazásával.

45. A pénzügyi intézményeknek biztosítaniuk kell, hogy a biztonsági intézkedések tesztelését elvégezzék az infrastruktúrában, a folyamatokban vagy az eljárásokban bekövetkező változások esetén, valamint nagyobb működési vagy biztonsági incidensek miatt változtatások, illetve új vagy jelentősen módosított, internettel összekötött kritikus alkalmazások éles üzembe állítása kapcsán.

46. A pénzügyi intézményeknek nyomon kell követniük és értékelniük kell a biztonsági tesztek eredményeit, és ennek megfelelően kell frissíteniük a biztonsági intézkedéseiket, a kritikus IKT-rendszerek esetében indokolatlan késedelem nélkül.

47. A pénzforgalmi szolgáltatók esetében a tesztelési keretrendszernek ki kell terjednie a következőkkel kapcsolatos biztonsági intézkedésekre 1) fizetési terminálok és pénzforgalmi szolgáltatások nyújtására használt eszközök, 2) fizetési terminálok és a pénzforgalmi szolgáltatás felhasználóinak azonosítására használt eszközök, 3) a pénzforgalmi szolgáltató által a pénzforgalmi szolgáltatás felhasználói számára a hitelesítő kód generálásához/fogadásához biztosított eszközök és szoftver.

48. Az észlelt biztonsági fenyegetések és az elvégzett változtatások alapján tesztet kell végezni a releváns és ismert potenciális támadásokra vonatkozó forgatókönyvek felhasználásával.

1.4.7. Információbiztonsági képzés és tudatosság

49. A pénzügyi intézményeknek képzési programot kell kialakítaniuk – beleértve a rendszeres biztonságtudatossági programokat is – a személyzet minden tagja és az összes vállalkozó számára, mely biztosítja a feladataiknak és felelősségeiknek a vonatkozó biztonsági elvekkel és eljárásokkal összhangban történő ellátásához szükséges képzést, az emberi hiba, lopás, csalás, visszaélés vagy veszteség lehetőségének csökkentése, továbbá az információbiztonsági kockázatok kezelésének megismertetése érdekében. A pénzügyi intézményeknek biztosítaniuk kell, hogy a képzési program a személyzet minden tagjának és az összes vállalkozónak legalább az éves gyakoriságú képzését biztosítsa.

1.5. IKT-üzemeltetés

50. A pénzügyi intézményeknek az IKT üzemeltetését a vezető testület által jóváhagyott dokumentált és bevezetett folyamatok és eljárások (amelyek a pénzforgalmi szolgáltatók esetében tartalmazzák a második pénzforgalmi szolgáltatási irányelv 5. cikke (1) bekezdésének j) pontja szerinti biztonságpolitikai dokumentumot) alapján kell irányítaniuk. Ezeknek a dokumentumoknak meg kell határozniuk, hogy a pénzügyi intézmények hogyan irányítják, monitorozzák és ellenőrzik IKT-rendszereiket és szolgáltatásaikat, beleértve a kritikus IKT üzemeltetési folyamatok dokumentálását, és lehetővé kell tenniük, hogy a pénzügyi intézmények naprakész nyilvántartást vezessenek az IKT-eszközökről.

51. A pénzügyi intézményeknek biztosítaniuk kell, hogy az IKT-üzemeltetés színvonala összhangban legyen az üzleti követelményeikkel. A pénzügyi intézményeknek fenn kell tartaniuk és lehetőség szerint javítaniuk kell az IKT üzemeltetés hatékonyságát, ideértve, de nem kizárólagosan, annak

szükségességét, hogy fontolóra vegyék a manuálisan végrehajtott feladatokból eredő lehetséges hibák minimalizálásának lehetőségeit.

52. A pénzügyi intézményeknek naplózási és monitorozási eljárásokat kell kialakítaniuk a kritikus IKT folyamatokra vonatkozóan, hogy lehetővé tegyék a hibák észlelését, elemzését és kijavítását.

53. A pénzügyi intézményeknek naprakész nyilvántartást kell vezetniük IKT-eszközeikről (ideértve az IKT-rendszereket, hálózati eszközöket, adatbázisokat stb.). Az IKT-eszközök nyilvántartásának tartalmaznia kell az IKT-eszközök konfigurációját, valamint a különféle IKT-eszközök közötti kapcsolatokat és kölcsönös függőségeket, a megfelelő konfiguráció- és változáskezelési folyamat lehetővé tétele érdekében.

54. Az IKT-eszközök nyilvántartásának kellően részletesnek kell lennie ahhoz, hogy lehetővé tegye az IKT-eszközök azonnali azonosítását, valamint elhelyezkedésének, biztonsági besorolásának és tulajdonjogának meghatározását. Az eszközök közötti kölcsönös függőségeket dokumentálni kell, hogy az elősegítse a biztonsági és működési incidensekre – beleértve a kibertámadásokat is – való reagálást.

55. A pénzügyi intézményeknek figyelemmel kell kísérniük és kezelniük kell az IKT-eszközök életciklusát, ezzel biztosítva, hogy azok folyamatosan megfeleljenek az üzleti és kockázatkezelési követelményeknek és támogassák azokat. A pénzügyi intézményeknek ellenőrizniük kell, hogy IKT-eszközeiket támogatják-e a külső vagy belső szállítók és fejlesztők, és hogy minden releváns javítás és frissítés telepítésre került-e a dokumentált folyamatok alapján. Fel kell mérni és mérsékelni kell az elavult vagy nem támogatott IKT-eszközökből eredő kockázatokat.

56. A pénzügyi intézményeknek teljesítmény- és kapacitástervezési, továbbá ellenőrzési folyamatokat kell bevezetniük annak érdekében, hogy időben megelőzzék, azonosítsák és kezeljék az IKT-rendszerek jelentős teljesítményproblémáit és az IKT-kapacitáshiányokat.

57. A pénzügyi intézményeknek meg kell határozniuk és be kell vezetniük az adatok és IKT-rendszerek biztonsági mentési és helyreállítási eljárásait, hogy biztosítsák azok szükség szerinti helyreállíthatóságát. A biztonsági mentések körét és gyakoriságát az üzleti helyreállítási követelményekkel, valamint az adatok és IKT-rendszerek kritikusságával összhangban meg kell határozni, és az elvégzett kockázatértékelés alapján értékelni kell. A biztonsági mentési és helyreállítási eljárások tesztelését rendszeresen el kell végezni.

58. A pénzügyi intézményeknek biztosítaniuk kell az adatok és az IKT-rendszerek biztonsági másolatainak biztonságos tárolását és azt, hogy kellő távolságra legyenek az elsődleges telephelytől, hogy ne legyenek kitéve ugyanazoknak a kockázatoknak.

3.5.1 IKT-incidens és problémakezelés

59. A pénzügyi intézményeknek ki kell dolgozniuk és be kell vezetniük egy incidens- és problémakezelési folyamatot a működési és biztonsági IKT-incidensek nyomon követése és naplózása érdekében, valamint annak lehetővé tételére, hogy zavar felmerülése esetén a pénzügyi intézmények időben folytathassák vagy újrakezdhessék a kritikus üzleti funkcióikat és

folyamataikat. A pénzügyi intézményeknek megfelelő kritériumokat és küszöbértékeket kell meghatározniuk arra vonatkozóan, hogy milyen eseményt minősítenek működési vagy biztonsági incidensnek a jelen iránymutatások „Fogalommeghatározások" részében leírtaknak megfelelően, valamint meg kell határozniuk riasztásként szolgáló korai előrejelző mutatókat is, amelyek lehetővé teszik a működési vagy biztonsági incidensek korai észlelését. Ezek a kritériumok és küszöbértékek a pénzforgalmi szolgáltatók esetében nem érintik a súlyos incidenseknek a második pénzforgalmi szolgáltatási irányelv 96. cikke és a súlyos incidensek bejelentéséről szóló iránymutatások (EBA/GL/2017/10) szerinti osztályozását.

60. A nemkívánatos események hatásának minimalizálása és az időben történő helyreállítás lehetővé tétele érdekében, a pénzügyi intézményeknek megfelelő folyamatokat és szervezeti felépítést kell kialakítaniuk a működési és biztonsági incidensek következetes és integrált monitorozásának, kezelésének és nyomon követésének biztosítására, valamint annak érdekében, hogy azonosítsák és megszüntessék a kiváltó okokat, és ezáltal megakadályozzák az incidensek megismétlődését. Az incidens- és problémakezelési folyamatnak meg kell határoznia a következőket:

a) az incidensek azonosítására, nyomon követésére, naplózására, prioritások szerinti kategorizálására és osztályozására vonatkozó eljárásokat az üzleti kritikusság alapján;
b) különféle incidens forgatókönyvekre vonatkozó szerepeket és felelősségi köröket (pl. hibák, hibás működés, kibertámadások);
c) problémakezelési eljárásokat egy vagy több incidens gyökérokainak azonosítására, elemzésére és megoldására – a pénzügyi intézménynek elemeznie kell azokat az azonosított vagy a szervezetben és/vagy azon kívül bekövetkező működési vagy biztonsági incidenseket, amelyek valószínűleg érintik a pénzügyi intézményt, és figyelembe kell vennie az ezen elemzésekből levont legfontosabb tapasztalatokat, és ennek megfelelően frissítenie kell a biztonsági intézkedéseket;
d) hatékony belső kommunikációs terveket, beleértve az incidensekre vonatkozó értesítési és eszkalációs eljárásokat – a biztonsággal kapcsolatos ügyfélpanaszokat is lefedve – annak érdekében, hogy
    i) biztosítsa a kritikus IKT-rendszerekre és IKT-szolgáltatásokra potenciálisan jelentősen káros hatást gyakorló incidensek jelentését az érintett felső vezetésnek és az IKT felső vezetésének;
    ii) biztosítsa, hogy a vezető testületet eseti alapon tájékoztassák a jelentős incidensekről, továbbá tájékoztassák legalább az incidensek hatásairól, az azokra való reagálásról és az incidensek eredményeként meghatározandó kiegészítő kontrollokról.
e) incidenskezelési eljárásokat, az incidensekkel kapcsolatos hatások mérséklésére, illetve a szolgáltatások időben működőképessé és biztonságossá tétele érdekében;
f) konkrét külső kommunikációs terveket a kritikus üzleti funkciókra és folyamatokra vonatkozóan annak érdekében, hogy:
    i) együttműködjenek a megfelelő érdekelt felekkel az incidensre való hatékony reagálás és az abból való helyreállás céljából;

ii) időben tájékoztassák a külső feleket (például ügyfeleket, más piaci szereplőket, a felügyeleti hatóságot), a vonatkozó szabályozásnak megfelelően.

1.6. IKT-projekt és változásmenedzsment

1.6.1. IKT-projektmenedzsment

61. A pénzügyi intézménynek be kell vezetnie egy program- és/vagy projektmenedzsment folyamatot, amely meghatározza a szerep- és felelősségi köröket és az elszámoltathatóságot az IKT-stratégia végrehajtásának hatékony támogatása érdekében.

62. A pénzügyi intézményeknek megfelelően figyelemmel kell kísérniük és mérsékelniük kell az IKT-projektportfóliójukból eredő kockázatokat (programmenedzsment), figyelembe véve a különféle projektek közötti kölcsönös függőségekből, valamint több projekt ugyanazon erőforrásoktól és/vagy szakértelemtől való függőségéből adódó kockázatokat is.

63. A pénzügyi intézményeknek IKT-projektmenedzsment szabályzatot kell kidolgozniuk és bevezetniük, amely legalább a következőkre kiterjed:

    a) projekt célok;
    b) szerepek és felelősségi körök;
    c) projektkockázat-értékelés;
    d) projektterv, időkeret és lépések;
    e) főbb mérföldkövek;
    f) a változáskezeléssel szemben támasztott követelmények.

64. Az IKT-projektmenedzsment szabályzatnak biztosítania kell, hogy az információbiztonsági követelményeket egy, a fejlesztési funkciótól független funkció elemezze és hagyja jóvá.

65. A pénzügyi intézményeknek biztosítaniuk kell, hogy az IKT-projekt által érintett összes terület képviseltesse magát a projektcsoportban, és hogy a projektcsoport rendelkezzen a projekt biztonságos és sikeres megvalósításához szükséges ismeretekkel.

66. Az IKT-projektek kidolgozásáról és előrehaladásáról, valamint az azokhoz kapcsolódó kockázatokról – az IKT-projektek fontosságától és méretétől függően külön-külön vagy összesítve – rendszeresen és adott esetben eseti alapon jelentést kell tenni az irányító testület számára. A pénzügyi intézményeknek fel kell venniük a projektkockázatot a kockázatkezelési keretrendszerükbe.

1.6.2. IKT-rendszerek beszerzése és fejlesztése

67. A pénzügyi intézményeknek ki kell dolgozniuk és be kell vezetniük egy folyamatot, amely szabályozza az IKT-rendszerek beszerzését, fejlesztését és karbantartását. Ezt a folyamatot kockázatalapú megközelítéssel kell megtervezni.

68. A pénzügyi intézményeknek biztosítaniuk kell, hogy mielőtt sor kerülne bármilyen IKT-rendszer beszerzésére vagy fejlesztésére, a vonatkozó üzleti vezetés egyértelműen határozza meg és

hagyja jóvá a funkcionális és nem funkcionális követelményeket (ideértve az információbiztonsági követelményeket is).

69. A pénzügyi intézményeknek biztosítaniuk kell azon intézkedéseket, amelyek mérséklik az IKT-rendszerek véletlen megváltoztatásának vagy szándékos manipulációjának kockázatát a fejlesztés és az éles környezetbe történő bevezetés során.

70. A pénzügyi intézményeknek rendelkezniük kell az IKT rendszerek használatba vételét megelőző tesztelésére és jóváhagyására vonatkozó módszertannal. Ennek a módszertannak figyelembe kell vennie az üzleti folyamatok és eszközök kritikusságát. A tesztelésnek biztosítania kell, hogy az új IKT-rendszerek az elvárásoknak megfelelően működjenek. Ennek során olyan tesztkörnyezetet is használniuk kell, amely megfelelően tükrözi az éles környezetet.

71. A pénzügyi intézményeknek tesztelniük kell az IKT-rendszereket, az IKT-szolgáltatásokat és az információbiztonsági intézkedéseket a lehetséges biztonsági gyengeségek és szabálysértések vagy incidensek azonosítása érdekében.

72. A pénzügyi intézményeknek külön IKT-környezeteket kell kialakítaniuk az összeférhetetlen feladatok elkülönítésének biztosítására és az éles rendszerek nem ellenőrzött változtatásai hatásainak mérséklésére. Konkrétabban, a pénzügyi intézményeknek biztosítaniuk kell az éles környezet elválasztását a fejlesztési, tesztelési és más, nem éles környezetektől. A pénzügyi intézményeknek biztosítaniuk kell az éles adatok sértetlenségét és bizalmasságát a nem éles környezetekben. Az éles adatokhoz való hozzáférést az arra feljogosított felhasználókra kell korlátozni.

73. A pénzügyi intézményeknek intézkedéseket kell végrehajtaniuk a házon belül fejlesztett IKT-rendszereik forráskódjainak sértetlenségének védelme érdekében. Továbbá teljeskörűen dokumentálniuk kell az IKT-rendszerek fejlesztését, bevezetését, üzemeltetését és/vagy konfigurálását annak érdekében, hogy csökkentsék az adott téma szakértőitől való indokolatlan függőséget. Az IKT-rendszer dokumentációjának lehetőség szerint tartalmaznia kell legalább a felhasználói dokumentációt, a rendszer műszaki dokumentációját és az üzemeltetési eljárásokat.

74. A pénzügyi intézmények IKT-rendszerek beszerzésére és fejlesztésére vonatkozó folyamatait az IKT-szervezeten kívüli üzleti funkciók végfelhasználói által fejlesztett vagy kezelt IKT-rendszerekre is alkalmazni kell (például végfelhasználói számítástechnikai alkalmazások), kockázatalapú megközelítés alapján. A pénzügyi intézménynek nyilvántartást kell vezetnie az ilyen az alkalmazásokról, amelyek kritikus üzleti funkciókat vagy folyamatokat támogatnak.

1.6.3. IKT változáskezelés

75. A pénzügyi intézményeknek ki kell dolgozniuk és be kell vezetniük egy IKT-változáskezelési folyamatot, mely biztosítja az IKT-rendszerekben bekövetkezett összes változás kontrollált módon történő rögzítését, tesztelését, értékelését, jóváhagyását, végrehajtását és ellenőrzését. A pénzügyi intézményeknek vészhelyzetekben a megfelelő biztosítékokat nyújtó eljárásokat követve kell kezelniük a változásokat (vagyis azokat a változtatásokat, amelyeket a lehető leghamarabb be kell vezetni).

76. A pénzügyi intézményeknek meg kell határozniuk, hogy a meglévő működési környezeten végrehajtott változtatások befolyásolják-e a meglévő biztonsági intézkedéseket, vagy kiegészítő intézkedések bevezetését teszik szükségessé a felmerülő kockázatok mérséklése érdekében. Ezeknek a változásoknak meg kell felelniük a pénzügyi intézmények formális változáskezelési folyamatának.

1.7. Üzletmenetfolytonosság-menedzsment

77. A pénzügyi intézményeknek megbízható üzletmenetfolytonosság-menedzsment (BCM) folyamatot kell kidolgozniuk annak érdekében, hogy maximalizálják folyamatos szolgáltatásnyújtási képességüket, és hogy az üzletmenet súlyos fennakadása esetén mérsékeljék a veszteségeket a 2013/36/EU irányelv 85. cikkének (2) bekezdésével, valamint az EBH belső irányításról szóló iránymutatásának (EBA/GL/2017/11) VI. címével összhangban.

1.7.1. Üzleti-hatáselemzés

78. A megbízható üzletmenet-folytonosság menedzsment részeként a pénzügyi intézményeknek üzleti hatáselemzést (BIA) kell végezniük az üzletmenet súlyos fennakadásának való kitettségük elemzésével és lehetséges hatásainak (beleértve a bizalmasságra, sértetlenségre és a rendelkezésre állásra gyakorolt hatást is) mennyiségi és minőségi értékelésével, belső és/vagy külső adatok (pl. üzleti folyamatra vonatkozó harmadik fél szolgáltató adatai vagy az üzleti-hatáselemzés szempontjából releváns, nyilvánosan hozzáférhető adatok) felhasználásával és forgatókönyv-elemzéssel. Az üzleti-hatáselemzésnek (BIA) figyelembe kell vennie az azonosított és osztályozott üzleti funkciók, támogató folyamatok, harmadik felek és információs eszközök kritikusságát, valamint ezek kölcsönös függőségét is a 1.3.3. pontnak megfelelően.

79. A pénzügyi intézményeknek biztosítaniuk kell, hogy IKT-rendszereiket és IKT-szolgáltatásaikat az üzleti-hatáselemzéseikkel összhangban tervezzék meg, például bizonyos kritikus elemek redundanciájával az ezen elemeket érintő események által okozott zavarok megakadályozása érdekében.

1.7.2. Üzletmenet-folytonosság tervezés

80. Üzleti-hatáselemzésük alapján a pénzügyi intézményeknek terveket kell kidolgozniuk az üzletmenet-folytonosság biztosítására (üzletmenet-folytonossági tervek, BCP-k), amelyeket dokumentálniuk kell és jóvá kell hagyatniuk a vezető testületükkel. A terveknek kifejezetten figyelembe kell venniük azokat a kockázatokat, amelyek hátrányosan érinthetik az IKT-rendszereket és az IKT-szolgáltatásokat. A terveknek támogatniuk kell azokat a célkitűzéseket, melyek az üzleti funkciók, a támogató folyamatok és információs eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére és szükség esetén helyreállítására vonatkoznak. A pénzügyi intézményeknek e tervek kidolgozása során szükség szerint egyeztetniük kell az érintett belső és külső érdekelt felekkel.

81. A pénzügyi intézményeknek üzletmenet-folytonossági terveket kell érvénybe léptetniük annak biztosítása érdekében, hogy megfelelően tudjanak reagálni a lehetséges meghibásodási

eshetőségekre, és hogy a fennakadás után képesek legyenek helyreállítani a kritikus üzleti tevékenységeik működését a helyreállítási időre vonatkozó célkitűzésen (RTO, az a maximális idő, amelyen belül egy incidens után vissza kell állítani a rendszert vagy a folyamatot) és a helyreállítási pontra vonatkozó célkitűzésen (RPO, az a maximális időtartam, amely alatt az adatvesztés elfogadható egy incidens bekövetkezése esetén) belül. Az üzleti működés súlyos fennakadása esetén, amely az adott üzletmenet-folytonossági tervek alkalmazásával jár, a pénzügyi intézményeknek kockázatalapú megközelítés alapján kell üzletmenet-folytonossági intézkedéseik sorrendjét meghatározniuk, ami a 1.3.3. pont szerint elvégzett kockázatértékeléseken alapulhat. A pénzforgalmi szolgáltatók esetében ez magában foglalhatja például a kritikus tranzakciók további feldolgozásának megkönnyítését, miközben folytatódnak a helyreállítási erőfeszítések.

82. A pénzügyi intézményeknek az üzletmenet-folytonossági tervekben az őket potenciálisan érintő különböző forgatókönyvek széles körét kell mérlegelniük, köztük a szélsőséges, de valószínűsíthető változatokat is – beleértve a kibertámadásra vonatkozó forgatókönyvet is – és fel kell mérniük az ilyen forgatókönyvek lehetséges hatását. Ezen forgatókönyvek alapján kell a pénzügyi intézményeknek megfogalmazniuk, hogy miként garantálják az IKT-rendszerek és szolgáltatások folytonosságát, valamint a pénzügyi intézmény információbiztonságát.

1.7.3. Katasztrófaelhárítási és helyreállítási tervek

83. Az üzleti-hatáselemzések (78. bekezdés) és a valószínűsíthető forgatókönyvek (82. bekezdés) alapján a pénzügyi intézményeknek katasztrófaelhárítási és helyreállítási terveket kell kidolgozniuk. Ezekben a tervekben meg kell határozni azokat a feltételeket, amelyek a tervek azonnali aktiválását okozhatják, és azokat az intézkedéseket, amelyeket végre kell hajtani a pénzügyi intézményeknek legalább a kritikus IKT-rendszerei és IKT-szolgáltatásai rendelkezésre állásának, folytonosságának és helyreállításának biztosítása érdekében. A katasztrófaelhárítási és helyreállítási terveknek törekedniük kell arra, hogy teljesítsék a pénzügyi intézmények működésére vonatkozó helyreállítási célkitűzéseket.

84. A katasztrófaelhárítási és helyreállítási terveknek rövid és hosszú távú helyreállítási lehetőségeket egyaránt figyelembe kell venniük. A tervek:

    a) a kritikus üzleti funkciók, a támogató folyamatok, az információs eszközök és ezek kölcsönös függőségei működésének helyreállítására irányulnak, a pénzügyi intézmények működésére és a pénzügyi rendszerre – beleértve a fizetési rendszereket és a pénzforgalmi szolgáltatást igénybe vevőket – gyakorolt káros hatások elkerülése, valamint a függőben lévő fizetési műveletek teljesítésének biztosítása érdekében;
    b) dokumentáltak és az üzleti és támogató egységek rendelkezésére állnak, valamint vészhelyzet esetén azonnal hozzáférhetők;
    c) frissítésre kerülnek az incidensekből, tesztekből levont tanulságokkal, az újonnan felismert kockázatokkal és fenyegetésekkel, valamint a megváltozott helyreállítási célokkal és prioritásokkal.

85. A terveknek alternatív lehetőségeket is figyelembe kell venniük, arra az esetre, ha a helyreállítás rövid távon nem megvalósítható a költségek, kockázatok, logisztikai vagy előre nem látható körülmények miatt.

86. Ezen kívül a katasztrófaelhárítási és helyreállítási tervek részeként a pénzügyi intézményeknek meg kell fontolniuk a pénzügyi intézmény IKT-szolgáltatásának folytonossága szempontjából kulcsfontosságú, harmadik fél szolgáltatók zavarainak enyhítésére vonatkozó üzletmenet-folytonossági intézkedések bevezetését (összhangban az EBH kiszervezésről szóló iránymutatásának rendelkezéseivel (EBA/GL/2019/02) az üzletmenet-folytonossági terveket illetően).

1.7.4. A tervek tesztelése

87. A pénzügyi intézményeknek rendszeresen tesztelniük kell az üzletmenet-folytonossági tervüket. Biztosítaniuk kell, különösen a kritikus üzleti funkciók, a támogató folyamatok, az információs eszközök és kölcsönös függőségeik (beleértve adott esetben a harmadik felek által biztosítottakat) üzletmenet-folytonossági terveinek legalább éves rendszerességgel megvalósuló tesztelését, a 89. bekezdéssel összhangban.

88. Az üzletmenet-folytonossági terveket legalább évente aktualizálni kell a tesztelés eredményei, a fenyegetésekkel kapcsolatos aktuális információk és a korábbi eseményekből levont tapasztalatok alapján. A helyreállítási célokban (ideértve az RTO-kat és RPO-kat) és/vagy az üzleti funkciókban, a támogató folyamatokban és az információs eszközökben bekövetkező változások az üzletmenet-folytonossági terv frissítésének alapjául szolgálhatnak.

89. A pénzügyi intézményeknek üzletmenet-folytonossági terveik tesztelésével igazolniuk kell, hogy képesek fenntartani vállalkozásuk életképességét a kritikus folyamataik helyreállításáig. Különösen:

    a) magában kell foglalnia a súlyos, de valószínű forgatókönyvek tesztelését, beleértve az üzletmenet-folytonossági tervek kidolgozásához figyelembe vett forgatókönyveket is (valamint adott esetben a harmadik felek által nyújtott szolgáltatások tesztelését); aminek ki kell terjednie a kritikus üzleti funkcióknak, a támogató folyamatoknak és az információs eszközöknek a katasztrófaelhárítási környezetre történő átállítására, és igazolni kell, hogy ezeket ott kellően reprezentatív ideig működtetni lehet, és hogy a normál működést később helyre lehet állítani;
    b) a teszteknek próbára kell tenniük azokat a feltételezéseket, amelyeken az üzletmenet-folytonossági tervek alapulnak, beleértve az irányítási rendszereket és a válságkommunikációs terveket; és
    c) olyan eljárásokat kell magában foglalnia, amelyek igazolják, hogy személyzetük, vállalkozóik, IKT-rendszereik és IKT-szolgáltatásaik képesek megfelelően reagálni a 89. bekezdés a) pontjában meghatározott forgatókönyvekre.

90. A teszteredményeket dokumentálni kell, és a tesztek eredményeként feltárt valamennyi hiányosságot elemezni és kezelni kell, továbbá azokról jelentést kell készíteni a vezető testület számára.

1.7.5. Válsághelyzeti kommunikáció

91. Fennakadás vagy vészhelyzet esetén, illetve az üzletmenet-folytonossági tervek végrehajtása során a pénzügyi intézményeknek gondoskodniuk kell arról, hogy hatékony válságkommunikációs intézkedéseket léptessenek életbe, hogy minden érintett belső és külső érdekelt fél – ideértve az illetékes hatóságokat, ha a nemzeti jogszabályok ezt megkövetelik, valamint az érintett szolgáltatókat (kiszervezési szolgáltatók, csoporthoz tartozó szervezetek vagy harmadik fél szolgáltatók) – időben és megfelelő módon tájékoztatást kapjon.

1.8. A pénzforgalmi szolgáltatást igénybe vevők ügyfélkapcsolati kezelése

92. A pénzforgalmi szolgáltatóknak folyamatokat kell kialakítaniuk és bevezetniük, hogy fejlesszék a pénzforgalmi szolgáltatást igénybe vevőknek a pénzforgalmi szolgáltatásokkal járó biztonsági kockázatokkal kapcsolatos tudatosságát, melyet a pénzforgalmi szolgáltatást igénybe vevők számára nyújtandó segítséggel és útmutatással biztosítanak.

93. A pénzforgalmi szolgáltatást igénybe vevőknek kínált segítséget és útmutatást az új fenyegetések és sérülékenységek alapján aktualizálni kell, és a változásokat közölni kell a pénzforgalmi szolgáltatást igénybe vevőkkel.

94. Ahol a termék funkcionalitása ezt megengedi, a pénzforgalmi szolgáltatóknak lehetővé kell tenniük, hogy a pénzforgalmi szolgáltatást igénybe vevők letiltsák a pénzforgalmi szolgáltatók által a pénzforgalmi szolgáltatást igénybe vevőknek kínált pénzforgalmi szolgáltatásokhoz kapcsolódó egyes fizetési funkciókat.

95. Ha az (EU) 2015/2366 irányelv 68. cikke (1) bekezdésének megfelelően egy pénzforgalmi szolgáltató az egyes készpénz-helyettesítő fizetési eszközökkel végrehajtott fizetési műveletekre vonatkozó összeghatárokról megállapodott a fizető féllel, a pénzforgalmi szolgáltatónak fel kell kínálnia a fizető fél számára azt a lehetőséget, hogy ezeket az összeghatárokat a maximálisan elfogadott összeghatárig módosítsa.

96. A pénzforgalmi szolgáltatóknak lehetőséget kell adniuk arra, hogy a pénzforgalmi szolgáltatást igénybe vevők értesítést kapjanak a fizetési műveletek kezdeményezésére tett, illetve a sikertelen fizetési kísérletekről, ami lehetővé teszi számláik csalárd vagy rosszindulatú használatának felderítését.

97. A pénzforgalmi szolgáltatóknak folyamatosan tájékoztatniuk kell a pénzforgalmi szolgáltatást igénybe vevőket a pénzforgalmi szolgáltatások nyújtásával kapcsolatban őket érintő biztonsági eljárások frissítéseiről.

98. A pénzforgalmi szolgáltatóknak a pénzforgalmi szolgáltatásokkal kapcsolatos mindenfajta kérdés, támogatáskérés, illetve anomáliát vagy biztonsági kérdéseket érintő értesítés esetén segítséget kell nyújtaniuk a pénzforgalmi szolgáltatást igénybe vevőknek. A pénzforgalmi szolgáltatást igénybe vevőket megfelelően tájékoztatni kell az ilyen segítségnyújtás igénybe vételének lehetőségeiről.