EIOPA-BoS-20/600

Az információs és kommunikációs technológiák biztonságára és irányítására vonatkozó iránymutatások

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Németország - Tel. + 49 69-951119-20;
Fax: + 49 69-951119-19; email: info@eiopa.europa.eu honlap: www.eiopa.europa.eu

Tartalomjegyzék

Háttér

1. Az 1094/2010/EU rendelet 16. cikke alapján a következetes, hatékony és eredményes felügyeleti gyakorlatok létrehozása, és az uniós jog közös, egységes és következetes alkalmazásának biztosítása céljából az EIOPA iránymutatásokat és ajánlásokat bocsáthat ki.

2. Az említett rendelet 16. cikkének (3) bekezdésével összhangban az illetékes hatóságok és pénzügyi intézmények kötelesek minden erőfeszítést megtenni azért, hogy megfeleljenek az iránymutatásoknak és az ajánlásoknak.

3. Az EIOPA megállapította, hogy a 2009/138/EK irányelv 41. és 44. cikke kapcsán konkrét iránymutatást kell kialakítani az információs és kommunikációs technológiákkal kapcsolatos biztonság és irányítás tárgyában, az Európai Bizottság pénzügyi technológiai cselekvési tervére (COM(2018)0109 final) való válaszadás érdekében végzett elemzéssel és az EIOPA felügyeleti egységesítési tervével[1] összefüggésben, több más érdekelt féllel folytatott párbeszédet[2] követően.

4. Amint az az európai felügyeleti hatóságok Európai Bizottság felé tett közös állásfoglalásában szerepel, az irányítási rendszerről szóló EIOPA iránymutatások *„nem tükrözik megfelelően az IKT kockázatkezelés (a kiberkockázatokat is beleértve) kezelésének jelentőségét*". Nincs iránymutatás olyan létfontosságú körülményekre vonatkozóan, amely általánosan elismerten a megfelelő IKT biztonság és -irányítás részét képezik".

5. Az Unióban fennálló jelenlegi (jogalkotási) helyzet fent hivatkozott közös állásfoglalás céljából végzett elemzéséből kitűnik, hogy az EU-tagállamok többsége meghatározta az IKT biztonság és -irányítás nemzeti szabályait. Noha a követelmények hasonlóak, a szabályozási keret még mindig széttagolt. Ezenfelül a jelenlegi felügyeleti gyakorlatokkal kapcsolatos felmérés változatos gyakorlatokat tárt fel – a „nincs konkrét felügyelettől" az „erős felügyeletig (beleértve a „helyszínen kívüli ellenőrzéseket" és a „helyszíni ellenőrzéseket" is).

6. Ezenfelül fokozódik az IKT összetettsége és az IKT incidensek gyakorisága is (a kiberincidenseket is beleértve), továbbá az ilyen incidensek által az intézmények operatív működésére gyakorolt káros hatás is egyre erősebb. Éppen ezért az IKT és biztonsági kockázatkezelés alapvető fontosságú az intézmények számára stratégiai, vállalati, működési és hírnévvel kapcsolatos céljaik elérése érdekében.

7. Ezenfelül az egész biztosítási ágazatban, a hagyományos és az innovatív üzleti modelleket is beleértve, egyre inkább az IKT-ra támaszkodnak a biztosítási szolgáltatások nyújtása, valamint az intézmények operatív működése során; ennek példái közé tartozik a biztosítási ágazat digitalizációja (biztosítástechnológia, dolgok internete stb.), valamint a távközlési csatornák (internet, mobil és vezetéknélküli kapcsolatok, nagy kiterjedésű hálózatok) révén elért összekapcsoltság. Mindez sebezhetőbbé teszi az intézmények működését a kibertámadásokat is magukban foglaló biztonsági incidensekkel szemben. Ennélfogva fontos annak biztosítása, hogy az intézmények megfelelően felkészüljenek az őket érintő IKT és biztonsági kockázatok kezelésére.

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Az EIOPA által az Európai Bizottság pénzügyi technológiai cselekvési tervére válaszul közzétett jelentés itt érhető el.

8. Ezenfelül, elismerve, hogy szükség van az intézmények kiberkockázatokkal szembeni felkészültségére,[3] valamint arra, hogy stabil kiberbiztonsági keretrendszerrel rendelkezzenek, a jelen iránymutatások kiterjednek a kiberbiztonságra is, mint az intézmény információbiztonsági intézkedéseinek részére. Noha a jelen iránymutatások elismerik, hogy a kiberbiztonsággal az intézmény általános IKT és biztonságikockázat-kezelése részeként kellene foglalkozni, fontos kiemelni, hogy a kibertámadások sajátos jellemzőkkel rendelkeznek, amelyeket figyelembe kell venni annak biztosítása érdekében, hogy az információbiztonsági intézkedések megfelelően enyhítsék a kiberkockázatot:

   a) a kibertámadásokat gyakran nehezebb kezelni (vagyis nehezebb az azonosításuk, a velük szembeni védekezés, a felderítésük, az azokra való reagálás, valamint az azokból való helyreállás), mint a más forrásokból származó IKT és biztonsági kockázatokat, illetve nehéz a kár mértékének meghatározása is;

   b) egyes kibertámadások hatástalanná tehetik az általános kockázatkezelést és az üzletmenet-folytonosságát biztosító intézkedéseket, valamint a katasztrófahelyreállítási eljárásokat, mivel rosszindulatú szoftverekkel (malware) fertőzhetik meg a tartalékrendszereket, annak érdekében, hogy azokat elérhetetlenné tegyék vagy tönkretegyék a biztonsági mentéseket;

   c) a szolgáltatók, alkuszok, (vezető) ügynökök és közvetítők a kibertámadások terjedési csatornáivá válhatnak. Az észrevétlen fertőző fenyegetések arra használhatják fel a harmadik felek által biztosított távközlési kapcsolatok révén fennálló összekapcsoltságot, hogy bejussanak az intézmény IKT rendszerébe. Ennélfogva egy önmagában csekély hatású összekapcsolt intézmény sebezhetővé válhat és a kockázat továbbterjedésének forrásává válhat, ami rendszerszintű hatással járhat. A leggyengébb láncszem szabályát követve a kiberbiztonsággal nem csak a jelentős piaci szereplőknek vagy a kritikus szolgáltatások nyújtóinak kell foglalkozniuk.

9. A jelen iránymutatások célja a következő:

   a) egyértelmű tájékoztatás és átláthatóság biztosítása a piaci szereplők számára a minimális elvárt információkkal és kiberbiztonsági képességekkel, vagyis az alapvető védelmi szinttel kapcsolatban;

   b) az esetleges szabályozási arbitrázs elkerülése;

   c) a felügyeleti konvergencia elősegítése az IKT biztonsággal és -irányítással kapcsolatos elvárások és folyamatok tekintetében, ami kulcsfontosságú a megfelelő IKT és biztonsági kockázatkezeléshez.

[3] A kiberkockázat meghatározásához lásd: FSB Cyber Lexicon, 2018. november 12., https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Az információs és kommunikációs technológiák biztonságára és irányítására vonatkozó iránymutatások

Bevezetés

1. Az EIOPA az 1094/2010/EU rendelet[4] 16. cikkével összhangban kibocsátja a jelen iránymutatásokat a felügyeleti hatóságok számára azzal kapcsolatban, hogy a biztosítóknak és viszontbiztosítóknak (a továbbiakban együtt: intézmények) hogyan kell alkalmazniuk a 2009/138/EK irányelvben[5] (a továbbiakban: Szolvencia II irányelv) és az (EU) 2015/35 felhatalmazáson alapuló bizottsági rendeletben[6] (a továbbiakban: felhatalmazáson alapuló rendelet) rögzített irányítási követelményeket az információs és kommunikációs technológiákkal (IKT) kapcsolatos biztonsággal és irányítással összefüggésben. Ennek érdekében a jelen iránymutatások a Szolvencia II irányelv 41., 44., 46., 47., 132. és 246. cikkében, illetve a felhatalmazáson alapuló rendelet 258–260., 266., 268–271. és 274. cikkében rögzített irányítással kapcsolatos rendelkezésekre támaszkodnak. Ezenfelül a jelen iránymutatások az EIOPA irányítási rendszerre vonatkozó iránymutatásaira (EIOPA-BoS-14/253),[7] illetve az EIOPA felhőszolgáltatókhoz történő kiszervezésről szóló iránymutatásaira (EIOPA-BoS-19/270)[8] is támaszkodnak.

2. A jelen iránymutatások az egyedi intézmények és *mutatis mutandis* a csoportok szintjén is alkalmazandók.[9]

3. Az illetékes hatóságoknak, a jelen iránymutatásoknak való megfelelésük, illetve a megfelelés felügyeleti ellenőrzése során figyelembe kell venniük az arányosság elvét,[10] amelynek biztosítania kell, hogy az irányítási intézkedések, az IKT biztonsággal és irányítással kapcsolatos intézkedéseket is beleértve, arányban álljanak a vonatkozó kockázatok jellegével, mértékével és összetettségével, amelyekkel az intézmények szembesülnek vagy szembesülhetnek.

4. A jelen iránymutatásokat a Szolvencia II. irányelvvel, a felhatalmazáson alapuló rendelettel, az EIOPA irányítási rendszerre vonatkozó iránymutatásaival és az EIOPA felhőszolgáltatókhoz történő kiszervezésről szóló iránymutatásaival együttesen, azok sérelme nélkül kell értelmezni. A jelen iránymutatások technológia és módszertan semlegesek.

Fogalommeghatározások

5. A jelen iránymutatásokban meg nem határozott fogalmak a Szolvencia II. irányelvben meghatározott jelentéssel bírnak.

6. A jelen iránymutatások alkalmazásában a következő fogalmak az alábbi jelentéssel bírnak:

---

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

[5] Az Európai Parlament és a Tanács 2019/138/EK irányelve (2009. november 25.) a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról (Szolvencia II) (HL L 335., 2009.12.17., 1. o.)

[6] A Bizottság (EU) 2015/35 felhatalmazáson alapuló rendelete (2014. október 10.) a biztosítási és viszontbiztosítási üzleti tevékenység megkezdéséről és gyakorlásáról szóló 2009/138/EK európai parlamenti és tanácsi irányelv (Szolvencia II) kiegészítéséről (HL L 12., 2015.1.17., 1. o.).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] A 2009/138/EU irányelv 212. cikkének (1) bekezdése.

[10] A 2009/138/EU irányelv 29. cikkének (3) bekezdése.

Eszközgazda:	Az adott információ és IKT eszköz vonatkozásában elszámoltathatósággal és hatáskörrel rendelkező személy vagy szerv.
Rendelkezésre állás:	A felhatalmazott szervezet általi, igény szerinti hozzáférhetőség és felhasználhatóság (időszerűség) tulajdonsága.
Bizalmasság:	Az a tulajdonság, hogy az információt nem teszik hozzáférhetővé illetéktelen személyek, szervezetek, folyamatok vagy rendszerek számára, velük azt nem közlik.
Kibertámadás:	A betörés (hacking) minden típusa, amelynek eredményeként az IKT rendszerekre irányulóan támadó jellegű / rosszindulatú kísérlet történik valamely információs eszköz megsemmisítésére, felfedésére, módosítására, hatástalanítására, eltulajdonítására, az ahhoz való jogosulatlan hozzáférésre, illetve jogosulatlan használatára.
Kiberbiztonság:	Az információk és/vagy az informatikai rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése a kibertérben.
IKT eszköz:	Az üzleti környezetben megtalálható szoftver- vagy hardvereszköz.
IKT projektek:	Minden olyan projekt vagy annak egy része, amely keretében IKT rendszereket és szolgáltatásokat módosítanak, cserélnek le, vagy vezetnek be.
IKT és biztonsági kockázat:	A működési kockázat része; a bizalmasság sérüléséből, a rendszerek és adatok sértetlenségének elvesztéséből, a rendszerek és adatok nem megfelelőségéből vagy elérhetetlenségéből, illetve a környezet vagy az üzleti követelmények változása esetén az IKT ésszerű időn és költségek mellett történő megváltoztatására (más néven rugalmasság) való képtelenségből adódó veszteség kockázata. Ide tartoznak a nem megfelelő vagy rosszul működő belső folyamatokból vagy külső eseményekből eredő kiberkockázatok és információbiztonsági kockázatok, beleértve a kibertámadásokat vagy a nem megfelelő fizikai biztonságot is.

Információbiztonság	Az információk és/vagy az informatikai rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése a kibertérben. Emellett további olyan tulajdonságok, mint a hitelesség, elszámoltathatóság, letagadhatatlanság és a megbízhatóság is érintettek lehetnek.
IKT szolgáltatások:	Az IKT rendszereken és szolgáltatókon keresztül egy vagy több belső vagy külső felhasználónak nyújtott szolgáltatások.
IKT rendszerek:	Alkalmazások, szolgáltatások, információtechnológiai eszközök, IKT eszközök vagy más információkezelési elemek halmaza, melyek a működési környezetben megtalálhatók.
Információs eszköz:	Kézzelfogható vagy nem kézzelfogható információk összessége, amelyek megvédése érdemes.
Sértetlenség:	A pontosságot és teljességet jelölő tulajdonság.
Működési vagy biztonsági incidens:	Egyetlen esemény vagy egymáshoz kapcsolódó események olyan sorozata, amelynek negatív hatása van vagy valószínűleg negatív hatást gyakorol az IKT rendszerek és szolgáltatások sértetlenségére, rendelkezésre állására, bizalmasságára.
Szolgáltató:	Olyan harmadik fél szervezet, amely kiszervezési megállapodás alapján végez valamely kiszervezett folyamatot, szolgáltatást vagy tevékenységet, illetve annak egy részét.
Fenyegetésalapú behatolási tesztelés:	Ellenőrzött kísérlet a szervezet kibertámadásokkal szembeni ellenállóképességének kijátszására, a valódi fenyegetést jelentő szereplők taktikáinak, technikáinak és eljárásainak utánzása révén. Ez célzott fenyegetés-elemzésen alapul és az adott szervezetnél tevékenykedő emberekre, a szervezet folyamataira és technológiáira irányul, minimális előzetes ismeret, illetve a működésre gyakorolt minimális hatás mellett.
Sérülékenység:	Valamely eszköz vagy ellenőrzés gyengesége, érzékenysége vagy hibája, amelyet egy vagy több fenyegetés képes kihasználni.

7. Ezek az iránymutatások 2021. július 1-jétől alkalmazandók.

1. iránymutatás – Arányosság

8. Az intézményeknek a jelen iránymutatásokat oly módon kell alkalmazniuk, amely igazodik az üzleti tevékenységükben rejlő kockázatok jellegéhez, nagyságrendjéhez és összetettségéhez.

2. iránymutatás – IKT az irányítási rendszerben

9. Az igazgatási, irányító vagy felügyelő testületnek biztosítania kell, hogy az intézmény irányítási rendszere, különösen a kockázatkezelési és a belső ellenőrzési rendszer megfelelően kezelje az intézményt érintő IKT és biztonsági kockázatokat.

10. Az igazgatási, irányító vagy felügyelő testületnek biztosítania kell, hogy az intézmény személyzetének létszáma és szakértelme megfelelő legyen az IKT-val kapcsolatos működési szükségleteihez, valamint az IKT és biztonsági kockázatkezelési folyamatainak folyamatos támogatásához, továbbá az IKT stratégiája megvalósításának biztosításához. Ezenfelül a személyzet számára rendszeresen megfelelő képzést kell biztosítani az IKT és biztonsági kockázatokkal kapcsolatban, a 13. iránymutatásnak megfelelően.

11. Az igazgatási, irányító vagy felügyelő testületnek biztosítania kell, hogy az előirányzott források megfelelőek legyenek a fenti követelmények eléréséhez.

3. iránymutatás – IKT stratégia

12. Az igazgatási, irányító vagy felügyelő testület viseli az általános felelősséget azért, hogy az átfogó üzleti stratégia részeként és azzal összhangban kialakítsa és jóváhagyja az intézmények írásba foglalt IKT stratégiáját, valamint felügyelje annak kommunikálását és végrehajtását.

13. Az IKT stratégiában meg kell határozni legalább a következőket:

    a) az intézmény IKT-ja hogyan fejlődjön, annak érdekében, hogy hatékonyan támogassa és megvalósítsa az üzleti stratégiát, beleértve a szervezeti felépítés, az üzleti modellek, az IKT rendszer és a szolgáltatókkal kapcsolatos fő függőségek fejlesztését;

    b) az IKT architektúra fejlesztését, a szolgáltatókkal kapcsolatos függőségeket is beleértve;

    c) az IKT rendszerekre és szolgáltatásokra, továbbá az alkalmazottakra és a folyamatokra irányuló, világos információbiztonsági célkitűzéseket.

14. Az intézményeknek biztosítaniuk kell az IKT stratégia megvalósítását és elfogadását, valamint azt, hogy azt kellő időben közlik minden érintett dolgozóval és szolgáltatóval.

15. Az intézményeknek folyamatot kell kidolgozniuk az IKT stratégia megvalósítási hatékonyságának nyomon követésére és mérésére. E folyamatot rendszeresen felül kell vizsgálni, valamint frissíteni kell.

4. iránymutatás – IKT és biztonsági kockázatok a kockázatkezelési rendszeren belül

16. Az igazgatási, irányító vagy felügyelő testület viseli az általános felelősséget az IKT és biztonsági kockázatok kezelését biztosító hatékony rendszer kialakításáért, az intézmény általános kockázatkezelési rendszerének részeként. Ez magában foglalja az ezen kockázatokra vonatkozó kockázatvállalási hajlandóság meghatározását, az intézmény írásba foglalt kockázati stratégiájával összhangban, valamint a

rendszeres írásbeli jelentéstételt az igazgatási, irányító vagy felügyelő testület részére a kockázatkezelési folyamat eredményéről.

17. Általános kockázatkezelési rendszerük részeként az intézményeknek az IKT és biztonsági kockázatok kapcsán (a lent ismertetett IKT védelmi követelmények meghatározása során) legalább az alábbiakat mérlegelniük kell:

    a) az intézményeknek fel kell térképezniük üzleti folyamataikat és tevékenységeiket, üzleti feladatköreiket, szerepeiket és eszközeiket (például az információs eszközöket és az IKT eszközöket), valamint rendszeresen frissíteniük kell e feltérképezést, annak érdekében, hogy azonosítsák a fentiek fontosságát és az IKT és biztonsági kockázatokkal fennálló kölcsönös függőségeiket;

    b) az intézményeknek azonosítaniuk kell, illetve fel kell mérniük minden őket érintő releváns IKT és biztonsági kockázatot, továbbá kritikusságuk szempontjából be kell sorolniuk az azonosított üzleti folyamatokat és tevékenységeket, üzleti feladatköröket, szerepeket és eszközöket (például az információs eszközöket és az IKT eszközöket). Az intézményeknek emellett értékelniük kell legalább az ezen üzleti folyamatok és tevékenységek, üzleti feladatkörök, szerepek és eszközök (például az információs eszközök és az IKT eszközök) bizalmasságára, sértetlenségére és rendelkezésre állására vonatkozó védelmi követelményeket. Azonosítani kell az eszközök besorolásáért felelős eszközgazdákat;

    c) a kritikusság, valamint az elvárt védelmi szint meghatározásához használt módszereknek, különös figyelemmel a sértetlenség, a rendelkezésre állás és a bizalmasság védelmi célokra, biztosítaniuk kell, hogy a fentiekből következő védelmi követelmények következetesek és teljes körűek legyenek;

    d) az IKT és biztonsági kockázatok felmérését a meghatározott IKT és biztonsági kockázati kritériumok alapján kell elvégezni, amelyek figyelembe veszik az intézmény üzleti folyamatai és tevékenységei, üzleti feladatkörei, szerepei és eszközei (például az információs eszközök és az IKT eszközök) kritikusságát, az ismert sérülékenységek mértékét, valamint az intézményt érintő korábbi incidenseket;

    e) el kell végezni az IKT és biztonsági kockázatok értékelését, továbbá dokumentálni kell azt. Az értékelést az infrastruktúra, a folyamatok vagy eljárások olyan jelentős változásait megelőzően is el kell végezni, amelyek érintik az üzleti folyamatokat és tevékenységeket, az üzleti feladatköröket, szerepeket és eszközöket (például az információs eszközöket és az IKT eszközöket).

    f) kockázatértékeléseik alapján az intézményeknek legalább meg kell határozniuk és végre kell hajtaniuk az azonosított IKT és biztonsági kockázatok kezelésére és az információs eszközök – besorolásuknak megfelelő – védelmére irányuló intézkedéseket. Ennek magában kell foglalnia a fennmaradó maradványkockázatokat kezelő intézkedések meghatározását.

18. Az IKT és biztonsági kockázatkezelési folyamat eredményeit jóvá kell hagynia az igazgatási, irányító vagy felügyelő testületnek, és azokat be kell építeni az intézmény működési kockázatkezelési folyamatába, az általános kockázatkezelési rendszerének részeként.

5. iránymutatás – Ellenőrzés

19. Az intézmények IKT és biztonsági kockázatokkal kapcsolatos irányítását, rendszereit és eljárásait az intézmény ellenőrzési tervével összhangban[11] az IKT és biztonsági kockázatok területén megfelelő ismeretekkel, készségekkel és szakértelemmel rendelkező ellenőröknek kell rendszeresen ellenőrizniük, annak érdekében, hogy független bizonyosságot nyújtsanak azok hatékonyságáról az igazgatási, irányító vagy felügyelő testület számára. Az ilyen ellenőrzések gyakoriságának és hatókörének arányban kell állnia a vonatkozó IKT és biztonsági kockázatokkal.

6. iránymutatás – Információbiztonsági politika és intézkedések

20. Az intézményeknek az igazgatási, irányító vagy felügyelő testület által jóváhagyott, írásba foglalt információbiztonsági politikát kell kialakítaniuk, amelyben meghatározzák az intézmény információi bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét célzó magas szintű elveket és szabályokat, az IKT stratégia végrehajtásának támogatása érdekében.

21. A politikának tartalmaznia kell az információbiztonsági irányítás legfontosabb szerepköreinek és felelősségi köreinek a leírását, és meg kell határoznia az információbiztonsággal kapcsolatban az alkalmazottakkal, az eljárásokkal és a technológiával szemben támasztott követelményeket, felismerve, hogy az alkalmazottak minden szinten felelősek az intézmények információbiztonságának biztosításáért.

22. E politikát az intézményen belül közzé kell tenni és azt a személyzet valamennyi tagjára alkalmazni kell. Adott esetben, amennyiben releváns, az információbiztonsági politikát vagy annak egyes részeit a szolgáltatókkal is közölni kell és alkalmazni kell rájuk.

23. A politika alapján az intézményeknek konkrétabb információbiztonsági eljárásokat és információbiztonsági intézkedéseket kell kialakítaniuk, illetve végrehajtaniuk, többek között az őket érintő IKT és biztonsági kockázatok enyhítése céljából. Ezeknek az eljárásoknak és információbiztonsági intézkedéseknek adott esetben a jelen iránymutatásokban ismertetett valamennyi folyamatot tartalmazniuk kell.

7. iránymutatás – Információbiztonsági feladatkör

24. Az intézményeknek irányítási rendszerükben, az arányosság elvének megfelelően, információbiztonsági feladatkört kell kialakítaniuk, a felelősségi körök kijelölt személyre telepítésével. Az intézménynek biztosítania kell az információbiztonsági feladatkör függetlenségét és objektivitását azáltal, hogy megfelelően elkülönítik azt az IKT fejlesztéstől és az üzemeltetési folyamatoktól. A feladatkör az igazgatási, irányító vagy felügyelő testületnek jelentsen.

25. Rendszerint a következők tartoznak az információbiztonsági feladatkör feladatai közé:

    a) az igazgatási, irányító vagy felügyelő testület támogatása az intézmények információbiztonsági politikájának meghatározása és fenntartása során, valamint a politika bevezetésének ellenőrzése;

[11] A felhatalmazáson alapuló rendelet 271. cikke.

b) rendszeres és eseti jelentéstétel, valamint tanácsadás az igazgatási, irányító vagy felügyelő testület részére az információbiztonság helyzetéről és annak alakulásáról;

c) az információbiztonsági intézkedések végrehajtásának nyomon követése és felülvizsgálata;

d) az információbiztonsági követelmények betartatásának biztosítása a szolgáltatók igénybe vétele során;

e) annak biztosítása, hogy az információkhoz és rendszerekhez hozzáférő valamennyi munkavállalót és szolgáltatót megfelelően tájékoztassanak az információbiztonsági politikáról, például információbiztonsági képzés és biztonságtudatossági események révén;

f) a működési vagy a biztonsági incidensekkel kapcsolatos vizsgálatok koordinálása, és a releváns esetek jelentése az igazgatási, irányító vagy felügyelő testület felé.

8. iránymutatás – Logikai biztonság

26. Az intézményeknek a védelmi követelményekkel összhangban meg kell meghatározniuk, dokumentálniuk kell és végre kell hajtaniuk a logikai hozzáférési kontrollok vagy a logikai biztonság (azonosítás és hozzáférés-kezelés) eljárásait, a 4. iránymutatásban meghatározottaknak megfelelően. Ezeket az eljárásokat be kell vezetni és be kell tartatni, nyomon kell követni, rendszeresen felül kell vizsgálni, valamint a rendellenességek nyomon követésére is kontrollokat kell tartalmazniuk. Ezeknek az eljárásoknak legalább a következő követelményeket 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: az intézményeknek az információs eszközökhöz és az azokat támogató rendszerekhez való hozzáféréseket (a távoli hozzáférést is beleértve) a „szükséges ismeret” elve alapján kell kezelniük. A felhasználók számára minimális hozzáférési jogokat kell biztosítani, amelyek szigorúan szükségesek a feladataik teljesítéséhez (a „legkisebb jogosultság” elve), vagyis, hogy megakadályozzák az adatokhoz való indokolatlan hozzáférést, illetve megakadályozzák a hozzáférési jogok olyan kombinációinak kiosztását, melyek a kontrollok megkerülésére használhatók (a „feladatok elkülönítésének” elve).

b) felhasználói elszámoltathatóság: az intézményeknek a lehető legnagyobb mértékben korlátozniuk kell az általános és a megosztott felhasználói fiókok használatát, valamint biztosítaniuk kell, hogy a felhasználók azonosíthatók és az IKT rendszerekben végzett tevékenységekért felelős természetes személyhez vagy engedélyezett feladathoz köthetők legyenek;

c) kiemelt hozzáférési jogok: az 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).

d) távoli hozzáférés: a biztonságos kommunikáció biztosítása és a kockázat csökkentése érdekében a kritikus IKT rendszerekhez távoli rendszergazdai hozzáférést csak a szükséges ismeret elve alapján szabad biztosítani, és csak erős azonosítási megoldások alkalmazása mellett;

e) a felhasználói tevékenységek naplózása: a felhasználói tevékenységeket a kockázatokkal arányos módon naplózni kell és nyomon kell követni, beleértve legalább a kiemelt felhasználói tevékenységeket. Biztosítani kell a hozzáférési naplók védelmét az illetéktelen módosítások vagy törlések ellen, és meg kell őrizni azokat a meghatározott üzleti feladatkörök, támogató folyamatok és információs eszközök kritikusságának megfelelően, az uniós és nemzeti jogszabályban előírt megőrzési követelmények sérelme nélkül. Az intézményeknek ezt az információt fel kell használniuk a szolgáltatások nyújtása során azonosított rendellenes tevékenységek felmérésére és kivizsgálására.

f) hozzáférés-kezelés: a hozzáférési jogokat kellő időben kell megadni, visszavonni és módosítani, az előzetesen meghatározott jóváhagyási munkafolyamatoknak megfelelően, amelyekbe be kell vonni a hozzáféréssel érintett információs eszköz gazdáját. Amennyiben a hozzáférésre már nincs szükség, a hozzáférési jogokat haladéktalanul vissza kell vonni;

g) hozzáférések felülvizsgálata: a hozzáférési jogokat rendszeres időközönként felül kell vizsgálni annak biztosítása érdekében, hogy a felhasználók ne rendelkezzenek túlzott jogosultságokkal, és hogy a hozzáférési jogokat visszavonják/megszüntessék, amikor azokra már nincs szükség.

h) a hozzáférési jogok megadását, módosítását és visszavonását olyan módon kell dokumentálni, amely megkönnyíti azok megértését és elemzését; továbbá

i) azonosítási módszerek: az intézményeknek hatásos azonosítási módszereket kell hatályba léptetniük, amelyek megfelelően és hatékonyan biztosítsák a hozzáférési szabályok 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 erős jelszavakat vagy erősebb azonosítási módszereket (mint a kétfaktoros azonosítást) tartalmaznia kell.

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

9. iránymutatás – Fizikai biztonság

28. Az intézményeknek fizikai biztonsági intézkedéseket (pl. áramkimaradással, tűzesettel, vízkárral és engedély nélküli fizikai hozzáféréssel szembeni védelem) kell meghatározniuk, dokumentálniuk és megvalósítaniuk, hogy megvédjék telephelyüket, adatközpontjaikat és érzékeny területeiket az engedély nélküli hozzáféréssel és környezeti fenyegetésekkel szemben.

29. Az IKT rendszerekhez való fizikai hozzáférést csak a feljogosított személyek számára szabad lehetővé tenni. A feljogosítást a személyek feladataival és felelősségi köreivel összhangban, valamint a megfelelően képzett és ellenőrzött személyekre korlátozva kell kiosztani. A fizikai hozzáférést rendszeresen felül kell vizsgálni annak biztosítása érdekében, hogy a felesleges hozzáférési jogokat haladéktalanul visszavonják/megszüntessék.

30. A környezeti veszélyekkel szembeni védelmet szolgáló megfelelő intézkedéseknek arányosnak kell lenniük az épületek fontosságával és a működés vagy az érintett épületekben található IKT rendszerek kritikusságával.

10. iránymutatás – IKT üzemeltetés biztonsága

31. Az intézményeknek eljárásokat kell kialakítaniuk az IKT rendszerek és az IKT szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében, hogy minimalizálják a biztonsági problémáknak az IKT szolgáltatások nyújtására gyakorolt hatását. Ezeknek az eljárásoknak a következő intézkedésekre kell megfelelően kiterjedniük:

    a) a lehetséges sérülékenységek azonosítására, amelyeket ki kell értékelni és javítani kell az IKT rendszerek naprakész állapotának biztosításával, ideértve az intézmények által a belső és külső felhasználóik számára biztosított szoftvert, a kritikus biztonsági javítások – a vírusdefiníciós állományokat is beleértve – telepítésével vagy kompenzáló kontrollok bevezetésével;

    b) az összes kritikus eszköz, mint az operációs rendszerek, adatbázisok, routerek, illetve switch-ek biztonságos alapkonfigurációinak bevezetésére;

    c) hálózati szegmentálás és adatszivárgás-megelőző rendszerek bevezetésére és a hálózati forgalom titkosítására (az információs eszközök osztályozásának megfelelően);

    d) a végpontok (beleértve a szervereket, munkaállomásokat és mobil eszközöket) védelmének megvalósítására. Az intézményeknek meg kell vizsgálniuk, hogy a végpont megfelel-e az általuk meghatározott biztonsági követelményeknek, mielőtt azok hozzáférést kapnak a vállalati hálózathoz;

    e) az IKT rendszerek sértetlenségét ellenőrző mechanizmusok bevezetésére;

    f) az adatok titkosítására tárolás és továbbítás során (az információs eszköz osztályozásának megfelelően).

11. iránymutatás – Biztonsági monitorozás

32. Az intézményeknek eljárásokat és folyamatokat kell kialakítaniuk, valamint bevezetniük, hogy folyamatosan monitorozzák az intézmények információbiztonságára ható tevékenységeket. A monitorozásnak legalább a következőkre kell kiterjednie:

    a) belső és külső tényezőkre, beleértve az üzleti és IKT rendszergazdai feladatköröket;

    b) a szolgáltatók, más szervezetek és belső felhasználók tranzakcióira; valamint

    c) a potenciális belső és külső fenyegetésekre.

33. A monitorozás alapján az intézményeknek megfelelő és hatékony képességeket kell kialakítaniuk, hogy felismerjék, jelentsék és kezeljék a rendellenes tevékenységeket és fenyegetéseket, mint a fizikai vagy logikai behatolás, az információs eszközök bizalmasságának, sértetlenségének és rendelkezésre állásának megsértései, a rosszindulatú kódok, valamint a szoftverek és hardverek közismert sérülékenységei.

34. A biztonsági monitorozási jelentéseknek segíteniük kell az intézményeket a működési és a biztonsági incidensek természetének megértésében, a tendenciák azonosításában, valamint támogatniuk kell az intézmények belső vizsgálatait, és lehetővé kell tenniük számukra a megfelelő döntések meghozatalát.

12. iránymutatás – Információbiztonsági vizsgálatok, értékelés és tesztelés

35. Az intézményeknek különféle információbiztonsági vizsgálatokat, értékeléseket és teszteket kell elvégezniük az IKT rendszereik és IKT szolgáltatásaik sérülékenységeinek hatékony azonosítása érdekében. Az intézmények végezhetnek például eltéréselemzést információbiztonsági szabványok, megfelelőségi vizsgálatok, információs rendszerek belső és külső ellenőrzése, vagy fizikai biztonsági vizsgálatok alapján.

36. Az intézményeknek ki kell dolgozniuk és be kell vezetniük egy információbiztonsági tesztelési keretrendszert, amely ellenőrzi az információbiztonsági intézkedések megbízhatóságát és hatékonyságát, továbbá biztosítaniuk kell, hogy ez a keretrendszer figyelembe veszi azon fenyegetéseket és sérülékenységeket, melyeket a fenyegetés-monitorozási, valamint az IKT és biztonsági kockázatértékelési folyamat azonosít.

37. A tesztelést biztonságos és védett módon kell végrehajtani, független tesztelők által, akik megfelelő tudással, készségekkel és szakértelemmel rendelkeznek a biztonsági intézkedések tesztelése terén.

38. Az intézményeknek rendszeresen el kell végezniük a teszteket. A tesztelés hatókörének, gyakoriságának és módszerének (például behatolási tesztelés, a fenyegetésalapú behatolási tesztelést is beleértve) arányban kell állnia az azonosított kockázati szinttel. A kritikus IKT rendszerek tesztelését, valamint a sérülékenységi vizsgálatokat évente el kell végezni.

39. Az 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 miatti változtatások, illetve új vagy jelentősen módosított kritikus alkalmazások üzembe állítása kapcsán. Az 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.

13. iránymutatás – Információbiztonsági oktatás és tudatosítás

40. Az intézményeknek információbiztonsági képzési programokat kell kialakítaniuk a személyzet valamennyi tagja (az igazgatási, irányító vagy felügyelő testületet is beleértve) számára, mely biztosítja az emberi hiba, a lopás, a csalás, a visszaélés és a veszteség csökkentése érdekében ellátandó feladataikhoz és felelősségeikhez szükséges képzést. Az intézményeknek biztosítaniuk kell, hogy a képzési program rendszeres képzést biztosít a személyzet valamennyi tagja számára.

41. Az intézményeknek rendszeres biztonságtudatossági programokat kell kialakítaniuk és végrehajtaniuk személyzetük (az igazgatási, irányító vagy felügyelő testületet is beleértve) oktatására, hogy miként kezeljék az információbiztonsággal kapcsolatos kockázatokat.

14. iránymutatás – IKT üzemeltetés

42. Az intézményeknek az IKT stratégia alapján kell irányítaniuk az IKT üzemeltetésüket. Írott dokumentumokban kell meghatározni, hogy az intézmények miként üzemeltetik, monitorozzák és ellenőrzik az IKT rendszereket és az IKT szolgáltatásokat, beleértve a kritikus IKT folyamatok, eljárások és üzemeltetés dokumentálását is.

43. Az intézményeknek naplózási és monitorozási eljárásokat kell működtetniük a kritikus IKT üzemeltetési tevékenységekre vonatkozóan, hogy lehetővé tegyék a hibák felderítését, elemzését és javítását.

44. Az intézményeknek naprakész nyilvántartást kell vezetniük IKT eszközeikről. Az IKT eszközök nyilvántartásának kellően részletesnek kell lennie ahhoz, hogy lehetővé tegye az IKT eszköz azonnali azonosítását, valamint elhelyezkedésének, biztonsági besorolásának és tulajdonjogának meghatározását.

45. Az intézményeknek nyomon kell követniük és kezelniük kell az IKT eszközök életciklusát annak biztosítása érdekében, hogy azok folyamatosan megfeleljenek az üzleti és kockázatkezelési követelményeknek, illetve támogassák azokat. Az intézményeknek nyomon kell követniük, hogy IKT eszközeik támogatása biztosított-e szállítóik vagy belső fejlesztőik által, és hogy minden releváns javítás és frissítés telepítésre került-e dokumentált folyamat alapján. Fel kell mérni és mérsékelni kell az elavult vagy nem támogatott IKT eszközökből eredő kockázatokat. A működésből kivont IKT eszközöket biztonságosan kell kezelni és megsemmisíteni.

46. Az intézményeknek teljesítmény- és kapacitástervezési, továbbá monitorozási folyamatokat kell bevezetniük annak érdekében, hogy megelőzzék és felderítsék az IKT rendszerek jelentős teljesítményproblémáit és az IKT kapacitáshiányokat, illetve azokra időben reagáljanak.

47. Az intézményeknek meg kell határozniuk és működtetniük kell az adatok és IKT rendszerek biztonsági mentési és helyreállítási eljárásait annak biztosítása érdekében, hogy azok szükség szerint helyreállíthatóak legyenek. A biztonsági mentések körét és gyakoriságát az üzleti helyreállítási követelményekkel, valamint az adatok és IKT rendszerek kritikusságával összhangban kell meghatározni, az elvégzett kockázatértékelésnek megfelelően. A biztonsági mentési és helyreállítási eljárások tesztelését rendszeresen el kell végezni.

48. Az intézményeknek biztosítaniuk kell, hogy az adatok és az IKT rendszerek biztonsági mentéseit az elsődleges helyszíntől eltérő, biztonságos helyen vagy helyeken tárolják, amely(ek) kellően messze található(k) az elsődleges helyszíntől ahhoz, hogy ne legyen(ek) kitéve ugyanazon kockázatoknak.

15. iránymutatás – IKT incidensek és problémák kezelése

49. Az intézményeknek incidens- és problémakezelési folyamatot kell kidolgozniuk és bevezetniük a működési és a biztonsági incidensek nyomon követése és naplózása céljából, valamint annak lehetővé tétele érdekében, hogy zavarok esetén az intézmények folytathassák vagy újrakezdhessék kritikus üzleti feladatköreiket és folyamataikat.

50. Az intézményeknek megfelelő kritériumokat és küszöbértékeket kell meghatározniuk arra vonatkozóan, hogy milyen eseményt minősítenek működési vagy biztonsági incidensnek, továbbá riasztásként szolgáló korai előrejelző mutatókat kell meghatározniuk, amelyek lehetővé teszik ezen incidensek korai észlelését.

51. A nemkívánatos események hatásának minimalizálása, illetve az időben történő helyreállítás lehetővé tétele céljából az intézményeknek megfelelő folyamatokat és szervezeti felépítést kell kialakítaniuk a működési és biztonsági incidensek következetes és integrált monitorozásának, kezelésének és nyomon követésének biztosítására, annak érdekében, hogy azonosítsák és kezeljék a kiváltó okokat, és javító tevékenységek/intézkedések révén megakadályozzák az incidens

megismétlődését. Az incidens- és problémakezelési folyamatnak meg kell határoznia legalább a következőket:

a) az incidensek azonosítását, nyomon követését, naplózását, kategorizálását és az intézmény által meghatározott prioritások szerinti osztályozását, mely az üzleti kritikusságon és a szolgáltatási megállapodásokon alapul;

b) különféle incidens forgatókönyvekre (pl. hibák, hibás működés, kibertámadások) vonatkozó szerepeket és felelősségi köröket;

c) problémakezelési eljárást az incidens(ek) gyökérokainak azonosítására, elemzésére és megoldására – az intézménynek elemeznie kell a szervezeten belül és/vagy azon kívül azonosított vagy bekövetkező működési vagy biztonsági incidenseket, figyelembe kell vennie az ezen elemzésekből levont legfontosabb tapasztalatokat, és ennek megfelelően frissítenie kell a biztonsági intézkedéseket;

d) hatékony belső kommunikációs terveket, ideértve az incidensekre vonatkozó értesítési és eszkalációs eljárásokat – a biztonsággal kapcsolatos ügyfélpanaszokra is kiterjedően – annak biztosítása érdekében, hogy

   i. a kritikus IKT rendszerekre és IKT szolgáltatásokra potenciálisan jelentős káros hatást gyakorló incidenseket jelentsék az érintett felső vezetésnek;

   ii. az igazgatási, irányító vagy felügyelő testületet eseti alapon tájékoztassák a jelentős incidensekről, továbbá tájékoztassák legalább az incidensek hatásairól, az azokra való reagálásról és az incidensek folytán meghatározandó kiegészítő ellenőrzésekről.

e) incidenskezelési eljárásokat az incidensek hatásának mérséklésére, valamint a szolgáltatásnak időben működőképessé és biztonságossá tétele érdekében;

f) konkrét külső kommunikációs terveket a kritikus üzleti feladatkörökre és folyamatokra vonatkozóan annak érdekében, hogy:

   i. együttműködjenek a megfelelő érdekelt felekkel az incidensre való hatékony reagálás és abból való helyreállás céljából;

   ii. szükség esetén időben tájékoztassák a külső feleket (például ügyfeleket, más piaci szereplőket, felügyeleti hatóságokat), az incidensjelentéseket is beleértve, a vonatkozó szabályozásnak megfelelően.

16. iránymutatás – IKT projektmenedzsment

52. Az intézményeknek IKT projektmódszertant kell bevezetniük (a független biztonsági követelményekre is kiterjedően), megfelelő irányítási folyamattal és projekt-vezetéssel, annak érdekében, hogy az IKT projektek hatékonyan támogassák az IKT stratégia megvalósítását.

53. Az intézményeknek megfelelően nyomon kell követniük és mérsékelniük kell az IKT projektportfólióból eredő kockázatokat, figyelembe véve azokat a kockázatokat is, amelyek a különféle projektek közötti kölcsönös függőségekből, valamint több projekt ugyanazon erőforrásoktól és/vagy szakértelemtől való függéséből fakadhatnak.

17. iránymutatás – IKT rendszerek beszerzése és fejlesztése

54. Az intézményeknek ki kell alakítaniuk és be kell vezetniük az IKT rendszerek beszerzését, fejlesztését és karbantartását szabályozó folyamatot, a feldolgozandó

adatok bizalmasságának, sértetlenségének és rendelkezésre állásának átfogó biztosítása céljából, valamint annak érdekében, hogy a meghatározott védelmi követelmények teljesüljenek. Ezt a folyamatot kockázatalapú megközelítéssel kell megtervezni.

55. Az intézményeknek gondoskodniuk kell arról, hogy a rendszerek beszerzését vagy a fejlesztői tevékenységek elvégzését megelőzően egyértelműen meghatározzák a funkcionális és a nem funkcionális követelményeket (az információbiztonsági követelményeket is beleértve), valamint a technikai célokat.

56. Az intézményeknek gondoskodniuk kell olyan intézkedésekről, amelyek megakadályozzák az IKT rendszerek véletlen módosítását vagy szándékos manipulációját a fejlesztés során.

57. Az intézményeknek rendelkezniük kell olyan módszerekkel, amelyek segítségével tesztelik és jóváhagyják az IKT rendszereket, az IKT szolgáltatásokat és az információbiztonsági intézkedéseket.

58. Az intézményeknek megfelelően tesztelniük kell az IKT rendszereket, az IKT szolgáltatásokat és az információbiztonsági intézkedéseket a lehetséges biztonsági hiányosságok, szabálysértések, valamint incidensek azonosítása érdekében.

59. Az intézményeknek biztosítaniuk kell az éles üzemi környezet elkülönítését a fejlesztési, tesztelési és más, nem üzemi környezetektől.

60. Az intézményeknek intézkedéseket kell bevezetniük az IKT rendszerek forráskódja (ha rendelkezésre áll) sértetlenségének védelmére. Továbbá teljeskörűen dokumentálniuk kell az IKT rendszerek fejlesztését, bevezetését, működését és/vagy konfigurálását annak érdekében, hogy csökkentsék a téma szakértőitől való indokolatlan függést.

61. Az intézmények IKT rendszerek beszerzésére és fejlesztésére vonatkozó folyamatait alkalmazni kell az IKT szervezeten kívüli üzleti feladatkörök végfelhasználói által fejlesztett vagy kezelt IKT rendszerekre is (például az üzleti területek által kezelt alkalmazások vagy végfelhasználói számítástechnikai alkalmazások), kockázatalapú megközelítést alkalmazva. Az intézményeknek nyilvántartást kell vezetniük az ilyen alkalmazásokról, amelyek a kritikus üzleti feladatköröket vagy folyamatokat támogatnak.

18. iránymutatás – IKT változáskezelés

62. Az intézményeknek ki kell dolgozniuk és be kell vezetniük egy IKT változáskezelési folyamatot annak biztosítására, hogy az IKT rendszerekben bekövetkezett összes változást ellenőrzött módon rögzítsék, értékeljék, teszteljék, hagyják jóvá, engedélyezzék és hajtsák végre. A sürgős vagy vészhelyzeti IKT változások során történő változásoknak nyomon követhetőknek kell lenniük, és azokat utólagos ellenőrzés céljából utólag be kell jelenteni a megfelelő eszközgazdának.

63. Az intézményeknek meg kell határozniuk, hogy a meglévő működési környezetben végrehajtott változtatások kihatnak-e a meglévő biztonsági intézkedésekre, vagy szükségessé teszik-e kiegészítő intézkedések megvalósítását a felmerülő kockázatok mérséklése érdekében. Ezeknek a változásoknak meg kell felelniük az intézmények formális változáskezelési folyamatának.

19. iránymutatás – Üzletmenet-folytonosság kezelése

64. Az intézmények átfogó üzletmenet-folytonossági szabályzatának részeként az igazgatási, irányító vagy felügyelő testület felel az intézmény IKT folytonossági

szabályzatának kialakításáért és jóváhagyásáért. Az IKT folytonossági szabályzatot az intézményeken belül megfelelően közzé kell tenni és azt a személyzet minden érintett tagjára, illetve adott esetben a szolgáltatókra is alkalmazni kell.

20. iránymutatás – Üzleti-hatáselemzés

65. A gondos üzletmenet-folytonosság menedzsment részeként az intézményeknek üzleti-hatáselemzést kell végezniük az üzletmenet súlyos fennakadásának való kitettségük elemzésével és lehetséges hatásainak mennyiségi és minőségi értékelésével, belső és/vagy külső adatok, valamint forgatókönyv-elemzés felhasználásával. Az üzleti-hatáselemzés során a 4. iránymutatásnak megfelelően mérlegelni kell az azonosított és besorolt üzleti folyamatok és tevékenységek, üzleti feladatkörök, szerepek és eszközök (pl. információs eszközök és IKT eszközök) kritikusságát, valamint kölcsönös függőségeiket.

66. Az intézményeknek biztosítaniuk kell, hogy IKT rendszereiket és IKT szolgáltatásaikat az üzleti-hatáselemzéssel összhangban tervezzék meg, illetve azzal összehangolják, például bizonyos kritikus elemek redundanciájának biztosításával az ezen összetevőket érintő események által okozott fennakadások megakadályozása érdekében.

21. iránymutatás – Az üzletmenet-folytonosság tervezése

67. Az intézmények átfogó üzletmenet-folytonossági terveinek figyelembe kell venniük azokat a lényeges kockázatokat, amelyek hátrányos hatást gyakorolhatnak az IKT rendszerekre és az IKT szolgáltatásokra. A terveknek támogatniuk kell azokat a célkitűzéseket, melyek az intézmény üzleti folyamatai és tevékenységei, üzleti feladatkörei, szerepei és eszközei (pl. információs eszközök és IKT eszközök) bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére és szükség esetén helyreállítására irányulnak. Az intézményeknek e tervek kidolgozása során szükség szerint egyeztetniük kell az érintett belső és külső érdekelt felekkel.

68. Az intézmények üzletmenet-folytonossági terveket kell érvénybe léptetniük annak érdekében, hogy megfelelően tudjanak reagálni a lehetséges meghibásodási forgatókönyvekre a helyreállítási idő célkitűzésen (RTO, az a maximális időtartam, amelynek során valamely rendszert vagy folyamatot helyre kell állítani az incidenst követően) és a helyreállítási pont célkitűzésen (az a maximális időtartam, amelynek során incidens esetén előre meghatározott szolgáltatási szint mellett adatok veszhetnek el) belül.

69. Az intézményeknek üzletmenet-folytonossági terveikben számos különböző forgatókönyvet kell mérlegelniük, beleértve a szélsőséges, de valószerű forgatókönyveket, illetve a kibertámadásokkal kapcsolatos forgatókönyveket is, és értékelniük kell az ilyen forgatókönyvek lehetséges hatását. Ezen forgatókönyvek alapján az intézményeknek rögzíteniük kell, hogy miként biztosítják az IKT rendszerek és szolgáltatások folytonosságát, valamint az intézmény információbiztonságát.

22. iránymutatás – Katasztrófaelhárítási és helyreállítási tervek

70. Az üzleti-hatáselemzés és a valószínűsíthető forgatókönyvek alapján az intézményeknek katasztrófaelhárítási és helyreállítási terveket kell kidolgozniuk. Ezekben a tervekben meg kell határozni azokat a feltételeket, amelyek kiválthatják a terv aktiválását, és azokat az intézkedéseket, amelyeket végre kell hajtani az intézményeknek legalább a kritikus IKT rendszerek, IKT szolgáltatások és adatok sértetlenségének, rendelkezésre állásának, folytonosságának és helyreállításának

biztosítása érdekében. A katasztrófaelhárítási és helyreállítási terveknek törekedniük kell arra, hogy teljesítsék az intézmények működésére vonatkozó helyreállítási célkitűzéseket.

71. A katasztrófaelhárítási és helyreállítási terveknek rövid és szükség esetén hosszú távú helyreállítási lehetőségeket egyaránt figyelembe kell venniük. A terveknek meg kell felelniük legalább az alábbiaknak:

    a) a fontos IKT szolgáltatások, üzleti feladatkörök, támogató folyamatok, információs eszközök működésének és ezek kölcsönös függőségeinek helyreállítására irányulnak, az intézmény működésére gyakorolt hátrányos hatások elkerülése érdekében;

    b) dokumentáltak és az üzleti és támogató egységek rendelkezésére állnak, továbbá vészhelyzet esetén azonnal hozzáférhetők, beleértve a szerepek és felelősségek egyértelmű meghatározását is; valamint

    c) folyamatosan frissítésre kerülnek az incidensekből, tesztekből levont tanulságokkal, az újonnan felismert kockázatokkal és fenyegetésekkel, valamint a megváltozott helyreállítási célokkal és prioritásokkal.

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

73. A katasztrófaelhárítási és helyreállítási tervek részeként az intézményeknek meg kell fontolniuk folytonossági intézkedések megvalósítását az intézmények IKT szolgáltatásainak folytonossága szempontjából kulcsfontosságú szolgáltatók zavarai esetére (az EIOPA irányítási rendszerre vonatkozó iránymutatásainak és a felhőszolgáltatókhoz történő kiszervezésről szóló iránymutatásainak megfelelően).

23. iránymutatás – A tervek tesztelése

74. Az intézményeknek tesztelniük kell üzletmenet-folytonosság terveiket, továbbá biztosítaniuk kell, hogy rendszeresen tesztelik kritikus üzleti folyamataik és tevékenységeik, üzleti feladatköreik, szerepeik és eszközeik (pl. információs eszközök), továbbá IKT eszközeik működését, valamint ezek kölcsönös függőségeit (a szolgáltatók által biztosítottakat is beleértve) az intézmény kockázati profilja alapján.

75. Az üzletmenet-folytonossági terveket rendszeresen aktualizálni kell a tesztelés eredményei, a fenyegetésekkel kapcsolatos aktuális információk és a korábbi eseményekből levont tapasztalatok alapján. A helyreállítási célokat (a helyreállítási idő-célkitűzést és a helyreállítási pont-célkitűzést is beleértve) érintő releváns változásokat és/vagy az üzleti folyamatokat és tevékenységeket, üzleti feladatköröket, szerepeket és eszközöket (pl. információs eszközök és IKT eszközök) érintő változásokat szintén be kell építeni.

76. Az üzletmenet-folytonossági tervek tesztelésével igazolni kell, hogy azok alkalmasak az intézmény életképességének fenntartására a kritikus működés előzetesen meghatározott szolgáltatási szinten történő vagy tolerált mértékű hatás szerinti helyreállításáig.

77. A teszteredményeket dokumentálni kell, a tesztek eredményeként feltárt hiányosságokat elemezni és kezelni kell, továbbá azokról jelentést kell készíteni az igazgatási, irányító vagy felügyelő testületnek.

24. iránymutatás – Válságkommunikáció

78. Fennakadás vagy vészhelyzet esetén és az üzletmenet-folytonossági tervek végrehajtása során az intézményeknek gondoskodniuk kell arról, hogy hatékony válságkommunikációs intézkedéseket léptessenek életbe, hogy minden érintett belső és külső érdekelt fél – beleértve az illetékes hatóságokat, ha a nemzeti jogszabályok ezt megkövetelik, valamint az érintett szolgáltatókat – időben és megfelelő módon tájékoztatást kapjon.

25. iránymutatás – Az IKT szolgáltatások és az IKT rendszerek kiszervezése

79. Az EIOPA felhőszolgáltatókhoz történő kiszervezésről szóló iránymutatásait nem sértve az intézmények kötelesek biztosítani, hogy az IKT szolgáltatások és az IKT rendszerek kiszervezése esetén is teljesüljenek az IKT szolgáltatásokra és az IKT rendszerekre vonatkozó követelmények.

80. A kritikus vagy fontos feladatkörök kiszervezése esetén az intézményeknek gondoskodniuk kell arról, hogy a szolgáltató szerződéses kötelezettségei (pl. szerződés, szolgáltatási szint megállapodások, megszüntetési rendelkezések a megfelelő szerződésekben) tartalmazzák legalább az alábbiakat:

    a) megfelelő és arányos információbiztonsági célkitűzések és intézkedések, olyan követelményeket is beleértve, mint a minimális információbiztonsági követelmények, az intézmények adatainak életciklusára vonatkozó specifikációk, ellenőrzési és hozzáférési jogok, továbbá az adatközpontok elhelyezkedésével, az adatok titkosításával, a hálózatbiztonsággal és a biztonsági monitorozási folyamatokkal kapcsolatos követelmények;

    b) szolgáltatási szint megállapodások, az IKT szolgáltatások és az IKT rendszerek folytonosságának biztosítása érdekében, valamint a rendes körülmények között elvárt, illetve a szolgáltatás fennakadása esetén alkalmazandó folytonossági tervekben meghatározott teljesítménycélok; valamint

    c) működési és biztonsági incidensek kezelési eljárásai, beleértve az eszkalációt és a jelentéstételt.

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

A megfelelésre és a jelentéstételre vonatkozó szabályok

82. Az e dokumentumban szereplő iránymutatásokat az 1094/2010/EU rendelet 16. cikke alapján adták ki. Az említett rendelet 16. cikkének (3) bekezdésével összhangban az illetékes hatóságok és az intézmények kötelesek minden erőfeszítést megtenni azért, hogy megfeleljenek az iránymutatásoknak és az ajánlásoknak.

83. Azoknak az illetékes hatóságoknak, amelyek megfelelnek vagy meg kívánnak felelni ezen iránymutatásoknak, megfelelő módon át kell ültetniük ezeket a szabályozási vagy felügyeleti rendjükbe.

84. Az illetékes hatóságoknak a lefordított változatok közzétételét követő két hónapon belül vissza kell igazolniuk az EIOPA felé, hogy megfelelnek-e, illetve meg kívánnak-e felelni ezen iránymutatásoknak, megjelölve a meg nem felelés indokait is.

85. Ha e határidőn belül nem érkezik válasz, azt úgy kell tekinteni, hogy az illetékes hatóság nem felel meg a jelentéstételi kötelezettségnek, és a jelentésben így kell szerepeltetni.

Felülvizsgálatra vonatkozó záró rendelkezések

86. A jelen iránymutatásokat az EIOPA felülvizsgálhatja.