EBA/GL/2017/05

11/09/2017

Iránymutatások

Iránymutatások a felügyeleti felülvizsgálati és értékelési eljárás (SREP) során végzendő IKT-kockázat értékeléshez

1. Megfelelés és beszámolási kötelezettségek

Az iránymutatások jogállása

1. Az e dokumentumban szereplő iránymutatásokat az EBH az 1093/2010/EU rendelet1 16. cikkének rendelkezéseivel összhangban adta 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 rögzítik az EBH álláspontját azzal kapcsolatban, hogy mi a megfelelő felügyeleti gyakorlat a Pénzügyi Felügyeletek Európai Rendszerében, és miként kell alkalmazni az uniós jogot 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 iránymutatásnak, hogy megfelelően beépítik azt saját felügyeleti gyakorlataikba (pl. saját jogi kereteik vagy felügyeleti folyamataik módosításával), beleértve azokat az eseteket is, ahol az iránymutatás elsősorban intézményekre vonatkozik.

Adatszolgáltatási követelmények

3. Az 1093/2010/EU rendelet 16. cikkének (3) bekezdése értelmében az egyes illetékes hatóságok 13.11.2017-ig kötelesek értesíteni az EBH-t arról, hogy megfelelnek-e vagy meg kívánnak-e felelni ennek az iránymutatásnak, 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 illetékes hatóság nem felel meg az iránymutatásnak. Az értesítéseket „EBA/GL/2017/05” hivatkozással az EBH honlapján szereplő formanyomtatványon kell megküldeni a compliance@eba.europa.eu címre. Az értesítéseket olyan személyek nyújthatják be, akik megfelelő felhatalmazással rendelkeznek arra nézve, hogy illetékes hatóságuk nevében nyilatkozzanak annak megfeleléséről. Az EBH-nak a 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.).

2. Tárgy, hatókör és fogalommeghatározások

Tárgy és hatókör

5. Ezen – a 2013/36/EU irányelv[2] 107. cikkének (3) bekezdése alapján készült – iránymutatások célja a felügyeleti gyakorlatok közelítése az információs és kommunikációs technológiai (IKT) kockázat értékelése során, a 2013/36/EU irányelv 97. cikkében említett felügyeleti felülvizsgálati és értékelési eljárás (SREP) keretében[3], amely a felügyeleti felülvizsgálati és értékelési eljárásra vonatkozó egységes eljárásokról és módszerekről szóló EBH-iránymutatásokban részletesebben meghatározásra kerül. Kifejezetten ezen iránymutatásokban kerül meghatározásra, hogy az illetékes hatóságoknak milyen értékelési kritériumokat kell alkalmazniuk az intézmények IKT-val kapcsolatos irányításának és stratégiájának felügyeleti értékelése, valamint az intézmények IKT-val kapcsolatos kockázati kitettségeinek és kontrollintézkedéseinek a felügyeleti értékelése során. Ezen iránymutatások az EBH SREP-iránymutatásainak szerves részét képezik.

6. Az illetékes hatóságoknak ezen iránymutatásokat az EBH SREP-iránymutatásaiban a SREP tekintetében meghatározott alkalmazási szinttel, valamint a SREP-iránymutatásokban meghatározott, a szerepvállalás minimumszintjére vonatkozó modellel és arányossági követelményekkel összhangban kell alkalmazniuk.

Címzettek

7. Az iránymutatás címzettjei az 1093/2010/EU rendelet 4. cikke 2. pontja i. alpontjának meghatározása szerinti illetékes hatóságok.

Fogalommeghatározások

8. Eltérő rendelkezés hiányában az ezen iránymutatásokban szereplő fogalmak megegyeznek a 2013/36/EU irányelvben, az 575/2013/EU rendeletben, valamint az EBH SREP-iránymutatásaiban meghatározottakkal. Ezen túlmenően ezen iránymutatásokban a következő fogalmak az alábbi jelentéssel bírnak:

[2] Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (1) – HL L 176., 2013.6.27.

[3] EBA/GL/2014/13

IKT-rendszerek:	az intézmény működését támogató mechanizmus vagy összekapcsolt hálózat részeként létrehozott információs és kommunikációs technológiák.
IKT-szolgáltatások:	az IKT-rendszerek által egy vagy több belső vagy külső felhasználónak nyújtott szolgáltatások. Erre példaként szolgálnak az adatbeviteli, adattárolási, adatfeldolgozási és jelentéstételi szolgáltatások, de ide tartoznak a monitoring-, üzleti és döntéstámogatási szolgáltatások is.
IKT rendelkezésre állási és folytonossági kockázat:	annak a kockázata, hogy az IKT-rendszerek és adatok teljesítményét és rendelkezésre állását káros hatás éri, ideértve, hogy az intézmény képtelen kellő időben helyreállítani az intézmény szolgáltatásait, mégpedig az IKT hardver- vagy szoftverkomponensek hibája, az IKT-rendszer üzemeltetésében fennálló hiányosságok vagy bármely egyéb – a mellékletben részletesebben ismertetett – esemény miatt.
IKT biztonsági kockázat:	az IKT-rendszerekhez és adatokhoz való jogosulatlan hozzáférés kockázata, az intézményen belülről vagy kívülről (pl. kibertámadások), a melléklet részletesebb leírása szerint.
az IKT-változásokkal járó kockázat:	az abból eredő kockázat, hogy az intézmény nem képes kellő időben és ellenőrzötten kezelni az IKT-rendszer változásait, különösen nagy és összetett változtatási programok esetén, a melléklet részletesebb leírása szerint.
IKT adatintegritási kockázat:	annak a kockázata, hogy az IKT-rendszerek által tárolt és feldolgozott adatok hiányosak, pontatlanok vagy nem konzisztensek a különböző IKT-rendszerekben, például az IKT-adat életciklus különböző szakaszainak (adatarchitektúra tervezés, az adatmodell és/vagy az adatszótárak kialakítása, a adatbevitel ellenőrzése, az adatok kinyerésének, továbbításának és feldolgozásának ellenőrzése, ideértve a számított adatkimeneteket is) IKT kontroll gyengesége vagy hiánya miatt, amely gátolja az intézményt abban, hogy szolgáltatásokat tudjon nyújtani és helyes módon és kellő időben elő tudja állítani a (kockázat)kezelési és pénzügyi információkat, a melléklet részletesebb leírása szerint.
IKT kiszervezési kockázat:	annak a kockázata, hogy egy harmadik fél vagy a csoportba tartozó másik szervezet megbízása (csoporton belüli kiszervezés) az IKT-rendszerek vagy a kapcsolódó szolgáltatások biztosításával, károsan érinti az intézmény teljesítményét és kockázatkezelését, a melléklet részletesebb leírása szerint.

3. Végrehajtás

Alkalmazás időpontja

9. Ezen iránymutatások 2018. január 1-jétől alkalmazandók.

4. Az IKT-kockázat értékelésére vonatkozó követelmények

1. cím – Általános rendelkezések

10. Az illetékes hatóságoknak az IKT kockázatkezelés és az irányítás kialakításának, valamint az IKT-stratégiának az értékelését a SREP-eljárás részeként kell elvégezniük, követve az EBH SREP-iránymutatásainak 2. címe szerinti, a szerepvállalás minimumszintjére vonatkozó modellt és arányossági kritériumokat. Ez főleg a következőket jelenti:

    a. az IKT-kockázat értékelés gyakorisága a szerepvállalás minimumszintjére vonatkozó modelltől függ, amely azon alapul, hogy az intézményt mely SREP-kategóriába sorolták be, valamint függ az intézményre vonatkozó egyedi felügyeleti vizsgálati programtól;

    b. az IKT-értékelés mélységének, részletességének és intenzitásának arányban kell állnia az intézmény méretével, felépítésével és működési környezetével, valamint tevékenységeinek jellegével, nagyságrendjével és összetettségével.

11. A felügyeleti szerepvállalás és az intézménnyel folytatott párbeszéd hatókörére, gyakoriságára és intenzitására, valamint az azon standardokra vonatkozó felügyeleti elvárásokra, amelyeknek az intézménynek meg kell felelnie, ezen iránymutatásokban mindvégig az arányosság elve alkalmazandó.

12. Az illetékes hatóságok az értékelés frissítése érdekében támaszkodhatnak az intézmény vagy az illetékes hatóság által más kockázatok vagy SREP-elemek értékelésével összefüggésben már elvégzett munkára, és figyelembe vehetik azt. Konkrétan, az ezen iránymutatásokban meghatározott értékelések elvégzésekor az illetékes hatóságoknak ki kell választaniuk a legmegfelelőbb felügyeleti értékelési megközelítést és módszertant, amely arányos és a legjobban illeszkedik az intézményhez, és az illetékes hatóságoknak a meglévő és rendelkezésre álló dokumentációt fel kell használniuk (pl. vonatkozó jelentések és más dokumentumok, a (kockázatkezelési) vezetőséggel folytatott megbeszélések, a helyszíni ellenőrzések megállapításai), hogy információkkal szolgáljanak az illetékes hatóságok által végzett értékeléséhez.

13. Az illetékes hatóságoknak össze kell foglalniuk az ezen iránymutatásokban meghatározott kritériumok értékelése során tett megállapításaikat, és ezeket kell felhasználniuk az EBH SREP-iránymutatásaiban meghatározott SREP-elemek értékelésére vonatkozó következtetések levonása céljából.

14. Az irányítás és az IKT-stratégia ezen iránymutatások 2. címével összhangban elvégzett értékelésének olyan megállapításokat kell eredményeznie, amelyek információkat szolgáltatnak a SREP-en belül a belső irányítás és az intézményi kontrollintézkedések EBH SREP-iránymutatásainak 5. címében meghatározott értékelése során szerzett eredmények összesítéséhez, és annak tükröződnie kell az adott SREP-elem

pontszámában. Továbbá, az illetékes hatóságoknak figyelemmel kell lenniük, hogy az IKT-stratégia értékelése által az intézmény üzleti stratégiájára gyakorolt bármilyen jelentős káros hatásról, illetve bármilyen azzal kapcsolatos aggodalomról, hogy az intézmény esetlegesen nem rendelkezik elegendő IKT-erőforrással és IKT-kapacitással a tervezett fontos stratégiai változtatások elvégzéséhez és támogatásához, információkat kell szolgáltatni az EBH SREP-iránymutatásainak 4. címével összhangban elvégzett üzletimodell-elemzéshez.

15. Az IKT-kockázat ezen iránymutatások 3. címében meghatározott értékeléséből adódó eredményeknek információkkal kell szolgálniuk a működési kockázat értékelésére vonatkozó megállapításokhoz, és azokat információként figyelembe kell venni az EBH SREP-iránymutatásainak 6.4. címében meghatározott vonatkozó pontszámban.

16. Megjegyzendő, hogy jóllehet az illetékes hatóságoknak a kockázatok alkategóriáit általában a fő kategóriák részeként kell értékelniük (azaz az IKT-kockázatot a működési kockázat részeként fogják értékelni), amennyiben az illetékes hatóságok egyes alkategóriákat lényegesnek ítélnek, ezen alkategóriákat egyedileg is értékelhetik. E célból, amennyiben az illetékes hatóság lényeges kockázatként azonosítja az IKT-kockázatot, ezen iránymutatások megadják azt a pontozási táblázatot (1. táblázat), amelyet az IKT-kockázat mint önálló alkategória pontozásakor a – tőkét érintő kockázatok pontozásának az EBH SREP-iránymutatásaiban foglalt általános megközelítését követve – alkalmazni kell.

17. Az arra vonatkozó álláspont kialakításakor, hogy az IKT-kockázatot lényegesnek kell-e tekinteni, és emiatt az IKT-kockázatot a működési kockázat egyedi alkategóriájaként értékeljék és pontozzák, az illetékes hatóságok az EBH SREP-iránymutatásainak 6.1. szakaszában meghatározott kritériumokat alkalmazhatják.

18. Ezen iránymutatások alkalmazásakor az illetékes hatóságoknak adott esetben az IKT-kockázatok alkategóriáinak a mellékletben megadott nem teljes körű felsorolását és a mellékletben megadott kockázati forgatókönyveket kell figyelembe venniük, annak megjegyzése mellett, hogy a melléklet azokra az IKT-kockázatokra helyezi a hangsúlyt, amelyek súlyos veszteségekhez vezethetnek. Az illetékes hatóságok kizárhatnak egyes, az osztályozási rendszerben szereplő IKT-kockázatokat, ha azok nem lényegesek értékelésük szempontjából. Az intézményekkel szemben elvárás, hogy az IKT-kockázatok mellékletben meghatározott osztályozási rendszere helyett saját kockázati osztályozási rendszert tartsanak fenn.

19. Amennyiben ezen iránymutatásokat határokon átnyúló tevékenységet folytató bankcsoportok és azok szervezetei tekintetében alkalmazzák és már sor került felügyeleti kollégium létrehozására, úgy a részt vevő illetékes hatóságoknak – az EBH SREP-iránymutatásainak 11.1. szakasza értelmében végrehajtott SREP-értékeléssel kapcsolatos együttműködés keretében – a csoport valamennyi szervezetére kiterjedően következetesen, a lehető legnagyobb mértékben össze kell hangolniuk az egyes információk pontos és részletes tartalmát.

2. cím – Az intézmények IKT-ra vonatkozó irányításának és stratégiájának az értékelése

2.1 Általános alapelvek

20. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény általános irányítási és belső ellenőrzési keretrendszere kellően lefedi-e az IKT-rendszereket és a kapcsolódó kockázatokat, és hogy a vezető testület megfelelően kezeli-e ezeket a szempontokat, mivel az IKT szervesen hozzátartozik az intézmények megfelelő működéséhez.

21. Ezen értékelés elvégzése során az illetékes hatóságoknak figyelembe kell venniük a belső irányításról szóló EBH-ajánlásban (GL 44)[4] meghatározott követelményeket és standardokat a felelős belső irányítást és a kockázatikontroll környezetet illetően, valamint az e területre vonatkozó nemzetközi ajánlásokat, szabványokat, amennyiben ezek – az IKT-rendszerek és -kockázatok egyediségére tekintettel – alkalmazhatóak.

22. Az e címben foglalt értékelés nem fedi le az IKT-rendszer irányításának, kockázatkezelésének és kontrollintézkedéseinek azokat a sajátos elemeit, amelyek az ezen iránymutatások 3. címében taglalt egyedi IKT-kockázatok kezelésére összpontosulnak, hanem a következő területekre összpontosít:

    a. IKT-stratégia – rendelkezik-e az intézmény olyan IKT-stratégiával, amelyet megfelelően irányítanak, és amely összhangban van az intézmény üzleti stratégiájával;

    b. általános belső irányítás – az intézmény általános belső irányítási mechanizmusai megfelelőek-e az intézmény IKT-rendszereinek vonatkozásában; és

    c. az IKT-kockázat az intézmény kockázatkezelési keretrendszerében – az intézmény kockázatkezelési és belső ellenőrzési keretrendszere megfelelően védi-e az intézmény IKT-rendszereit.

23. A 22. bekezdés a) pontjának – jóllehet az intézmény irányításának az elemeiről biztosít információkat – főként az üzleti modell értékeléséhez kell alapanyagot szolgáltatnia, amellyel az EBH SREP-iránymutatásainak 4. címe foglalkozik. A b) és a c) pont az EBH SREP-iránymutatásainak 5. címe által felölelt témák értékelését egészíti ki, és az ezen iránymutatásokban leírt értékelésnek az EBH SREP-iránymutatásainak 5. címe szerinti érintett értékeléshez kell adatokat szolgáltatnia.

24. Ezen értékelés eredményének adott esetben a kockázatkezelés és kontrollintézkedések ezen iránymutatások 3. címében foglalt értékeléséhez kell információkat szolgáltatnia.

[4] Az EBH iránymutatása a felelős belső irányításról, GL 44, 2011. szeptember 27.

2.2 IKT-stratégia

25. Az illetékes hatóságoknak e szakasz keretében értékelniük kell, hogy az intézmény rendelkezik-e olyan IKT-stratégiával, amely felett az intézmény vezető testülete megfelelő felügyeletet gyakorol; összhangban van az üzleti stratégiával, különösen az IKT naprakészen tartása és a fontos és összetett IKT-változások megtervezése és végrehajtása tekintetében; és támogatja az intézmény üzleti modelljét.

2.2.1 Az IKT-stratégia fejlesztése és megfelelősége

26. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény rendelkezik-e az intézmény IKT-stratégiájának az előkészítésére és fejlesztésére szolgáló olyan keretrendszerrel, amely arányban áll IKT-tevékenységeinek jellegével, nagyságrendjével és összetettségével. Ezen értékelés elvégzése során az illetékes hatóságoknak a következőket kell figyelembe venniük:

    a. az üzletág(ak) felső vezetését [5] megfelelően bevonják-e az intézmény stratégiai IKT-prioritásainak a meghatározásába, illetve az IKT-ért felelős szakterület felső vezetése tisztában van-e a főbb üzleti stratégiák és kezdeményezések fejlesztésével, tervezésével és elindításával, azt biztosítandó, hogy az IKT-rendszerek, IKT-szolgáltatások és az IKT-szervezet (azaz az e rendszerek és szolgáltatások irányításáért és bevezetéséért felelős személyek), valamint az intézmény üzleti stratégiája között folyamatos legyen az összhang, és hogy az IKT-t eredményesen frissítsék;

    b. az IKT-stratégiát dokumentálják és támogatják-e konkrét végrehajtási tervek, különös tekintettel a fontos mérföldkövekre és az erőforrás-tervezésre (ideértve a pénzügyi forrásokat és a humán erőforrásokat), azt biztosítandó, hogy azok reálisak legyenek és lehetővé tegyék az IKT-stratégia megvalósítását;

    c. az intézmény időszakonként frissíti-e IKT-stratégiáját, különösen az üzleti stratégia változtatásakor, hogy biztosítsa az IKT-ra és az üzleti tevékenységre vonatkozó közép- és hosszú távú célkitűzések, tervek és tevékenységek közötti folyamatos összhangot; valamint

    d. az intézmény vezető testülete jóváhagyja-e az IKT-stratégiát, a végrehajtási terveket, és nyomon követi-e azok végrehajtását.

2.2.2 Az IKT-stratégia végrehajtása

27. Ha az intézmény IKT-stratégiája fontos és összetett IKT-változtatások végrehajtását követeli meg, vagy az intézmény üzleti modelljét érintő lényeges következményekkel járó változtatásokat igényel, az illetékes hatóságoknak értékelniük kell, hogy az intézmény rendelkezik-e a méretének, IKT-tevékenységeinek, valamint a változtatási tevékenységek szintjének megfelelő kontrollrendszerrel, az intézmény IKT-stratégiája eredményes végrehajtásának támogatása érdekében. Ezen értékelés elvégzése során az illetékes hatóságoknak figyelembe kell venniük, hogy a kontrollrendszer:

[5] Felső vezetés és vezető testület: a 2013. június 26-i 2013/36/EU irányelv 3. cikkének 7. pontjában meghatározott „vezető testület” és 3. cikkének 9. pontjában meghatározott „felső vezetés”.

a. magában foglal-e irányítási folyamatokat (pl. a haladás és a költségvetés nyomon követése és az ezekről való beszámolás) és megfelelő szervezeteket (pl. projektvezetési iroda, IKT irányítócsoport vagy ezzel egyenértékű), hogy az IKT stratégia programjainak végrehajtását eredményesen támogassák;

b. meghatározta-e és kiosztotta-e az IKT-ra vonatkozó stratégiai programok végrehajtásával kapcsolatos szerepeket és felelősségeket, külön figyelmet fordítva a kulcsszereplők tapasztalataira az alábbi területeken: fontos és összetett IKT-változások megszervezése, irányítása és nyomon követése, valamint a tágabb szervezetet és az emberi erőforrásokat érintő hatások kezelése (pl. a változással szembeni ellenállás kezelése, képzés, kommunikáció);

c. van-e a független kontroll- és belső ellenőrzési funkció, melyek biztosítják, hogy az IKT-stratégia végrehajtásával kapcsolatos kockázatokat azonosították, értékelték és eredményesen mérsékelték, és hogy az IKT-stratégia végrehajtását vezérlő irányítási keretrendszer eredményes; valamint

d. tartalmaz-e olyan tervezési és a tervezés felülvizsgálatára szolgáló folyamatot, amely rugalmasságot biztosít az azonosított fontos problémákra (pl. a végrehajtás során felmerülő problémák vagy késedelmek) vagy külső fejleményekre (pl. az üzleti környezetben bekövetkező fontos változások, technológiai problémák vagy innovációk) való reagáláshoz, biztosítva a stratégiai végrehajtási terv kellő időben történő kiigazítását.

2.3 Általános belső irányítás

28. Az illetékes hatóságoknak az EBH SREP-iránymutatásainak 5. címével összehangban értékelniük kell, hogy az intézmény megfelelő és átlátható, „a célnak megfelelő” vállalati struktúrával rendelkezik-e, és megfelelő irányítási rendszert hozott-e létre. Különös tekintettel az IKT-rendszerekre, összhangban az EBH belső irányításról szóló iránymutatásaival ennek az értékelésnek magában kell foglalnia annak az értékelését, hogy az intézmény megfelel-e az alábbi követelményeknek:

    a. stabil, átlátható szervezeti felépítés az IKT-ra vonatkozó egyértelmű feladatkörökkel, beleértve a vezető testületet és annak bizottságait, és az IKT-ért felelős legfontosabb személyek (pl. az informatikai igazgató, az operatív igazgató vagy ezzel egyenértékű szerepkör) megfelelő közvetett vagy közvetlen csatornával rendelkeznek a vezető testülethez, azt biztosítandó, hogy az IKT-val kapcsolatos fontos információkat vagy problémákat megfelelően jelentsék a vezető testületnek, és azokról annak szintjén folytassanak vitát és döntsenek; valamint

    b. a vezető testület ismeri az IKT-val kapcsolatos kockázatokat, és kezeli azokat;

29. Az EBH SREP-iránymutatásainak 5.2. szakasza szerint az illetékes hatóságoknak értékelniük kell, hogy az intézmény IKT kiszervezésére vonatkozó politikája és stratégiája figyelembe veszi-e adott esetben az IKT kiszervezése által az intézmény üzletmenetére és üzleti modelljére gyakorolt hatást.

2.4 Az IKT-kockázat az intézmény kockázatkezelési keretrendszerében

30. Az intézmény egész intézményre kiterjedő kockázatkezelési és belső kontrolljainak az EBH SREP-iránymutatásainak 5. címében meghatározott értékelése során az illetékes hatóságoknak mérlegelniük kell, hogy az intézmény kockázatkezelési és belső kontroll keretrendszere megfelelően védi-e az intézmény IKT-rendszereit, az intézmény méretével és tevékenységeivel, valamint az intézmény 3. címben meghatározott IKT-kockázati profiljával arányos módon. Az illetékes hatóságoknak különösen a következőket kell megállapítaniuk:

    a. a kockázatvállalási hajlandóság és a tőkemegfelelés belső értékelési eljárása (ICAAP) a működési kockázatok tágabb kategóriájának részeként lefedi-e az IKT-kockázatokat az általános kockázati stratégia meghatározása és a belső tőke megállapítása céljából; és

    b. az IKT-kockázatok az intézményi kockázatkezelési és belső kontroll keretrendszerek hatálya alá tartoznak-e.

31. Az illetékes hatóságoknak a fenti a) pont szerinti értékelést úgy kell elvégezniük, hogy mind az elvárt, mind a kedvezőtlen forgatókönyveket – pl. az intézményspecifikus vagy felügyeleti stressztesztben foglalt forgatókönyveket – figyelembe veszik.

32. Külön tekintettel a b) pontra, az illetékes hatóságoknak értékelniük kell, hogy az EBH SREP-iránymutatásai 104. bekezdésének a) és b) pontjában és 105. bekezdésének a) és c) pontjában részletezett független kontroll- és belső ellenőrzési funkciók megfelelőek-e ahhoz, hogy biztosítsák az IKT, illetve a kontroll- és ellenőrzési funkciók egymástól való megfelelő szintű függetlenségét, tekintettel az intézmény méretére és IKT-kockázati profiljára.

2.5 Az eredmények összesítése

33. Ezeknek az eredményeknek tükröződniük kell a megállapítások EBH SREP-iránymutatásainak 5. címe szerinti összesítésében, és az EBH SREP-iránymutatásainak 3. táblázatában foglalt szempontokkal összhangban a vonatkozó pontozás részét kell képezniük.

34. A fenti értékelés összegzése során az IKT-stratégia értékelése tekintetében a következő pontokat kell figyelembe venni:

    a. ha az illetékes hatóságok arra a következtetésre jutnak, hogy az intézmény irányítási keretrendszere nem megfelelő az intézmény 2.2. pont szerinti IKT-stratégiájának kialakításához és végrehajtásához, úgy ennek tükröződnie kell az intézmény belső irányításának az EBH SREP-iránymutatásai 5. címe 87. bekezdésének a) pontja szerinti értékelésében;

    b. ha az illetékes hatóságok a 2.2. pont szerinti fenti értékelésekből azt a következtetést vonják le, hogy az IKT-stratégia és az üzleti stratégia között az összehangolás jelentős hiánya áll fenn, amely jelentős káros hatást gyakorolhat az intézmény hosszú távú üzleti és/vagy pénzügyi célkitűzéseire, az intézmény fenntarthatóságára és/vagy üzleti modelljére vagy az intézmény azon üzletterületeire/üzletágaira, amelyeket az EBH SREP-iránymutatásai 62. bekezdésének a) pontjában a leglényegesebb üzletterületként határoztak meg, úgy ennek információként kell szolgálnia az üzleti modell SREP-iránymutatások 70. bekezdésének b) és c) pontja szerinti értékeléséhez; és

c. ha az illetékes hatóságok arra a következtetésre jutnak a fenti 2.2. pont szerinti értékelés alapján, hogy az intézmény nem feltétlenül rendelkezik elegendő IKT-erőforrással és IKT végrehajtási kapacitásokkal, hogy elvégezze és támogassa a fontos tervezett stratégiai változásokat, úgy ennek információként kell szolgálnia az üzleti modell EBH SREP-iránymutatásai 4. címe 70. bekezdésének b) pontja szerinti értékeléséhez.

3. cím – Az intézmény IKT-kockázatoknak való kitettségeinek és kontrollintézkedéseinek az értékelése

3.1 Általános szempontok

35. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény megfelelően azonosította-e, értékelte-e és mérsékelte-e IKT-kockázatait. E folyamatnak a működésikockázat-kezelési keretrendszer részét kell képeznie, és összhangban kell lennie a működési kockázat tekintetében alkalmazott megközelítéssel.

36. Az illetékes hatóságoknak először azonosítaniuk kell azokat a lényeges inherens IKT-kockázatokat, amelyeknek az intézmény ki van vagy ki lehet téve, majd értékelniük kell, hogy az intézmény IKT-kockázatok kezelésére szolgáló keretrendszere, eljárásai és kontrollintézkedései mennyire eredményesen mérsékelik e kockázatokat. Az értékelés eredményét a megállapítások összegzésében kell bemutatni, amely a SREP-iránymutatásokban szereplő, működési kockázatra vonatkozó pontszám egyik alapja. Amennyiben az IKT-kockázatot lényegesnek ítélik, és az illetékes hatóságok külön pontszámot kívánnak adni, az 1. táblázatot kell felhasználni a működési kockázat ezen alkategóriájának a pontozásához.

37. Az e cím szerinti értékelés során az illetékes hatóságoknak a felügyeleti értékelés prioritásainak azonosításához kiindulási alapként fel kell használniuk az EBH SREP-iránymutatásai 6. címének 127. bekezdésében meghatározott minden rendelkezésre álló információforrást, pl. az intézmény kockázatkezelési tevékenységeit, a jelentéstételt és az eredményeket. Az illetékes hatóságoknak ezen értékelés elvégzéséhez más információforrásokat is fel kell használniuk, adott esetben ideértve a következőket:

    a. az IKT-kockázat és a kontrollintézkedések önértékelése (ha az ICAAP-információkban megadják);
    b. az intézmény vezető testületének benyújtott, IKT-kockázattal kapcsolatos vezetői információk, pl. rendszeres és incidens vezérelt IKT kockázati jelentések (ezen belül a működési veszteségek adatbázisában szereplő információk), az intézmény kockázatkezelési szakterületéről származó IKT-kockázati kitettségi adatok;
    c. az intézmény audit bizottságának jelentett, IKT-val kapcsolatos belső és külső ellenőrzések megállapításai.

3.2 A lényeges IKT-kockázatok azonosítása

38. Az illetékes hatóságoknak az alábbi lépéseket követve kell azonosítaniuk azokat a lényeges IKT-kockázatokat, amelyeknek az intézmény ki van téve vagy ki lehet téve.

3.2.1 Az intézmény IKT-kockázati profiljának felülvizsgálata

39. Az intézmény IKT-kockázati profiljának felülvizsgálatakor az illetékes hatóságoknak az intézmény IKT-kockázati kitettségeire vonatkozó összes releváns információt figyelembe kell venniük, ideértve a 37. bekezdés szerinti információkat és az ezen iránymutatások 2. címe szerinti IKT szervezeti és intézményi kontrollintézkedésekben azonosított lényeges hiányosságokat és gyengeségeket, és ezeket az információkat adott esetben arányosan felül kell vizsgálniuk. E felülvizsgálat részeként az illetékes hatóságoknak a következőket kell figyelembe venniük:

    a. az intézmény IKT-rendszerének jelentős zavara által gyakorolt lehetséges hatás a pénzügyi rendszerre, belföldi és nemzetközi szinten egyaránt;
    b. az intézmény ki lehet-e téve IKT biztonsági kockázatoknak vagy IKT rendelkezésre állási és folytonossági kockázatoknak internetes függőségek, innovatív IKT-megoldások vagy egyéb üzleti forgalmazási csatornák nagymértékű bevezetése miatt, amelyek az intézményt nagyobb valószínűséggel tehetik kibertámadások céltáblájává;
    c. az intézmény jobban ki lehet-e téve IKT biztonsági kockázatoknak, IKT rendelkezésre állási és folytonossági kockázatoknak, IKT adatintegritási kockázatoknak vagy IKT-változásokkal kapcsolatos kockázatoknak IKT-rendszereinek (pl. fúziók és felvásárlások következményeként adódó) összetettsége vagy elavult jellege miatt;
    d. az intézmény végrehajt-e olyan lényeges változtatásokat IKT-rendszereiben és/vagy IKT-működésében (pl. fúziók és felvásárlások, elidegenítések vagy az alapvető IKT-rendszerek cseréjének következményeként), amelyek hátrányosan érinthetik az IKT-rendszerek stabilitását vagy szabályszerű működését, és lényeges IKT rendelkezésre állási és folytonossági kockázatokat, IKT biztonsági kockázatokat, IKT-változásokkal kapcsolatos kockázatokat vagy IKT adatintegritási kockázatokat eredményezhetnek;
    e. az intézmény kiszervezett-e a csoporton belül vagy kívül IKT-szolgáltatásokat vagy IKT-rendszereket, ami lényeges IKT kiszervezési kockázatnak teheti ki az intézményt;
    f. az intézmény agresszív IKT-költség-csökkentési intézkedéseket hajt-e végre, amelyek a szükséges IKT-beruházások, erőforrások és informatikai szakértelem csökkenéséhez vezethetnek, és növelhetik a kockázati osztályozási rendszerben szereplő valamennyi IKT-kockázati típusnak való kitettséget;
    g. egyes fontos IKT-tevékenységek/adatközpontok helye (pl. régiók, országok) növelheti-e az intézmény természeti katasztrófáknak (pl. árvíz, földrengés), politikai instabilitásnak vagy munkajogi konfliktusoknak és közrendi problémáknak való kitettségét, amelyek az IKT rendelkezésre állási és folytonossági kockázatok és az IKT biztonsági kockázatok lényeges növekedéséhez vezethetnek.

3.2.2 A kritikus IKT-rendszerek és szolgáltatások felülvizsgálata

40. Az intézményre potenciálisan jelentős prudenciális hatást gyakorló IKT-kockázatok azonosítására irányuló folyamat részeként az illetékes hatóságoknak felül kell vizsgálniuk az intézménytől származó dokumentumokat, és véleményt kell kialakítaniuk arról, hogy mely IKT-rendszerek és szolgáltatások kritikusak az intézmény alapvető tevékenységeinek megfelelő működése, rendelkezésre állása, folytonossága és biztonságossága szempontjából.

41. Az illetékes hatóságoknak e célból felül kell vizsgálniuk az intézmény által a kritikus IKT-rendszerek és -szolgáltatások azonosítása céljából alkalmazott módszereket és folyamatokat, figyelembe véve, hogy az intézmény egyes IKT-rendszereket üzletmenet-folytonossági és rendelkezésre állási, biztonsági (pl. a csalások megelőzése) és/vagy bizalmassági szempontból (pl. bizalmas adatok) minősíthet kritikusnak. A felülvizsgálat elvégzésekor az illetékes hatóságoknak figyelembe kell venniük, hogy a kritikus IKT-rendszereknek és -szolgáltatásoknak az alábbiak közül legalább egy feltételnek meg kell felelniük:

    a. az intézmény alapvető üzleti tevékenységeit és forgalmazási csatornáit (pl. ATM-ek, internet és mobilbanki szolgáltatások) támogatják;

    b. alapvető irányítási folyamatokat és szervezeti funkciókat támogatnak, a kockázatkezelést is ide értve (pl. kockázatkezelési és pénzgazdálkodási rendszerek);

    c. külön jogi vagy szabályozási követelmények hatálya alá tartoznak (adott esetben), amelyek emelt követelményeket szabnak meg a rendelkezésre állás, az ellenálló képesség, a bizalmasság vagy a biztonságosság tekintetében (pl. adatvédelmi jogszabályok vagy lehetséges „helyreállítási időre vonatkozó célkitűzések” (Recovery Time Objectives – RTO, az a maximális idő, amelyen belül valamely rendszert vagy folyamatot az incidenst követően helyre kell állítani) és „helyreállítási pontra vonatkozó célkitűzések” (Recovery Point Objective – RPO, az a maximális időtartam, amelyen át incidens bekövetkezése esetén adatok veszhetnek el)) egyes rendszerszinten fontos szolgáltatások vonatkozásában (adott esetben);

    d. olyan bizalmas vagy érzékeny adatokat dolgoznak fel vagy tárolnak, amelyekhez való jogosulatlan hozzáférés jelentősen kihatna az intézmény hírnevére, pénzügyi eredményeire vagy üzletmenetének megbízhatóságára és folytonosságára (pl. érzékeny ügyféladatokat tartalmazó adatbázisok); és/vagy

    e. alapvető funkciókat biztosítanak, amelyek létfontosságúak az intézmény megfelelő működéséhez (pl. távközlési és csatlakoztatási szolgáltatások, IKT- és kiberbiztonsági szolgáltatások).

3.2.3 A kritikus IKT-rendszereket és -szolgáltatásokat érintő lényeges IKT-kockázatok azonosítása

42. Az illetékes hatóságoknak – az intézmény IKT-kockázati profiljának és kritikus IKT-rendszereinek és -szolgáltatásainak az elvégzett felülvizsgálatait figyelembe véve – véleményt kell alkotniuk a lényeges IKT-kockázatokról, amelyek felügyeleti megítélésük alapján jelentős prudenciális hatást gyakorolhatnak az intézmény kritikus IKT-rendszereire és -szolgáltatásaira.

43. Az IKT-kockázatok által az intézmény kritikus IKT-rendszereire és -szolgáltatásaira gyakorolt potenciális hatás értékelésekor az illetékes hatóságoknak a következőket kell figyelembe venniük:

    a. pénzügyi hatás, ideértve (többek között) a források vagy eszközök elvesztését, az ügyfelek potenciális kártalanítását, a jogi és rendezési költségeket, a szerződéses kötbéreket, a kieső bevételt;

    b. az üzletmenet zavarának lehetősége, ideértve (többek között) az érintett pénzügyi szolgáltatások kritikus voltát; a potenciálisan érintett ügyfelek és/vagy fiókok és alkalmazottak számát;

c. az intézményre gyakorolt, hírnévvel kapcsolatos potenciális hatás, az érintett banki szolgáltatás vagy operatív tevékenység kritikus volta alapján (pl. ügyféladatok ellopása); az érintett IKT-rendszerek és -szolgáltatások külső profilja/láthatósága alapján (pl. mobil vagy online banki rendszerek, értékesítési helyi (POS) rendszerek, ATM-ek vagy pénzforgalmi rendszerek);

d. szabályozási hatás, ideértve a szabályozó hatóság általi nyilvános bírálatot, bírságokat, sőt, akár az engedélyek módosítását;

e. az intézményre gyakorolt stratégiai hatás, például ha stratégiai termék- vagy üzleti terveket tesznek tönkre vagy lopnak el.

44. Az illetékes hatóságoknak ezt követően be kell sorolniuk az azonosított és lényegesnek minősített IKT-kockázatokat a következő IKT-kockázati kategóriákba, amelyek tekintetében a melléklet további kockázati leírásokat és példákat ad meg. Az illetékes hatóságoknak a 3. cím szerinti értékelés részeként át kell gondolniuk a mellékletben szereplő következő IKT-kockázatokat:

a. IKT rendelkezésre állási és folytonossági kockázat
b. IKT biztonsági kockázat
c. IKT-változások kockázata
d. IKT adatintegritási kockázat
e. IKT kiszervezési kockázat

A besorolás célja az illetékes hatóságok annak eldöntésében való segítése, hogy mely kockázatok lényegesek (adott esetben), és így mely kockázatok tekintetében kell a következő értékelési lépések során közelebbi és/vagy mélyrehatóbb felülvizsgálatot végezni.

3.3 A lényeges IKT-kockázatok mérséklésére szolgáló kontrollintézkedések értékelése

45. Az intézmény fennmaradó IKT-kockázati kitettségének értékelése érdekében az illetékes hatóságoknak felül kell vizsgálniuk, hogy az intézmény hogyan azonosítja, kíséri figyelemmel, értékeli és mérsékli az illetékes hatóságok által a fenti értékelés során azonosított lényeges kockázatokat.

46. E célból az illetékes hatóságoknak az azonosított lényeges IKT-kockázatok tekintetében felül kell vizsgálniuk:

a. az alkalmazandó IKT-kockázatkezelési politikát, -folyamatokat és kockázatvállalási limiteket;

b. az alkalmazandó szervezetirányítási és felügyeleti keretrendszert;

c. az alkalmazandó belső ellenőrzési lefedettséget és a megállapításokat;

d. a kifejezetten az azonosított lényeges IKT-kockázathoz kapcsolódó IKT-kockázati kontrollintézkedéseket.

47. Az értékelésnek figyelembe kell vennie az általános kockázatkezelési és belső kontroll keretrendszer EBH SREP-iránymutatásainak 5. címében említett elemzésének az eredményét, valamint az intézmény irányítására és stratégiájára irányuló, ezen iránymutatások 2. címében tárgyalt elemzés eredményét,

mivel az e területeken azonosított jelentős hiányosságok befolyásolhatják az intézmény képességét arra, hogy kezelje és mérsékelje IKT-kockázati kitettségeit. Az illetékes hatóságoknak adott esetben az ezen iránymutatások 37. bekezdésében foglalt információforrásokat is fel kell használniuk.

48. Az illetékes hatóságoknak a következő értékelési lépéseket az intézmény tevékenységeinek jellegével, nagyságrendjével és összetettségével arányos módon kell elvégeznie, az intézmény IKT-kockázati profiljának megfelelő felügyeleti felülvizsgálat alkalmazásával.

3.3.1 IKT-kockázatkezelési politika, folyamatok és kockázatvállalási limitek

49. Az illetékes hatóságoknak felül kell vizsgálniuk, hogy az intézmény megfelelő kockázatkezelési politikákkal, folyamatokkal és kockázatvállalási limitekkel rendelkezik-e az azonosított lényeges IKT-kockázatok tekintetében. Ezek a működési kockázat kezelésére szolgáló keretrendszer részei is lehetnek, vagy külön dokumentumban is szerepelhetnek. Ezen értékelés során az illetékes hatóságoknak a következőket kell figyelembe venniük:

    a. a kockázatkezelési politikát hivatalossá tették-e és a vezető testület jóváhagyta-e, és elégséges útmutatást tartalmaz-e az intézmény IKT-kockázatvállalási hajlandóságára és az IKT-kockázat kezelésével kapcsolatban követett fő célkitűzésekre és/vagy az alkalmazott IKT-kockázatvállalási limitekre vonatkozóan. A vonatkozó IKT-kockázatkezelési politikát az összes érintett érdekelt féllel is közölni kell;

    b. az alkalmazandó politika lefedi-e az azonosított lényeges IKT-kockázatok kockázatkezelése szempontjából jelentős összes elemet;

    c. az intézmény bevezetett-e az érintett lényeges IKT-kockázatok azonosítását (pl. kockázati kontroll önértékelés (RCSA), kockázati forgatókönyv-elemzés) és nyomon követését célzó folyamatot és mögöttes eljárásokat;

    d. az intézmény rendelkezik-e az IKT-kockázat kezelésével kapcsolatos jelentéstétellel, amely kellő időben információkkal látja el a felső vezetést és a vezető testületet, és amely lehetővé teszi a felső vezetés és/vagy a vezető testület számára annak értékelését és nyomon követését, hogy az intézmény IKT-kockázatmérséklési tervei és intézkedései összhangban vannak-e kockázatvállalási hajlandóságra/kockázati toleranciára vonatkozó jóváhagyott limitekkel (adott esetben), továbbá lehetővé teszi a lényeges IKT-kockázatok változásának nyomon követését.

3.3.2 A kockázat kezelésére és ellenőrzésére szolgáló szervezeti keretrendszer

50. Az illetékes hatóságoknak értékelniük kell, hogy az alkalmazandó kockázatkezelési szerepek és felelősségek hogyan ágyazódnak be és integrálódnak az azonosított lényeges IKT-kockázatok kezelésére és felügyeletére szolgáló belső szervezetbe. Az illetékes hatóságoknak e tekintetben értékelniük kell, hogy az intézmény bizonyítani tudja-e a következők fennállását:

    a. az érintett lényeges IKT-kockázatok azonosításával, értékelésével, monitorozásával, mérséklésével, jelentésével és felügyeletével kapcsolatos egyértelmű szerepkörök és felelősségek;

b. a kockázati felelősségeket és szerepeket egyértelműen közölték, kiosztották és beágyazták a szervezet valamennyi érintett részébe (pl. üzletágak, IT) és szervezetébe, ideértve a kockázati információk összegyűjtésével és összesítésével, valamint azoknak a felső vezetés és/vagy a vezető testület felé való jelentésével kapcsolatos szerepeket és felelősségeket is;
c. az IKT-kockázatkezelési tevékenységeket elegendő és minőségi szempontból megfelelő humán és technikai erőforrás segítségével végzik el. Az alkalmazandó kockázatmérséklési tervek hitelességének értékelése érdekében az illetékes hatóságoknak azt is értékelniük kell, hogy az intézmény elégséges pénzügyi költségvetést és/vagy egyéb szükséges erőforrást biztosított-e e tervek végrehajtásához;
d. A független kontrollintézkedések IKT-kockázat(ok)ra vonatkozó fontos megállapításait a vezető testület megfelelően nyomon követi és reagál azokra, figyelembe véve a hatáskör – valamely bizottságra (ha létezik ilyen) való lehetséges átruházását bizonyos szempontokat illetően; és
e. az alkalmazandó IKT-szabályzatok és -politikák alóli kivételeket nyilvántartják, azokat független kontrolintézkedés keretében – a kapcsolódó kockázatokra összpontosítva – dokumentált felülvizsgálatnak vetik alá, és azokról jelentést tesznek.

3.3.3 A belső ellenőrzés által lefedett terület és annak megállapításai

51. Az illetékes hatóságoknak mérlegelniük kell, hogy a belső ellenőrzési funkció eredményes-e az alkalmazandó IKT-kockázatkezelési keretrendszer ellenőrzését illetően, a következők felülvizsgálata révén:

a. az IKT-kockázatkezelési keretrendszert az előírt minőségben, mélységben és gyakorisággal, valamint az intézmény méretével, tevékenységeivel és IKT-kockázati profiljával arányosan ellenőrzik-e;

b. az ellenőrzési terv magában foglal-e az intézmény által azonosított kritikus IKT-kockázatokra irányuló ellenőrzéseket;

c. jelentik-e a vezető testületnek az IKT-val kapcsolatos ellenőrzések fontos megállapításait, ezen belül az elfogadott javító intézkedéseket; és

d. az IKT-val kapcsolatos ellenőrzések megállapításait, ezen belül az elfogadott egyeztetett javító intézkedéseket nyomon követik-e, és a státusz jelentéseket a felső vezetés és/vagy az audit bizottság rendszeres időközönként tárgyalja-e.

3.3.4 A kifejezetten az azonosított lényeges IKT-kockázathoz kapcsolódó IKT-kockázati kontrollintézkedések

52. Az azonosított lényeges IKT-kockázatok tekintetében az illetékes hatóságoknak értékelniük kell, hogy az intézmény rendelkezik-e külön kontrollintézkedésekkel e kockázatok kezeléséhez. A következő szakaszok tartalmazzák a 3.2.3. pont szerint azonosított lényeges kockázatok értékelésekor figyelembe veendő külön kontrollintézkedések nem teljes körű felsorolását, amelyeket a következő IKT-kockázati kategóriákba soroltak be:

a. IKT rendelkezésre állási és folytonossági kockázatok;
b. IKT biztonsági kockázatok;

c. IKT-változások kockázatai;
d. IKT adatintegritási kockázatok;
e. IKT kiszervezési kockázatok.

(a) A lényeges IKT rendelkezésre állási és folytonossági kockázatok kezelésére szolgáló kontrollintézkedések

53. Az EBH SREP-iránymutatásaiban (279–281. bekezdés) foglalt követelményeken túlmenően az illetékes hatóságoknak értékelniük kell, hogy az intézmény megfelelő keretrendszerrel rendelkezik-e az IKT rendelkezésre állási és folytonossági kockázatok azonosításához, megértéséhez, méréséhez és mérsékléséhez.

54. Ezen értékelés érdekében az illetékes hatóságoknak különösen azt kell figyelembe venniük, hogy a keretrendszer:

a. azonosítja-e a kritikus IKT-folyamatokat és az érintett támogató IKT-rendszereket, amelyeknek az üzletmenet-ellenállósági és -folytonossági tervek részét kell képezniük, a következők révén:

   i. a kritikus üzleti folyamatok és a támogató rendszerek közötti függőségek átfogó elemzése;

   ii. a támogató IKT-rendszerekre vonatkozó helyreállítási célkitűzések meghatározása (ezt az üzlet és/vagy a szabályzatok jellemzően RTO és RPO megadásával határozzák meg);

   iii. megfelelő készenléti tervezés, amely lehetővé teszi a kritikus IKT-rendszerek és -szolgáltatások rendelkezésre állását, folytonosságát és helyreállítását, hogy elfogadható korlátokon belül minimálisra csökkentsék az intézmény tevékenységének zavarát.

b. rendelkezik-e az üzletmenet-rugalmasság és az üzletmenet-folytonosság ellenőrzésére szolgáló környezetre vonatkozó politikákkal és standardokkal, valamint működési kontrollintézkedésekkel, amelyek a következőket foglalják magukban:

   i. az annak elkerülését szolgáló intézkedések, hogy egyazon forgatókönyv, esemény vagy katasztrófa az éles és a tartalék IKT-rendszereket egyaránt sújtsa;

   ii. az IKT-rendszer mentését és helyreállítását célzó eljárások a kritikus szoftverek és adatok tekintetében, amelyek biztosítják, hogy e mentéseket biztonságos és kellően távoli helyen tárolják, hogy a rendszert érintő esemény vagy katasztrófa ne tudja megsemmisíteni vagy megrongálni e kritikus adatokat;

   iii. az IKT rendelkezésre állását vagy folytonosságát érintő incidensek kellő időben történő felderítésére szolgáló nyomonkövetési megoldások;

   iv. dokumentált incidenskezelési és eszkalációs folyamat, amely az incidensek kezelésével és eszkalálásával kapcsolatos különböző szerepekre és felelősségekre, a válságbizottság(ok) tagjaira és a vészhelyzet esetén alkalmazandó parancsnoki láncra vonatkozóan is útmutatást nyújt;

v. az intézmény kritikus IKT-infrastruktúráinak (pl. adatközpontok) a környezeti kockázatokkal (pl. árvíz és egyéb természeti katasztrófák) szembeni védelmét szolgáló és az IKT-rendszerek megfelelő működési környezetét biztosító (pl. légkondicionálás) fizikai intézkedések;

vi. olyan folyamatok, szerepek és felelősségek, amelyek biztosítják, hogy a kiszervezett IKT-rendszerekre és -szolgáltatásokra is megfelelő üzletmenet-rugalmassági és -folytonossági megoldások és tervek vonatkozzanak;

vii. a kritikus IKT-rendszereket és -szolgáltatásokat érintő IKT teljesítmény- és kapacitástervezési és nyomonkövetési megoldások, meghatározott rendelkezésre állási követelményekkel, hogy kellő időben feltárják a teljesítménnyel és kapacitással kapcsolatos korlátokat;

viii. amennyiben szükséges és helyénvaló, a kritikus internetes tevékenységek vagy szolgáltatások (pl. e-banki szolgáltatások) túlterheléses támadásokkal és más, az internet irányából érkező kibertámadásokkal szembeni védelmét szolgáló megoldások, amely támadások célja az e tevékenységekhez és szolgáltatásokhoz való hozzáférés megakadályozása vagy zavarása;

c. reális teszt forgatókönyvek körén teszteli-e az IKT rendelkezésre állási és folytonossági megoldásokat, amelyek kibertámadások, vészhelyzeti átkapcsolások és a kritikus szoftverek és adatok biztonsági mentéseinek tesztelését foglalják magukban, és:

i. e teszteket megtervezik, kihirdetik és dokumentálják, és a teszteredményeket felhasználják az IKT rendelkezésre állási és folytonossági megoldások eredményességének megerősítésére;

ii. e tesztekbe bevonják a szervezeten belüli érdekelt feleket és funkciókat, így például az üzletágak vezetőit, ideértve az üzletfolytonossági, incidens- és válságreagálási csoportokat, valamint a szervezet normál működéséhez szükséges külső közreműködőket;

iii. a vezető testületet és a felső vezetést (pl. a válságkezelési csoportok részeként) megfelelően bevonják a tesztekbe, és tájékoztatják a tesztek eredményeiről.

(b) A lényeges IKT biztonsági kockázatok kezelésére szolgáló kontrollintézkedések

55. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény hatékony keretrendszerrel rendelkezik-e az IKT biztonsági kockázatok azonosítása, megértése, mérése és mérséklése céljából. Ezen értékelés érdekében az illetékes hatóságoknak különösen azt kell figyelembe venniük, hogy a keretrendszer vizsgálja-e a következőket:

a. léteznek-e egyértelműen meghatározott szerepek és felelősségek a következőket illetően:

i. az IKT-biztonság mindennapi irányításáért és az átfogó IKT-biztonsági politikák kidolgozásáért felelős és/vagy elszámoltatható személy(ek) és/vagy bizottságok, odafigyelve ezek szükséges függetlenségére;

ii. az IKT-biztonsági kontrollintézkedések kialakítása, végrehajtása, irányítása és nyomon követése;

iii. a kritikus IKT-rendszerek és -szolgáltatások védelme például sebezhetőségi értékelési folyamat, a szoftver-javítócsomagok kezelése, végponti védelem (pl. rosszindulatú vírusok), behatolásfelderítési és -megelőzési eszközök bevezetése révén;
iv. a külső és belső IKT-biztonsági események nyomon követése, minősítése és kezelése, ideértve az eseményekre való reagálást és az IKT-rendszerek és -szolgáltatások újraindítását és helyreállítását;
v. rendszeres és proaktív fenyegetésértékelések a megfelelő biztonsági kontrollintézkedések fenntartása érdekében.

b. létezik-e olyan IKT-biztonsági politika, amely figyelembe veszi, és ahol lehet, illeszkedik a nemzetközileg elismert IKT-biztonsági szabványokhoz és biztonsági elvekhez (pl. a „legkisebb jogosultság elve", azaz a hozzáférés azon minimális szintre való korlátozása, amely lehetővé teszi a hozzáférési jogok kezelésének rendes működését, valamint a „mélységi védelem" elve, azaz a biztonsági architektúra kialakítása terén a többrétegű biztonsági mechanizmusok növelik a rendszer egészének biztonságát);

c. létezik-e olyan folyamat, mely azonosítja az IKT-rendszereket, szolgáltatásokat és az olyan arányos biztonsági követelményeket, melyek választ adnak a potenciális csalás kockázatára és/vagy a bizalmas adatokkal való lehetséges visszaélésre és/vagy azok lehetséges helytelen felhasználására. Továbbá ez a folyamat meghatározza azokat a dokumentált biztonsági elvárásokat, amelyeket ezen azonosított IKT-rendszerek, -szolgáltatások és adatok tekintetében be kell tartani; illeszkedve az intézmény kockázatvállalási hajlandóságához, és biztosítja a helyes végrehajtás nyomon követését;

d. létezik-e a biztonsági incidensek kezelésének és eszkalálásának dokumentált folyamata, amely az incidensek kezelésével és eszkalálásával kapcsolatos különböző szerepekre és felelősségekre, a válságbizottság(ok) tagjaira és a biztonsági vészhelyzet esetén alkalmazandó parancsnoki láncra vonatkozóan is útmutatást nyújt;

e. a felhasználói és adminisztratív tevékenységek naplózása, amely lehetővé teszi a jogosulatlan tevékenységek eredményes nyomon követését és kellő időben való felderítését; és segíti a biztonsági eseményekre irányuló bűnügyi vizsgálatok lefolytatását. Az intézménynek olyan naplózási politikákkal kell rendelkeznie, amelyek meghatározzák a vezetendő naplók megfelelő típusait és azok megőrzési idejét;

f. biztonságtudatosság növelő és tájékoztató kampányok vagy kezdeményezések, hogy az intézményben minden szintet tájékoztassanak az intézmény IKT-rendszereinek biztonságos használatáról és védelméről, valamint a fő IKT-biztonsági (és egyéb) kockázatokról, amelyekről az adott szintnek tudnia kell, különösen a fennálló vagy a későbbiekben megjelenő kiberfenyegetéseket (pl. számítógépes vírusok, lehetséges belső vagy külső visszaélések vagy támadások, kibertámadások) illetően, valamint a munkavállalók a biztonság megsértésének mérséklésében betöltendő szerepéről;

g. megfelelő fizikai intézkedések (pl. CCTV, riasztóberendezés, biztonsági ajtók), a kritikus és érzékeny IKT-rendszerekhez (pl. adatközpontok) való jogosulatlan fizikai hozzáférés megakadályozása érdekében;

h. az IKT-rendszerek internet felől érkező támadásokkal (azaz kibertámadásokkal) vagy más külső hálózatok (pl. hagyományos távközlési kapcsolatok vagy megbízható partnerekkel fenntartott

kapcsolatok) irányából érkező támadásokkal szembeni védelmét szolgáló intézkedések. Az illetékes hatóságoknak felül kell vizsgálniuk, hogy az intézmény keretrendszere figyelembe veszi-e a következőket:

i. az összes olyan kifelé tekintő hálózati kapcsolati pont (pl. weboldalak, internetalkalmazások, WIFI, távoli elérés) teljes és naprakész leltárának és áttekintésének fenntartását célzó folyamat és megoldások, amelyen keresztül harmadik felek betörhetnének a belső IKT-rendszerekbe.

ii. szorosan kezelt és nyomon követett biztonsági intézkedések (pl. tűzfalak, proxy szerverek, levéltovábbítók, vírusirtók és tartalomszűrők), amelyek célja a bejövő és kimenő hálózati forgalom (pl. e-mail), valamint azon kifelé tekintő hálózati kapcsolatok biztonságának biztosítása, amelyen keresztül harmadik felek betörhetnének a belső IKT-rendszerekbe;

iii. az azon weboldalak és alkalmazások biztosítását célzó folyamatok és megoldások, amelyek az internetről és/vagy kívülről közvetlenül támadhatók, és amelyek a belső IKT-rendszerekbe való belépés pontjaként szolgálhatnak. Ezek általában a következő együttesét foglalják magukban: elismert biztonságos fejlesztési gyakorlatok, az IKT-rendszer támadási felületének csökkentésére (hardening) és sérülékenységének szűrésére szolgáló gyakorlatok, és/vagy további biztonsági megoldások, mint például alkalmazási tűzfalak és/vagy behatolásfelderítési (IDS) és/vagy behatolásmegelőzési (IPS) rendszerek bevezetése;

iv. a biztonsági behatolási tesztelések időszakonkénti végzése, hogy értékeljék a bevezetett kiberbiztonsági és belső IKT-biztonsági intézkedések és folyamatok eredményességét. E teszteket a személyzetnek és/vagy a szükséges szakértelemmel rendelkező külső szakértőknek kell elvégezniük, a teszteredmények dokumentálásával és a következtetések felső vezetésnek és/vagy vezető testületnek való jelentésével. Amennyiben szükséges és alkalmazandó, az intézménynek le kell vonnia a tanulságot e tesztekből arra vonatkozóan, hogy hol kell tovább javítani a biztonsági kontrollintézkedéseket és folyamatokat és/vagy jobb bizonyosságot szerezni azok eredményességére vonatkozóan.

(c) Az IKT változásaival kapcsolatos lényeges kockázatok kezelésére szolgáló kontrollintézkedések

56. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény hatékony keretrendszerrel rendelkezik-e az IKT-változásokhoz kapcsolódó kockázatok azonosítása, megértése, mérése és mérséklése céljából, amely arányban áll az intézmény tevékenységeinek jellegével, nagyságrendjével és összetettségével, valamint az intézmény IKT-kockázati profiljával. Az intézmény keretrendszerének fel kell ölelnie az IKT-rendszerek fejlesztésével, tesztelésével és változtatásainak jóváhagyásával kapcsolatos kockázatokat, ideértve a szoftverek fejlesztését vagy változtatását, mielőtt azokat az éles környezetbe migrálnák, és biztosítania kell a megfelelő IKT-életciklus kezelést. Ezen értékelés érdekében az illetékes hatóságoknak különösen azt kell figyelembe venniük, hogy a keretrendszer vizsgálja-e a következőket:

a. dokumentált folyamatok az IKT-rendszerek változásainak kezelése és ellenőrzése céljából (pl. konfiguráció- és javítócsomag-kezelés) és az adatok változásainak kezelése és ellenőrzése céljából (pl. hibajavítás és adatjavítások), amelyek biztosítják az IKT-kockázatkezelés megfelelő bevonását az

IKT olyan fontos változásai esetén, amelyek jelentős hatást gyakorolhatnak az intézmény kockázati profiljára vagy kitettségére;

b. a bevezetett IKT-változások különböző szakaszaira vonatkozó összeférhetetlenségi előírások (pl. megoldások tervezése és fejlesztése, új szoftverek és/vagy változások tesztelése és jóváhagyása, migráció és az éles környezetben való bevezetés, valamint hibajavítás), a bevezetett megoldásokra és az éles IKT-rendszereket és adatokat érintő változások kezelésével és ellenőrzésével kapcsolatos, az IKT-személyzet (pl. fejlesztők, IKT-rendszergazdák, adatbázis-adminisztrátorok) vagy bármely másik fél (pl. üzleti felhasználók, szolgáltatók) által ellátott feladatok elkülönítésére összpontosítva;

c. az éles környezetet megfelelően tükröző tesztkörnyezetek;

d. az éles környezet, valamint a teszt- és fejlesztési környezet meglévő alkalmazásainak és IKT-rendszereinek eszköz nyilvántartása, hogy a szükséges változtatásokat (pl. verziófrissítések, javítások, konfigurációs változtatások) az érintett IKT-rendszerek tekintetében megfelelően lehessen kezelni, végrehajtani és nyomon követni;

e. a használatban lévő IKT-rendszerek életciklusának nyomon követésére és kezelésére szolgáló folyamat, amellyel biztosítható, hogy azok továbbra is megfeleljenek az aktuális üzleti és kockázatkezelési követelményeknek és támogassák azokat, valamint amellyel meg lehet győződni arról, hogy a használatban lévő IKT-megoldásokat és -rendszereket szállítóik továbbra is támogatják-e; és hogy ezt a szoftverfejlesztési életciklusra (SDLC) vonatkozó megfelelő eljárások kísérik-e;

f. a szoftverforráskódok ellenőrzési rendszere és megfelelő eljárások, amelyek célja, hogy megakadályozzák a jogosulatlan változtatásokat a házon belül fejlesztett szoftverek forráskódjában;

g. az új vagy lényegesen átalakított IKT-rendszerek biztonsági és sérülékenységi szűrésének folyamata az éles üzembe állítást és a lehetséges kibertámadásoknak való kitettséget megelőzően;

h. az IKT-rendszerek cseréjekor, archiválásakor, megszüntetésekor vagy megsemmisítésekor a bizalmas adatok jogosulatlan vagy nem szándékos kiszolgáltatásának megelőzésére szolgáló folyamat és megoldások;

i. független felülvizsgálati és hitelesítési folyamatok, amelyek célja az emberi hibák kockázatának csökkentése az IKT-rendszerek azon változtatásainak a végrehajtása során, amelyek fontos káros hatást gyakorolhatnak az intézmény rendelkezésre állására, üzletmenet-folytonosságára vagy biztonságára (pl. a tűzfal beállításának fontos változtatásai) vagy az intézmény biztonságára (pl. a tűzfalak változtatásai).

(d) Az IKT adatintegritással kapcsolatos lényeges kockázatok kezelésére szolgáló kontrollintézkedések

57. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény hatékony keretrendszerrel rendelkezik-e az IKT adatintegritáshoz kapcsolódó kockázatok azonosítása, megértése, mérése és mérséklése céljából, amely arányban áll az intézmény tevékenységeinek jellegével, nagyságrendjével és összetettségével és az intézmény IKT-kockázati profiljával. Az intézmény keretrendszerének figyelembe kell vennie az IKT-rendszerek által tárolt és feldolgozott adatok integritásának megőrzésével kapcsolatos kockázatokat. Ezen értékelés érdekében az illetékes hatóságoknak különösen azt kell figyelembe venniük, hogy a keretrendszer vizsgálja-e a következőket:

a. olyan politika, amely meghatározza az IKT-rendszerekben lévő adatok integritásának a kezelésével kapcsolatos szerepeket és felelősségeket (pl. adatépítész, adatmenedzserek[6], adatgondozók[7], adatgazdák/adatgazdászok[8]), és útmutatást nyújt azzal kapcsolatban, hogy az adatintegritás szempontjából mely adatok kritikusak, és mely adatokat kell meghatározott IKT-ellenőrzéseknek (pl. automatizált beviteli hitelesítési ellenőrzések, adatátadási ellenőrzések, egyeztetések stb.) vagy felülvizsgálatoknak (pl. az adatarchitektúrával való összeegyeztethetőség ellenőrzése) alávetni az IKT-adatok életciklusának különböző szakaszaiban;

b. dokumentált adatarchitektúra, adatmodell és/vagy -szótár, amelyet az érintett üzleti és IT érdekelt felekkel hitelesítenek, és amely támogatja az IKT-rendszerek körében az adatok szükséges következetességét, és biztosítja, hogy az adatarchitektúra, az adatmodell és/vagy az adatszótár folyamatosan illeszkedjen az üzleti és kockázatkezelési szükségletekhez;

c. a végfelhasználói számítástechnika (end-user computing – EUC) megengedett felhasználására és az arra való támaszkodásra vonatkozó politika, különösen a fontos végfelhasználói számítástechnikai megoldások azonosítását, nyilvántartását és dokumentálását illetően (pl. fontos adatok feldolgozásakor), valamint a jogosulatlan – akár magában az eszközben, akár az abban tárolt adatokban elvégzett – átalakítások megelőzése céljából elvárt biztonsági szintek;

d. a kivételek kezelésére szolgáló dokumentált folyamatok, amelyek célja az azonosított adatintegritási problémák azok kritikusságával és érzékenységével összhangban való megoldása.

58. Azon felügyelt intézmények esetében, amelyek a BCBS kockázati adatok eredményes összesítésére és a kockázati jelentéstételre vonatkozó 239. sz. elveinek[9] a hatálya alá tartoznak, az illetékes hatóságoknak felül kell vizsgálniuk az intézmény kockázati jelentéstételi és adatösszesítési kapacitásainak kockázati elemzését, az elvekkel és az erre vonatkozó, elkészített dokumentációval összehasonlítva azt, figyelembe véve az ezen elvekben foglalt végrehajtási időkeretet és átmeneti rendelkezéseket.

(e) Az IKT kiszervezésével kapcsolatos lényeges kockázatok kezelésére szolgáló kontrollintézkedések

59. Az illetékes hatóságoknak értékelniük kell, hogy az intézmény kiszervezési stratégiája, a CEBS kiszervezési iránymutatásaiban (2006) foglalt követelményekkel összhangban van-e és az EBH SREP-iránymutatásai 85. bekezdésének d) pontjában foglalt követelmények szerint megfelelően alkalmazandó-e az IKT kiszervezésére, beleértve a csoporton belüli kiszervezést is, amelynek keretében a csoporton belül nyújtanak IKT-szolgáltatásokat. Az IKT kiszervezési kockázatok értékelésekor az illetékes hatóságoknak figyelembe kell venniük, hogy az IKT kiszervezési kockázatok az inherens működési kockázatok EBH SREP-iránymutatásai 240. bekezdésének j) pontja szerinti értékelésének részeként is lefedhetők, a párhuzamos munka vagy a kétszeres beszámítás elkerülése érdekében.

[6] Az adatmenedzser az adatok feldolgozásáért és felhasználásáért felel.

[7] Az adatgondozó az adatok biztonságos őrzéséért, szállításáért és tárolásáért felel.

[8] Az adatgazdász az adatelemek – mind a tartalom, mind a metaadatok – kezeléséért és alkalmasságáért felel.

[9] Bázeli Bankfelügyeleti Bizottság, A kockázati adatok eredményes összesítésére és a kockázati jelentéstételre vonatkozó elvek, 2013. január, az interneten a következő címen érhető el: http://www.bis.org/publ/bcbs239.pdf.

60. Az illetékes hatóságoknak értékelniük kell különösen, hogy az intézmény hatékony keretrendszerrel rendelkezik-e az IKT kiszervezési kockázatok azonosítása, megértése és mérése céljából, és különösen, hogy rendelkezik-e olyan, a lényeges kiszervezett IKT-szolgáltatásokkal kapcsolatos kockázatok mérséklésére szolgáló kontrollintézkedésekkel és kontrollkörnyezettel, amely arányban áll az intézmény méretével, tevékenységeivel és IKT-kockázati profiljával, és magában foglalja a következőket:

a. az IKT kiszervezése által az intézmény kockázatkezelésére gyakorolt, a szolgáltatók (pl. felhőalapú szolgáltatások nyújtói) igénybevételével és ezek szolgáltatásaival összefüggő hatás a beszerzési folyamat során történő értékelése, amelyet dokumentálnak, és amelyet a felső vezetés vagy a vezető testület figyelembe vesz az arra vonatkozó döntés meghozatalakor, hogy kiszervezzék-e a szolgáltatásokat vagy sem. Az intézménynek felül kell vizsgálnia a szolgáltató IKT-kockázatkezelési politikáit, IKT-kontrollintézkedéseit és kontrollkörnyezetét, azt biztosítandó, hogy ezek megfeleljenek az intézmény belső kockázatkezelési célkitűzéseinek és kockázatvállalási hajlandóságának. E felülvizsgálatot a szerződéses kiszervezési időszak alatt rendszeresen frissíteni kell, figyelembe véve a kiszervezett szolgáltatások jellemzőit;

b. a kiszervezett szolgáltatások IKT-kockázatainak nyomon követése a szerződéses kiszervezési időszak alatt az intézmény kockázatkezelésének részeként, amely alapanyagot szolgáltat az IKT-kockázat kezelésére vonatkozó jelentéstételhez (pl. az üzletfolytonossági jelentés, biztonsági jelentés elkészítéséhez);

c. a kapott szolgáltatási szintek nyomon követése és összehasonlítása a szerződésben vállalt szolgáltatási szintekkel, amelyeknek a kiszervezési szerződés vagy a szolgáltatási szintre vonatkozó megállapodás (SLA) részét kell képezniük; és

d. megfelelő személyzet, erőforrások és hatáskörök a kiszervezett szolgáltatásokból származó IKT-kockázatok nyomon követéséhez és kezeléséhez.

3.4 Az eredmények összesítése és a pontszám meghatározása

61. A fenti értékelést követően az illetékes hatóságoknak véleményt kell alkotniuk az intézmény IKT-kockázatáról. Ennek a véleménynek tükröződnie kell az eredmények összegzésében, amelyet az illetékes hatóságoknak figyelembe kell venniük, amikor az EBH SREP-iránymutatásainak 6. táblázatában pontozzák a működési kockázatot. Az illetékes hatóságoknak a lényeges IKT-kockázatokra kell alapozniuk véleményüket, figyelembe véve a következő szempontokat, amelyeknek a működési kockázat értékelésének alapjául kell szolgálniuk:

a. Kockázattal kapcsolatos szempontok

i. az intézmény IKT-kockázati profilja és kitettségei;
ii. az azonosított kritikus IKT-rendszerek és -szolgáltatások; valamint
iii. a kritikus IKT-rendszereket érintő IKT-kockázat lényegessége.

b. A vezetéssel és a kontrollintézkedésekkel kapcsolatos szempontok

i. összhangban van-e az intézmény IKT-kockázatkezelési politikája és stratégiája, valamint általános stratégiája és kockázati hajlandósága;

ii. az IKT-kockázatkezelés szervezeti keretrendszere szilárd-e, és magában foglalja-e a kockázatgazdák és a vezetési és ellenőrzési funkciók világos felelősségeit és ezek feladatainak egyértelmű elkülönítését;
iii. megfelelőek-e az IKT-kockázatok mérésére, nyomon követésére és jelentésére szolgáló rendszerek; és
iv. szilárdak-e a lényeges IKT-kockázatok kontrollkeretei.

62. Ha az illetékes hatóságok lényegesnek ítélik az IKT-kockázatot, és az illetékes hatóság úgy dönt, hogy e kockázatot a működési kockázat alkategóriájaként értékeli és pontozza, az IKT-kockázat pontozásának szempontjait az alábbi táblázat (1. táblázat) adja meg.

1. táblázat: Felügyeleti szempontok az IKT-kockázat pontozásához

Kockázati pontszám	Felügyeleti vélemény	Inherens kockázatokra vonatkozó szempontok	Kockázatkezelés és kontrollintézkedések megfelelőségére vonatkozó szempontok
1	Az inherens kockázat szintjét, valamint a kockázatkezelést és a kontrollintézkedéseket figyelembe véve az intézményt érő jelentős prudenciális hatás kockázata nem észlelhető.	• A 37. bekezdés alapján figyelembe veendő információforrások nem tártak fel jelentős IKT-kockázati kitettségeket. • Az intézmény IKT-kockázati profiljának jellege, a kritikus IKT-rendszerek és az IKT-rendszereket és szolgáltatásokat érintő lényeges IKT-kockázatok felülvizsgálatával karöltve, nem utal semmilyen lényeges IKT-kockázatra.	• Az intézmény IKT-kockázati politikája és stratégiája arányban áll az általános stratégiájával és kockázatvállalási hajlandóságával. • Az IKT-kockázatra vonatkozó szervezeti keretrendszer szilárd, a felelősségi körök egyértelműen rögzítettek, a kockázatgazdák, illetve az irányítási és ellenőrzési funkciók feladatai
2	Az inherens kockázat szintjét, valamint a kockázatkezelést és a kontrollintézkedéseket figyelembe véve az intézményre nézve jelentős prudenciális hatás kockázata alacsony.	• A 37. bekezdés alapján figyelembe veendő információforrások nem tártak fel jelentős IKT-kockázati kitettségeket. • Az intézmény IKT-kockázati profiljának jellege, a kritikus IKT-rendszerek és az IKT-rendszereket és -szolgáltatásokat érintő lényeges IKT-kockázatok felülvizsgálatával karöltve, korlátozott IKT-kockázati kitettségre utalt (pl. az előre meghatározott IKT-	

		kockázati kategóriák közül ötből legfeljebb kettő).	egyértelműen elkülönülnek.
3	Az inherens kockázat szintjét, valamint az irányítást és a kontrollintézkedéseket figyelembe véve az intézményt érő jelentős prudenciális hatás kockázata közepes.	• A 37. bekezdés alapján figyelembe veendő információforrások lehetséges jelentős IKT-kockázati kitettségekre utaló jelzéseket tártak fel. • Az intézmény IKT-kockázati profiljának jellege, a kritikus IKT-rendszerek és az IKT-rendszereket és -szolgáltatásokat érintő lényeges IKT-kockázatok felülvizsgálatával karöltve, emelt IKT-kockázati kitettségre utalt (pl. az előre meghatározott IKT-kockázati kategóriák közül három vagy több).	• Az IKT-kockázat mérésére, nyomon követésére és jelentésére szolgáló rendszerek megfelelőek. • Az IKT-kockázatra vonatkozó ellenőrzési keretrendszerek észszerűek.
4	Az inherens kockázat szintjét, valamint a kockázatkezelést és a kontrollintézkedéseket figyelembe véve az intézményre nézve jelentős prudenciális hatás kockázata magas.	• A 37. bekezdés alapján figyelembe veendő információforrások több, jelentős IKT-kockázati kitettségekre utaló jelzést adtak. • Az intézmény IKT-kockázati profiljának jellege, a kritikus IKT-rendszerek és az IKT-rendszereket és -szolgáltatásokat érintő lényeges IKT-kockázatok felülvizsgálatával karöltve, magas IKT-kockázati kitettségre utalt (pl. az előre meghatározott IKT-kockázati kategóriák közül ötből négy vagy öt).	

Melléklet – Az IKT-kockázatok osztályozási rendszere

5 IKT-kockázati kategória azon IKT-kockázatok nem teljes körű felsorolásával, amelyek potenciálisan nagyon súlyosak és/vagy működési, hírnévvel kapcsolatos vagy pénzügyi hatással járnak

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
IKT rendelkezésre állási és folytonossági kockázatok	Nem megfelelő kapacitáskezelés	Az erőforrások (pl. hardverek, szoftverek, személyzet, szolgáltatók) hiánya azt eredményezheti, hogy nem tudják a szolgáltatást úgy méretezni, hogy megfeleljen az üzleti igényeknek, valamint a rendszer működésének megszakításához, a szolgáltatás romlásához és/vagy működési hibákhoz vezethet.	• A kapacitáshiány hátrányosan érintheti az átviteli sebességet és a hálózat (internet) olyan szolgáltatásokhoz való rendelkezésre állását, mint az internetes banki szolgáltatások. • A személyzet (belső vagy harmadik fél) hiánya a rendszer működésének megszakadásához és/vagy működési hibákhoz vezethet.
	Az IKT-rendszer hibái	A rendelkezésre állás hardverhibák miatti kiesése.	• A tárolás (merevlemezek), a szerver vagy más IKT-berendezés hibája/rossz működése, amelyet pl. a karbantartás hibája okozott.
		A rendelkezésre állás szoftverhibák miatti kiesése.	• Az alkalmazási szoftver végtelen ciklusa megakadályozza a tranzakció végrehajtását. • Olyan elavult IKT-rendszerek és -megoldások folytatódó használata miatti üzemszünetek, amelyek már nem felelnek meg a jelenlegi rendelkezésre állási és rugalmassági követelményeknek, és/vagy amelyeket a szállítóik már nem támogatnak.
	Nem megfelelő IKT-val kapcsolatos folytonossági és katasztrófa utáni	Az IKT-val kapcsolatban tervbe vett rendelkezésre állási és/vagy folytonossági megoldások és/vagy katasztrófa utáni helyreállítás (pl. a helyreállításhoz használt tartalék adatközpont) hibája, amikor azt eseményre reagálva aktiválják.	• Az elsődleges és a másodlagos adatközpont közötti konfigurációs különbségek következtében előfordulhat, hogy a tartalék adatközpont nem képes biztosítani a szolgáltatás tervbe vett folytonosságát.

[10] Az IKT-kockázatok azon kockázati kategóriában szerepelnek, amelyben a legnagyobb hatást gyakorolják, de más kockázati kategóriákban is hatást gyakorolhatnak.

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
	helyreállítási tervezés		
	Üzemzavart és pusztítást okozó kibertámadások	Különböző célú (pl. aktivista tevékenység, zsarolás) támadások, amelyek a rendszerek és a hálózat túlterheléséhez vezetnek, és megakadályozzák a jogszerű felhasználók online számítógépes szolgáltatásokhoz való hozzáférését.	• Az elosztott szolgáltatásmegtagadással járó támadásokat (Distributed Denial of Service, DDoS) a hekker által ellenőrzött több számítógépes rendszer segítségével hajtják végre az interneten, amelyek nagymennyiségű, látszólag jogszerű szolgáltatási kérelmet küldenek az internetes (pl. e-banki) szolgáltatásoknak.
IKT biztonsági kockázatok	Kibertámadások és más külső, IKT-n alapuló támadások	Az internetről vagy külső hálózatról, különböző célokból (pl. csalás, kémkedés, aktivista tevékenység/szabotázs, kiberterrorizmus), különféle technikák alkalmazásával (pl. társadalmi manipuláció, a sebezhetőségek kihasználásával végrehajtott behatolási kísérletek, rosszindulatú szoftverek felhasználása) végrehajtott támadások, amelyek eredményeképpen átveszik a belső IKT-rendszerek feletti ellenőrzést.	A támadások különböző típusai: • APT (Advanced Persistent Threat – fejlett állandó fenyegetés), amelynek célja a belső rendszerek feletti ellenőrzés megszerzése vagy információk ellopása (pl. személyazonossággal kapcsolatos információk vagy hitelkártya-információk ellopása). • Rosszindulatú szoftverek (pl. zsarolóvírusok – ransomware), amelyek zsarolás céljából titkosítják az adatokat. • A belső IKT-rendszerek trójai falovakkal való megfertőzése a rendszer elleni rosszindulatú lépések rejtett módon történő elkövetése érdekében. • Az IKT-rendszer és/vagy a (webes) alkalmazások sebezhetőségeinek a kihasználása (pl. SQL befecskendezés – SQL injection), a belső IKT-rendszerhez való hozzáférés megszerzése céljából.
		Csalárd pénzügyi tranzakciók hekkerek általi végrehajtása az e-banki és pénzforgalmi szolgáltatások feltörése vagy megkerülése révén és/vagy az intézmény belső pénzforgalmi rendszereiben fennálló biztonsági sebezhetőségek támadásával és kihasználásával.	• Az e-banki vagy pénzforgalmi szolgáltatások elleni támadások, jogosulatlan tranzakciók végrehajtása céljából. • Csalárd pénzforgalmi tranzakciók létrehozása és elküldése az intézmény belső pénzforgalmi

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
			rendszerein belülről (pl. csalárd SWIFT-üzenetek).
		Csalárd értékpapír-tranzakciók hekkerek általi végrehajtása az e-banki szolgáltatások biztonságának feltörése vagy megkerülése révén, amely az ügyfelek értékpapírszámláihoz is hozzáférést biztosít.	• Pump and dump támadások, amelyben a támadók ügyfelek e-banki értékpapírszámláihoz szereznek hozzáférést, és csalárd eladási vagy vételi utasításokat adnak, hogy befolyásolják a piaci árat és/vagy korábban létrehozott értékpapír-pozíciók alapján nyereségre tegyenek szert.
		A kommunikációs kapcsolatok és mindenfajta beszélgetések vagy az IKT-rendszerek elleni támadások információk gyűjtése és/vagy csalás elkövetése céljából.	• Hitelesítési adatok sima szöveges formátumban történő továbbításának kihallgatása/elfogása.
	Nem megfelelő belső IKT-biztonság	Jogosulatlan hozzáférés szerzése a kritikus IKT-rendszerekhez az intézményen belülről, különböző célokból (pl. csalás, tisztességtelen kereskedési tevékenységek végzése és elrejtése, adatlopás, aktivista tevékenység/szabotázs), különféle technikák segítségével (pl. jogosultságokkal való visszaélés és/vagy jogosultságok eszkalálása, személyazonosság-lopás, társadalmi manipuláció, az IKT-rendszerek sérülékenységeinek kihasználása, rosszindulatú szoftverek elterjesztése).	• A billentyűleütéseket figyelő alkalmazások (key(stroke) logger) telepítése, hogy felhasználói azonosítókat és jelszavakat lopjanak el bizalmas adatokhoz való hozzáférés megszerzése és/vagy csalás elkövetése céljából. • Gyenge jelszavak feltörése/kitalálása, hogy jogszerűtlen vagy bővített hozzáférési jogokhoz jussanak. • A rendszeradminisztrátor csalás elkövetésére használja fel az operációs rendszereket vagy (az adatbázis közvetlen módosítására szolgáló) adatbázis-kezelő eszközöket.
		Jogosulatlan IKT-manipulációk, amelyeket az IKT-val kapcsolatos hozzáférés-kezelési eljárások és gyakorlatok nem megfelelő volta tesz lehetővé.	• A szükségtelen fiókok üzemen kívül helyezésének vagy törlésének elmulasztása, így az olyan munkatársakhoz tartozó fiókok üzemen kívül helyezésének vagy törlésének elmulasztása, akik más beosztásba kerültek és/vagy kiléptek az intézményből, ideértve azokat a vendégeket vagy szállítókat is, akiknek már nincs szükségük hozzáférésre, jogosulatlan hozzáférést biztosítva ezáltal az IKT-rendszerekhez.

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
			• Túlzott hozzáférési jogok és jogosultságok biztosítása, ami jogosulatlan hozzáférést tesz lehetővé és/vagy lehetőséget nyújt tisztességtelen tevékenységek elrejtésére.
		A biztonság tudatosságának hiánya miatti biztonsági fenyegetések, ami miatt az alkalmazottak nem értik és elhanyagolják az IKT-val kapcsolatos biztonsági politikákat és eljárásokat, vagy nem tartják magukat ezekhez.	• Az alkalmazottak becsapása azzal a céllal, hogy segítséget nyújtsanak támadásokhoz (azaz társadalmi manipuláció). • A hitelesítő adatokkal kapcsolatos rossz gyakorlatok: a jelszavak megosztása, „könnyen” kitalálható jelszavak használata, ugyanazon jelszó használata sok különböző célra stb. • Nem titkosított bizalmas adatok laptopokon és olyan hordozható adattárolási megoldásokon (pl. USB-kulcsok) való tárolása, amelyek elveszíthetők vagy ellophatók.
		Bizalmas információk intézményen kívüli jogosulatlan tárolása vagy átadása.	• Bizalmas adatokat ellopó, illetve bizalmas adatokat jogosulatlan személyeknek vagy a nyilvánosságnak szándékosan kiszivárogtató vagy kicsempésző személyek.
	Nem megfelelő fizikai IKT-biztonság	IKT-eszközök helytelen felhasználása vagy ellopása fizikai hozzáférés útján, ami kárt okoz, eszközök vagy adatok elvesztéséhez vezet vagy más fenyegetéseket tesz lehetővé.	• Az irodaépületekbe és/vagy adatközpontokba való fizikai betörés IKT-berendezések (pl. számítógépek, laptopok, tárolási megoldások) ellopása és/vagy adatok IKT-rendszerekhez való fizikai hozzáférés révén történő lemásolása céljából.
		A fizikai IKT-eszközöket érő szándékos vagy véletlenszerű kár, amelyet terrorizmus, baleset vagy az intézmény személyzete és/vagy harmadik felek (szállítók, szervizemberek) általi sajnálatos/hibás manipuláció okoz.	• Az IKT-eszközök elleni fizikai terrorizmus (azaz terrorista bombák) vagy szabotázs. • Az adatközpont tűz, vízszivárgás vagy más tényezők okozta megsemmisülése.
		A természeti katasztrófákkal szembeni elégtelen fizikai védelem, amely az IKT-rendszerek/adatközpontok	• Földrengés, szélsőséges hőség, szélvihar, súlyos hóvihar, árvíz, tűz, villámlás.

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
		természeti katasztrófa miatti részleges vagy teljes megsemmisüléséhez vezet.	
IKT-változások kockázatai	Nem megfelelő ellenőrzés az IKT-rendszer változásai és az IKT-fejlesztés felett	A változások következtében fellépő felderítetlen hibák vagy sebezhetőségek (pl. valamely változás előre nem látott hatásai vagy a tesztelés hiánya vagy a nem megfelelő változásirányítási gyakorlatok miatt rosszul kezelt változás) okozta, pl. a szoftvereket, az IKT-rendszereket és az adatokat érintő események.	• Nem kellően letesztelt szoftverek beélesítése vagy olyan konfigurációs változtatások, amelyek nem várt káros hatást gyakorolnak az adatokra (pl. sérülés, törlés) és/vagy az IKT-rendszer teljesítményére (pl. összeomlás, a teljesítmény romlása). • Az IKT-rendszereket vagy az adatokat érintő ellenőrizetlen változtatások az éles környezetben. • Biztonsági szempontból gyenge IKT-rendszerek és internetes alkalmazások beélesítése, amely lehetőséget teremt a hekkerek számára, hogy megtámadják a nyújtott internetes szolgáltatásokat és/vagy feltörjék a belső IKT-rendszereket. • A belső fejlesztésű szoftverek forráskódjában elvégzett ellenőrizetlen változtatások. • Nem elégséges tesztelés a megfelelő tesztkörnyezetek hiánya miatt.
	Nem megfelelő IKT-architektúra	Az IKT-architektúra IKT-rendszerek (pl. szoftverek, hardverek, adatok) megtervezése, kiépítése és karbantartása során való gyenge kezelése idővel összetett, nehézkes, költségesen kezelhető és merev IKT-rendszerekhez vezethet, amelyek már nem illeszkednek kellően az üzleti szükségletekhez, és nem felelnek meg az aktuális kockázatkezelési követelményeknek.	• Az IKT-rendszereket, szoftvereket és/vagy adatokat érintő, hosszabb időn át nem megfelelően kezelt változások, amelyek összetett, heterogén és nehezen kezelhető IKT-rendszerekhez és -architektúrákhoz vezetnek, amelyek sok káros üzleti és kockázatkezelési hatást okoznak (pl. a rugalmasság és gyorsaság hiánya, IKT-események és -hibák, magas üzemeltetési költség, az IKT-biztonság és -rugalmasság meggyengülése, az adatminőség és a jelentéstételi képességek csökkenése). • Kereskedelemben kapható szoftvercsomagok túlzott testre szabása és belső fejlesztésű

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
			szoftverekkel való bővítése, aminek következtében a kereskedelemben kapható szoftver későbbi kiadásai és frissítései nem telepíthetők, és fennáll annak a kockázata, hogy azt a gyártó a továbbiakban nem támogatja.
	Nem megfelelő életciklus- és javítócsomag-kezelés	Nem vezetnek megfelelő leltárt valamennyi IKT-eszközről, amely támogatná és kiegészítené a megalapozott életciklus- és javítócsomag-kezelési gyakorlatokat. Ez nem kellően javított (és emiatt sérülékenyebb) és elavult IKT-rendszerekhez vezet, amelyek nem feltétlenül támogatják az üzleti és kockázatkezelési igényeket.	• Nem javított és elavult IKT-rendszerek, amelyek káros üzleti és kockázatkezelési hatásokkal járhatnak (pl. a rugalmasság és gyorsaság hiánya, IKT-kimaradások, az IKT-biztonság és -rugalmasság gyengülése).
IKT adatintegritási kockázatok	Nem jól működő IKT adatfeldolgozás vagy -kezelés	A rendszerek, a kommunikáció és/vagy az alkalmazások hibái vagy a hibásan végrehajtott adatkinyerési, -továbbítási és -betöltési (extraction, transfer and load – ETL) folyamatok miatt az adatok sérülhetnek vagy elveszhetnek.	• Az informatikai rendszer hibája a kötegelt feldolgozás során, amely az ügyfelek bankszámláinak hibás egyenlegéhez vezet. • Hibásan végrehajtott lekérdezések. • Az adatok másodpéldányban való eltárolásának (biztonsági mentésének) hibája miatti adatvesztés.
	Rosszul kialakított adathitelesítési kontrollok az IKT-rendszerekben	Az automatizált adatbevitelre és -elfogadásra vonatkozó kontrollintézkedések (pl. a harmadik felektől származó felhasznált adatok kapcsán), az adattovábbításra, -feldolgozásra és -kimenetre vonatkozó kontrollintézkedések (pl. a bemenet hitelesítéséhez kapcsolódó kontrollintézkedések, adategyeztetések) hiányához vagy eredménytelenségéhez kapcsolódó hibák az IKT-rendszerekben.	• A bemeneti adatok nem kellő vagy érvénytelen formázása/hitelesítése az alkalmazásokban és/vagy felhasználói felületeken. • Adategyeztetési kontrollintézkedések hiánya az előállított kimenetekkel kapcsolatban. • A végrehajtott adatkinyerési folyamatokra (pl. adatbázis-lekérdezések) vonatkozó kontrollintézkedések hiánya, amely hibás adatokhoz vezet. • Hibás külső adatok felhasználása.
	Az adatok rosszul ellenőrzött módosítása az	Az éles IKT-rendszerekben elvégzett adatmanipulációk helyességére és indokoltságára vonatkozó kontrollintézkedések hiánya miatt bekövetkező	• Fejlesztők vagy adatbázis-adminisztrátorok ellenőrizetlen módon, közvetlenül hozzáférnek az éles IKT-rendszerekben lévő adatokhoz, és

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
	éles IKT-rendszerekben.	adathibák.	módosítják azokat, pl. IKT-esemény bekövetkezésekor.
	Rosszul kialakított és/vagy kezelt adatarchitektúra, adatáramlások, adatmodellek vagy adatszótárak	A rosszul kezelt adatarchitektúrák, adatmodellek, adatáramlások vagy adatszótárak azt eredményezhetik, hogy ugyanazok az adatok többféle változatban fordulnak elő az IKT-rendszerekben, amelyek az eltérően alkalmazott adatmodellek vagy adatmeghatározások és/vagy a mögöttes adat-előállítási és -módosítási folyamat eltérései miatt már nem konzisztensek.	• Termékenként vagy üzletegységenként különböző ügyfél-adatbázisok megléte, amelyek különböző adatdefiníciókkal és -mezőkkel rendelkeznek, és ennek következtében hiányzik az ügyféladatok teljes pénzügyi intézmény vagy csoport szintjén való egyeztetése, vagy az ügyféladatok nehezen összehasonlíthatók és integrálhatók a teljes pénzügyi intézmény vagy csoport szintjén.
IKT kiszervezési kockázatok	A harmadik felek vagy a csoport más szervezetei által nyújtott szolgáltatások nem megfelelő rugalmassága	Kritikus kiszervezett IKT-szolgáltatások, távközlési szolgáltatások és közművek rendelkezésre állásának hiánya. Szolgáltatóra bízott kritikus/szenzitív adatok elvesztése vagy sérülése	• Alapvető szolgáltatások rendelkezésre állásának hiánya a szállítók (kiszervezett) IKT-rendszereiben vagy alkalmazásaiban fennálló hibák miatt. • Távközlési összeköttetések zavara. • Az áramellátás hiánya.
	A kiszervezés nem megfelelő irányítása	A szolgáltatások jelentős romlása vagy hibái a kiszervezett szolgáltató nem hatékony készültségi vagy kontrollfolyamatai miatt. A kiszervezés nem eredményes irányítása az IKT-kockázatok teljes körű azonosításához, értékeléséhez, mérsékléséhez és nyomon követéséhez szükséges megfelelő készségek és képességek hiányához vezethet, és korlátozhatja az intézmények működési kapacitásait.	• A szolgáltatói megállapodásba beépített gyenge eseménykezelési eljárások, szerződéses kontrollintézkedések és garanciák, amelyek növelik a harmadik felek és szolgáltatók kulcsemberektől való függőségét. • A szolgáltató IKT-környezetét érintő nem megfelelő változásirányítási kontrollintézkedések a szolgáltatás jelentős romlásához vagy hibájához vezethetnek.
	Nem megfelelő biztonság harmadik feleknél vagy a csoport másik	A harmadik fél szolgáltató IKT-rendszereinek hekkelése, amely közvetlenül kihat a kiszervezett szolgáltatásokra vagy a szolgáltatónál tárolt kritikus/bizalmas adatokra. A szolgáltató személyzete jogosulatlan hozzáférést szerez a szolgáltatónál tárolt kritikus/bizalmas	• A szolgáltatók bűnözők vagy terroristák általi meghekkelése, hogy be tudjanak lépni az intézmény IKT-rendszereibe, vagy hozzáférjenek a szolgáltatónál tárolt kritikus vagy bizalmas adatokhoz vagy megsemmisítsék azokat.

IKT-kockázati kategóriák	IKT-kockázatok (nem teljes körű[10])	Kockázatleírás	Példák
	szervezeténél	adatokhoz.	• A szolgáltató oldalán működő rosszindulatú bennfentesek érzékeny adatokat próbálnak meg ellopni és eladni.