A Magyar Nemzeti Bank
1/2015. számú ajánlása

az informatikai rendszer védelméről

(kiadás ideje: 2015.02.25.)

TARTALOM

Bevezetés

A saját- és a rájuk bízott ügyfél vagyon, valamint az ügyfél adatok védelmének a biztosítására a pénzügyi szervezeteknek fokozottan kell gondoskodniuk a tevékenységükhöz használt informatikai rendszerük védelméről. Az egyes pénzügyi tevékenységek végzésére, valamint a pénzügyi szervezetekre vonatkozó ágazati jogszabályok[1] vonatkozó szakaszai a pénzügyi szervezeteket erre különböző módon és mértékben, jogilag is kötelezik.

Jelen dokumentum célja, hogy a pénzügyi szervezetek számára gyakorlati útmutatást adjon az informatikai rendszerük védelmének a jogszabályi kötelezettségek szerint a kockázatokkal arányos szinten történő kiépítéséhez, amelynek alapja a pénzügyi szervezet releváns informatikai kockázatainak a feltárása, valamint azok megfelelő módon történő kezelése.

Mivel az egyes pénzügyi szervezetek eltérő mérete, üzleti jellege és valós működése különböző biztonsági kockázatot jelent, továbbá az informatikai- és telekommunikációs technológia rohamos fejlődése miatt nem lehetséges „örök érvényű", és a pénzügyi szervezetekre egységesen javasolható biztonsági kontrollokat meghatározni, ezért jelen dokumentum az informatikai biztonsági kontrollok kialakítása szempontjából szakmai vezetői útmutatónak tekintendő.

Az anyagban csak az 535/2013 Kormány rendelet, a Bszt., Mpt., Öpt. és a Bit. vonatkozó szakaszaiban előírtakra hivatkozunk tételesen, de a leírtak az informatikai témakört más struktúrában megjelenítő Kbftv. és Tpt. hatálya alá tartozó szervezetek, illetve tevékenységek esetében is érvényesek.

Az ajánlásban a felsorolt jogszabályok hatálya alá tartozó szervezetekre egységesen „pénzügyi szervezet" néven hivatkozunk.

Jelen dokumentum a felügyeleti vizsgálati tapasztalatok és az informatikai biztonságnak az ajánlásnak a kiadása idején közismert és általánosan elvárható követelményei szerint készült, és a PSZÁF azonos című **1/2013 számú módszertani útmutatójának a helyébe lép**. Felhívjuk a figyelmet az informatikai rendszer védelméhez kapcsolódóan korábban kiadott, az internetbanki szolgáltatások biztonságáról szóló MNB ajánlásra, valamint a közösségi és publikus felhőszolgáltatás igénybevételéből eredő kockázatokról szóló MNB vezetői körlevélre, ezek figyelembe vételét szintén szükségesnek tartjuk a biztonságos informatikai rendszerek kialakítása és üzemeltetése során.

A dokumentum a törvényi előírásokban szereplő védelmi területek szerint fókuszál, ezekhez fűz útmutatásokat és sorolja fel az előremutató gyakorlatokat. Ennek megfelelően eltér a jogszabályokban szereplő sorrendtől, szó szerinti szövegrészek szerepeltetése helyett az előírásokból kiemeli, esetenként összevonja a védelmi területeken felmerülő kockázatok kezelésére vonatkozó követelményeket, és azokhoz kapcsolódóan adja meg a vonatkozó jogszabályi helyekre való hivatkozásokat.

A jogszabályok lehetővé teszik, hogy a pénzügyi szervezetek az informatikai tevékenységet csak részben lássák el saját maguk, annak egy részét vagy egészét kiszervezhetik. Az ajánlás a kiszervezés informatikai biztonsági vonatkozásaira is kitér, annak fenntartása mellett, hogy a kiszervezett tevékenységek végzéséért minden esetben a megbízó pénzügyi szervezet a felelős.

---

[1] 535/2013 Korm. rendelet a pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről (Korm.r.) 1.§, 2.§, 3.§, 4.§, 5.§
2007. évi CXXXVIII. törvény a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról (Bszt.) 12.§
1997. évi LXXXII. törvény a magánnyugdíjról és a magánnyugdíj pénztárakról (Mpt) 77/A.§
1993. évi XCVI. törvény az Önkéntes Kölcsönös biztosító pénztárakról (Öpt.) 40/C.§
2003. évi LX. törvény a biztosítókról és a biztosítási tevékenységről (Bit.)
2014. évi XVI. törvény (Kbftv.)
2001. évi CXX. törvény a tőkepiacról (Tpt.)

Az ajánlás tanulmányozását és használatát a pénzügyi szervezetek vezetőinek, az üzleti működési kockázatok kezeléséért felelős vezetőknek, és az informatikai- és informatikai biztonsági szakembereknek egyaránt javasoljuk.

1 Az informatikai biztonsági szabályozás és a szabályzati rendszer

A pénzügyi szervezeteknek ki kell alakítaniuk a szolgáltatási tevékenységük ellátásához használt informatikai rendszerük biztonságával kapcsolatos szabályozási rendszerüket, és a szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, valamint a használatból adódó biztonsági kockázatok felmérésére és kezelésére ***az informatikai vállalatirányítás,*** *a tervezés, a* ***fejlesztés és*** *beszerzés, az üzemeltetés és* ***a monitorozás és független*** *ellenőrzés területén.*[2]

Az informatikai és adatkommunikációs rendszerek védelmének meghatározó alapeleme a rendszerek működésére és a működtetésre vonatkozó szabályozás. Ez a követendő szabályok bevezetését, betartását, ellenőrzését, valamint az ellenőrzések során feltárt hiányosságok megszüntetését, azaz együttesen az informatika szabályozását jelenti.

Az informatikai szabályozás alapeleme az informatikai biztonsági szabályzati rendszer. Annak ellenére, hogy szabályozás megvalósításának nem minden esetben feltétele a dokumentáltság, a pénzügyi szervezetek szigorú szabályozási fogalmához illeszkedően informatikai biztonsági szabályzati rendszeren jelen ajánlásban minden esetben dokumentált szabályzati rendszert értünk, és javasoljuk, hogy a szabályzati rendszer kialakítása az alábbiak figyelembe vételével történjen:

1.1 Az informatikai biztonsági szabályzati rendszer célja, a kialakítás alapelvei

Az informatikai biztonsági szabályzati rendszer célja, hogy elvárások meghatározásán keresztül csökkentse a hibás emberi tevékenység végzésből, az információ hiányából és az elvégzett tevékenységek dokumentálásának elmaradásából származó, informatikai jellegű működési kockázatokat. A szabályzati rendszer a pénzügyi szervezetek informatikai biztonságának egyik közvetett kockázat csökkentő kontrollja: megléte és folyamatos megfelelősége a teljesítés számonkérésének alapjául szolgál.

Céljaival összhangban, a szabályzati rendszer az alábbi dokumentum körökből tevődhet össze:

- informatikai szabályzatok: az emberi munkavégzést előíró dokumentumok – konkrét elnevezésüktől függetlenül, pl. üzemeltetési utasítások, mentési előírások, üzletmenet folytonossági eljárások, cselekvési tervek, tevékenységi listák stb.
- műszaki- és nyilvántartási dokumentumok: pl. hálózati diagramok, eszköznyilvántartások, mentési eljárások, parancs állományok, logikai hozzáférési rendek, stb.
- elvégzett tevékenységek dokumentumai, a továbbiakban feljegyzések: pl. jegyzőkönyvek, emlékeztetők, beszámolók, elkészített terv dokumentumok, az informatikai tárgyú vizsgálatok dokumentumai, stb.

A pénzügyi szervezet számára bizonyos szabályzati dokumentumok elkészítését a vonatkozó törvények kötelezően előírják. Ezek képezik a szabályzati rendszer alapját – és az ajánlás későbbi részében ismertetésre kerülnek -, ezeken túlmenően a pénzügyi szervezet maga dönthet arról, hogy mely további szabályozások elkészítését tartja szükségesnek. Döntésük meghozatala során a pénzügyi szervezeteknek figyelemmel kell lenniük arra, hogy a szabályzati rendszerük illeszkedjen a pénzügyi tevékenységük jellegéhez, legyen arányos annak a nagyságrendjével és összetettségével, és álljon összhangban az informatikai rendszer kockázatokkal arányos védelmét biztosító eszközrendszerrel.

Az informatikai biztonsági szabályzati rendszer dokumentumainak formátumát a pénzügyi szervezet az ésszerűség szem előtt tartása mellett – pl. a tartalomhoz igazodva - szabadon választhatja meg,

[2] Bit. 65/A.§ (1), Bszt.12.§ (1) (2), Mpt.77/A.§ (1), Öpt.40/C.§ (1), Korm.r.2.§ (1)

valamint saját hatáskörben dönthet arról, hogy alkalmaz-e dokumentum hierarchiát, illetve milyen belső eljárást alkalmaz a szabályzati rendszer elkészítésére, illetve bevezetésére.

Az informatikai biztonsági szabályzati rendszer előírásainak – szándékos vagy vétlen - figyelmen kívül hagyása, valamint a bármilyen okból betarthatatlan előírások, nem naprakész műszaki- és nyilvántartási dokumentumok jelentős működési kockázatot jelentenek a pénzügyi szervezet informatikai működésében.

1.2 Kiszervezett tevékenységek szabályozása

A szabályzati rendszer kialakításának törvényi kötelezettségét nem befolyásolja, ha a pénzügyi szervezet informatikai tevékenységének egészét vagy részeit kiszervezi. A kiszervezett tevékenységi területekre vonatkozó szabályzati dokumentumok elkészítése a pénzügyi szervezet és a kiszervezett tevékenységet végző megállapodásától függően általában - de nem feltétlenül - a kiszervezett tevékenységet végző feladata.

A kiszervezett tevékenység szerződésben foglaltaknak megfelelő végzését a Hpt[3]., Öpt., és az Mpt. hatálya alá tartozó pénzügyi szervezetek esetében a szervezetek belső ellenőrzése évente ellenőrizni köteles.[4] Ennek keretében a belső ellenőr vizsgálhatja a kiszervezett tevékenységet végző e tevékenységre vonatkozó belső szabályzatait is.

1.3 A szabályzati rendszer kialakításának javasolt gyakorlati szempontjai

1.3.1 A pénzügyi szervezet belső szabályzatban rögzíti informatikai biztonsági szabályzati rendszeréről legalább az alábbiakat:

a) a hatályos szabályzati rendszer elemeinek tételes felsorolása - informatikai szabályzatok, műszaki- nyilvántartási dokumentumok, valamint a feljegyzések köre,

b) az informatikai biztonsági szabályzati rendszer elemeinek nyilvántartási módja, tárolási helye, ezen felül informatikai szabályzatok esetében a hatályon kívül helyezett szabályzatok nyilvántartási módja és tárolási helye,

c) nyilvántartásonként a nyilvántartásra kijelölt adatok felsorolása,

d) az egyes informatikai szabályzati rendszer elemek felelősei, a szerepköröknek illetve munkaköröknek a megnevezése, amelyek betöltői az adott szabályzati dokumentum tartalmi megfelelőségért és teljességért, továbbá aktuális állapotukért felelősek,

e) az informatikai szabályzatok személyi és tárgyi hatálya, hatályba léptetésének a dátuma,

f) az informatikai szabályzatok közzétételének módja és eljárása, a hatályos verziók elérési módja, a kiadás- és a változáskezelés módja,

g) az informatikai biztonsági szabályzati rendszer, kötelező formai elemei.

1.3.2 Tevékenységek szabályozására a pénzügyi szervezet az elvégzendő tevékenységek részletes műveleteit írja elő, ezek helyett irányelvek és normák előírására csak azokban az esetben kerüljön sor, amikor a részletes szabályozás nem lehetséges (pl. titoktartási kötelezettség).

1.3.3 A pénzügyi szervezet a szabályzati rendszerét olyan mélységig dolgozza ki, hogy:

[3] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Hpt.)

[4] Hpt.68.§ (6), Mpt. 77/B.§ (5), Öpt.40/D.§ (5). Az ellenőrzés során külső megbízott szakértő is igénybe vehető.

a) az informatikai szabályzatok részletezettsége, a műszaki- és nyilvántartási dokumentumok és a feljegyzések adattartalma informatikus- vagy informatikai szolgáltató kiesése esetén is lehetővé teszi az informatikai rendszer folyamatos üzemét, valamint az esetleges kieséseket követő újraindítását,

b) a szabályozás a pénzügyi szervezet az elvégzendő tevékenységek részletes műveleteit írja elő, és ennek a részletezettsége olyan mélységű, hogy a szabályozott tevékenységet egy, az adott szakterületen jártas informatikus a szabályzati rendszer alapján el tudja végezni,

c) egy független informatikai vizsgálat meggyőződhessen a tevékenység tartalmának a megfelelőségéről, és ellenőrizhesse, hogy a tevékenységet a pénzügyi szervezet megfelelően látja-e el.

1.3.4 A pénzügyi szervezet szabályzati dokumentumai

a) egyértelmű, világos, könnyen érthető formában vannak megfogalmazva,

b) lényegre törően tömörek, és az érintettek számára csak releváns előírásokat tartalmaznak. A nem informatikus munkatársak részére az alapvető informatikai biztonsági ismeretek és biztonsági feladataik – pl. teendők vírusgyanús esetekben, jelszóváltoztatás gyakorisága, eljárása stb. - önálló dolgozói biztonsági szabályzatban vannak összefoglalva, ezen felül az egyes informatikai szakterületekre vonatkozó előírásokat szakterületenként területi szabályozás tartalmazza,

c) az aláírásokhoz kapcsolódóan minden esetben feltüntetik, hogy az adott aláírás mit igazol – pl. a leírtakat végrehajtotta, ellenőrizte, átvette, megismerte, tudomásul vette, stb.

1.3.5 A pénzügyi szervezet és a kiszervezett tevékenységet végzők a kiszervezési tevékenységek végzésére vonatkozó szerződésükben vagy ahhoz kapcsolódóan rögzítik a kiszervezett tevékenység végzője által minimálisan elkészítendő szabályzati dokumentumokat, és ezeket a pénzügyi szervezet – a szerződésben foglaltaknak megfelelő teljesítés ellenőrzésének a keretében – vizsgálhatja.

1.3.6 A pénzügyi szervezet biztosítja szabályzati rendszerének mindenkori érvényességét és aktuális állapotát, ennek érdekében azt minden változással egyidejűleg aktualizálja, és ezen felül a teljes szabályzati rendszerét legalább kétévente felülvizsgálja, és ennek elvégzését dokumentálja.

1.3.7 A pénzügyi szervezet szabályzati rendszerében előírja az informatikai rendszere biztonsági kockázatainak rendszeres időközönként történő kötelező felmérését, kijelöli a kockázatok felmérésének felelősét, és meghatározza a felmérés elvégzésének és az azt követő tevékenységek elvégzésének az alapvető lényeges szabályait.

2 Az informatikai kockázatelemzés és az informatikai rendszer kockázatokkal arányos védelme

A pénzügyi szervezeteknek gondoskodniuk kell informatikai rendszerük kockázatokkal arányos védelméről. Ehhez kötelesek az informatikai rendszerük biztonsági kockázatelemzését elkészíteni - és szükség szerint, de legalább kétévente felülvizsgálni és aktualizálni, valamint a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítani.[5]

[5] Bit.65/A.§ (2) (6), Bszt.12.§ (3) (7), Mpt.77/A.§ (2) (6), Öpt.40/C.§ (2) (6), Korm.r. 2.§ (2) 3.§ (3)

A vonatkozó törvényi előírások az informatikai biztonsági kontrollok egy halmazának kötelező alkalmazását írják elő, a kockázatarányos védelem kialakításához azonban szükséges, hogy a pénzügyi szervezet az informatikai kockázatait és az alkalmazható biztonsági kontrollokat az informatikai és adatkommunikációs technológia mindenkori szintjére figyelemmel egy teljes körűen végrehajtott kockázatelemzés során megvizsgálja, valamint a feltárt kockázatokat megfelelően kezelje.

Az informatikai rendszerek biztonsági kockázatelemzésének elvégzéséhez és a kockázatarányos védelem biztosításához a Felügyelet az alábbi szempontokat javasolja megfontolni:

2.1 Az informatikai biztonsági kockázatelemzés célja

Az informatikai kockázatelemzés közvetett biztonsági kontroll, azaz elvégzése önmagában nem erősíti a védelmet, de elvégzése szükséges ahhoz, illetve eredménye teszi lehetővé, hogy a pénzügyi szervezet a tevékenysége jellegének, nagyságrendjének és összetettségének megfelelő, kockázataival arányos biztonságos informatikai rendszert alakíthasson ki. Az informatikai kockázatelemzés célja ennek megfelelően az, hogy meghatározza az informatikai rendszer biztonsági hiányosságait, azaz feltárja, és kockázati alapon értékelje annak hiányzó, továbbá a bevezetett, de nem kielégítően működő, informatikai biztonsági kontrolljait.

Az informatikai biztonsági kontrollok egy csoportjának kötelező, illetve kockázatokkal arányosan kötelező alkalmazását a vonatkozó törvények előírják. A kockázatokkal arányos informatikai biztonság kialakításához azonban nélkülözhetetlen, hogy sor kerüljön a pénzügyi szervezetek specifikus informatikai biztonsági hiányosságainak – pl. architektúra, fizikai biztonság - a feltárására is, amely a kockázatelemzésnek szintén részét képezi.

2.2 Az informatikai biztonsági kockázatelemzés minősítése

A vonatkozó törvények a kockázatelemzés elvégzésének módját – módszerét, eljárását - nem írják elő, erről a pénzügyi szervezet szabadon dönthet. A Felügyelet a pénzügyi szervezet kockázatelemzését annak végeredménye alapján minősíti, és a kötelezően elkészítendő kockázatelemzési jelentés alapján azt vizsgálja és értékeli, hogy a pénzügyi szervezet a kockázataival arányos módon és az informatikai biztonsággal érintett valamennyi területen – tervezés, beszerzés, üzemeltetés, ellenőrzés – az elvárható gondosság mellett teljes körűen tárta-e fel és értékelte az informatikai rendszerének az informatikai biztonsági hiányosságait.

2.3 A kockázatelemzés javasolt folyamata

A kockázatelemzés során alkalmazott módtól – módszertől, eljárástól – függetlenül a pénzügyi szervezet a kockázatelemzés során elvégzi az alábbi lépéseket:

a) az üzleti folyamatok meghatározása, ezen belül az adatok felmérése és minősítése, a folyamatok kockázati besorolásának elvégzése az adatok bizalmassága, sértetlensége és rendelkezésre állása, a folyamatok sértetlensége és rendelkezésre állási követelményei alapján,
b) az üzletileg kritikus, fő folyamatok azonosítása és kockázatelemzésre történő kiválasztása,
c) a kiválasztott folyamatok informatikai működését biztosító informatikai és adatkommunikációs rendszerelemek, valamint a folyamatok informatikai biztonsági szempontú gyenge pontjainak - pl. kézi adatbeviteli- és módosítási lehetőségek, rendszerek közötti adatátadások, távoli hozzáférések, technikai felhasználói

azonosítók, megosztott adatterületek, átmeneti adatállományok, szoftver sérülékenységek, stb. - azonosítása,

d) a rendszerelemekhez, valamint a gyenge pontokhoz kapcsolódó informatikai biztonsági kontrollok meglétére és működésük megfelelőségére vonatkozó vizsgálatok elvégzésével a biztonsági hiányosságok és elégtelenségek azonosítása és a kockázatok értékelése,

e) az általános informatikai biztonsági kontrollok - a rendszer elemekhez közvetlenül nem kapcsolódó biztonsági kontrollok, mint pl. az emberi erőforrás, a szabályozás, az infrastruktúra területek biztonsági intézkedései - vizsgálata és értékelése, ennek során a vonatkozó törvényekben közvetlen módon nem előírt informatikai biztonsági kontrollok azonosítását és a kockázatok értékelését a „legjobb gyakorlatok" alapján javasolt elvégezni,

f) a szabályzati előírások és a gyakorlat összhangjának a vizsgálata,

g) végezetül a pénzügyi szervezet kritikus informatikai környezetére vonatkozó informatikai biztonsági helyzetkép kialakítása, és a kockázatelemzési jelentés dokumentum elkészítése.

A kockázatelemzési tevékenységek elvégzése során a pénzügyi szervezet az alábbiak szerint jár el:

a) A kockázatelemzés a) és b) lépésében informatikai, informatikai biztonsági, valamint a pénzügyi szervezet üzleti működését és annak fő folyamatait naprakészen ismerő pénzintézeti szakemberek együtt vesznek részt.

b) A kockázatelemzés c), d) és e) lépését olyan szakemberek végzik, akik az informatikai biztonsági kontrollokat, valamint ezek alkalmazásának a „legjobb gyakorlatát" napi szinten ismerik. Számos nemzetközi ajánlás tartalmaz informatikai biztonsági kontroll katalógusokat, amelyek a vizsgálat elvégzése során felhasználhatók – pl. COBIT5, MSZ ISO/IEC 27001:2006, BSI IT-Grundschutz-Kataloge, stb. Ezekben a katalógusokban a pénzügyi szervezetekre vonatkozó követelmények is megtalálhatók, az ajánlás *I. Melléklete* bemutatja az egyes jogszabályi kontroll követelményekkel érintett COBIT, illetve MSZ ISO/IEC 27001:2006 fejezeteket.

c) A pénzügyi szervezet a kockázatelemzési jelentésben a vizsgált folyamatokat, rendszerelemeket, a feltárt gyenge pontokat, a vizsgálat alá vont biztonsági intézkedéseket, biztonsági intézkedésenként a megállapítást és a kockázat mértékét, valamint a vizsgálat szempontjából releváns egyéb körülményeket teljes körűen dokumentálja. A dokumentum így lehetővé teszi visszaellenőrzések elvégzését, rögzíti a vizsgálat hatókörét, így kiinduló pontja lehet a következő időszak kockázatelemzésének.

d) A kockázatok feltárását követően, az esetleges téves megállapítások feltárására, eltérő kockázati értékelések egyeztetésére a kockázatelemzést végző és a vizsgált terület között egyeztetésre kerül sor.

e) Mivel a kockázatelemzési jelentés a kockázatkezelés döntés előkészítő dokumentuma is egyben, ezért a kockázatelemzési jelentés a feltárt kockázatok mértékét a legjellemzőbb lehetséges káresemény és a negatív üzleti hatás - a pénzügyi szervezetet fenyegető legjellemzőbb üzleti kár - bemutatásával érzékelteti. Az üzleti kockázatok összehasonlítását a jelentés a biztonsági hiányosságokhoz rendelt kockázati skála használatával végzi el.

f) A kockázatelemzést a pénzügyi szervezet felső vezetése tárgyalja és hagyja jóvá.

2.4 A feltárt kockázatok kezelése

A pénzügyi szervezetnek az informatikai rendszer kockázatokkal arányos védelméhez a biztonsági kockázatelemzés alapján indokolt védelmi kontrollokat meg kell valósítania.

Függetlenül attól, hogy a kockázatelemzését saját maga készíti, vagy külső partnerrel készítteti, a pénzügyi szervezet viseli a felelősséget mind a kockázatelemzés során fel nem tárt, mind a feltárt, de nem megszüntetett kockázatokért.

A kockázatok kezelésének javasolt lépései

2.4.1 A biztonsági hiányosságok megszüntetésére a pénzügyi szervezet a kockázatelemzés befejezését követően intézkedési feladatokat dolgoz ki, és megállapítja a feladatok erőforrás igényeit.

2.4.2 A pénzügyi szervezet a feladatok végrehajtását ütemezi, amelynek során figyelembe veszi az erőforrás igényt, a kockázati értéket, kijelöli a felelősöket, majd dokumentált intézkedési tervet készít.

2.4.3 Az intézkedési terv – teljes vagy részleges – végrehajtását a pénzügyi szervezet erre kijelölt vezetője illetve vezetői testülete jóváhagyja, és a döntését dokumentálja. A döntés igazolja, hogy a vezetőség a kockázatelemzés eredményét megismerte, és a feltárt, de az intézkedési tervben nem szereplő kockázatokat felvállalja.

2.4.4 Az intézkedési feladatok végrehajtását a pénzügyi szervezet kijelölt felelős(ök) útján nyomon követi, ellenőrzi, és amennyiben a végrehajtás a feladattervtől eltér, korrekciós intézkedéseket hoz a feladat határidőre és a tervezett módon történő befejezésére.

2.5 A kockázatelemzés felülvizsgálata

A pénzügyi szervezetnek az informatikai rendszerét érintő változások esetében, a változással érintett területekre vonatkozóan, de legalább kétévente az informatikai biztonságát érintő valamennyi területen, el kell végeznie a biztonsági kockázatok elemzését. A kötelező kockázatelemzés elvégezhető rendszeres – belső és/vagy külső – informatikai ellenőrzések sorozatával is, amennyiben a pénzügyi szervezet biztosítja, hogy kétéves ciklusban az informatikai rendszer egésze vizsgálat alá kerüljön, a megállapításaik dokumentálva legyenek, valamint a felső vezetés azokat megismerje és elfogadja.

2.6 A kockázatelemzés elvégzése kiszervezett tevékenységek esetében

Amennyiben a pénzügyi szervezet az informatikai tevékenységének egészét vagy részeit kiszervezi, a kockázatelemzés hatóköre és tartalma kiegészül a kiszervezésnek a pénzügyi szervezetre jelentett kockázatainak a vizsgálatával. Ezen túlmenően a pénzügyi szervezetek számára az alábbiakat javasoljuk:

2.6.1 A pénzügyi szervezet és a kiszervezett tevékenységet végzők a szerződésükben vagy ahhoz kapcsolódóan rögzítik a tevékenységet végző informatikai biztonsági feladatait és felelősségét, ezen belül rögzítik a kiszervezett tevékenységekre vonatkozó kockázatelemzés elvégzésének feladatát, valamint meghatározzák annak a hatókörét.

2.6.2 A pénzügyi szervezet a kiszervezett tevékenységre vonatkozó kockázatelemzés megtörténtét – a szerződésben foglaltaknak megfelelő teljesítés ellenőrzésének a keretében – vizsgálhatja, a vizsgálat eredményét dokumentálja, és azt a vezetőség értékeli.

3 Törvényi előírás alapján kötelező szabályzati dokumentumok

3.1 Üzletfolytonossági terv

Az üzletfolytonossági terv elkészítése

A folyamatos működés fenntartására, továbbá a súlyos üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében a pénzügyi szervezetnek rendelkeznie kell a szolgáltatásai folyamatosságát akadályozó rendkívüli események és helyzetek kezelésére vonatkozó vészhelyzeti és üzletmenet-folytonossági tervvel.[6] *Továbbá, rendelkeznie kell a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb – a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal.*[7]

A törvényekben előírt rendkívüli események és helyzetek kezelésére vonatkozó vészhelyzeti és üzletmenet-folytonossági terv elkészítése során a pénzügyi szervezet tetszőleges tartalom felosztást és elnevezést alkalmazhat - pl. Üzletmenet Folytonossági Terv (Business Continuity Plan, BCP), Katasztrófa Helyzet Elhárítási Terv (Disaster Recovery Plan, DRP), stb.

A tervet a továbbiakban az ajánlásban üzletfolytonossági tervnek nevezzük. Elkészítése során a pénzügyi szervezetnek legalább az alábbi tevékenységeket javasolt elvégeznie:

3.1.1 Üzletfolytonossági követelmények meghatározása

1. A pénzügyi szervezet meghatározza kritikus üzleti szolgáltatásait. Azonosítja a szolgáltatások nyújtásához szükséges folyamatait, meghatározza a folyamatok informatikai működés hibáiból származó lehetséges kiesései eseteit. Meghatározza az üzletszabályzatán alapuló igények alapján elfogadott visszaállási pontokat (recovery point objective, RPO: az a korábbi rendszer állapot, amely visszaállítása esetén az adatvesztés még elfogadható, illetve az adatok pótlása még lehetséges), valamint kritikus helyreállítási időket (recovery time objective, RTO: az elfogadható helyreállítási idő), és ennek során kitér legalább az alábbi típusok életszerű eseteire:
   a) természeti csapások, ember okozta működési rendellenességek, informatikai és adatkommunikációs infrastruktúra hibákból fakadó, a munkahely használatát akadályozó tényezők okozta részleges, teljes szolgáltatás kiesés különböző esetei,
   b) az alkalmazott üzemeltetési rendszer és/vagy az informatikai üzemeltetési helyszín használhatatlanná válása,
   c) külső szolgáltatások hibás teljesítése, teljes kiesése vagy elérhetetlenné válása.
2. A pénzügyi szervezet elvégzi a rendszer elemek rendelkezésre állási szempontú biztonsági osztályokba sorolását (lásd 3.5 fejezet), és az egyes eszközökre vetített technológiai követelmények alapján kialakítja informatikai rendszerét.

[6] Bit. 65/A.§ (6) g), Bszt.12.§ (7) g), Mpt.77/A.§ (6) g), Öpt.40/C.§ (6) g), Korm.r.3.§ (3) g)
[7] Bit. 65/A.§ (6) c), Bszt.12.§ (7) c), Mpt.77/A.§ (6) c), Öpt.40/C.§ (6) c), Korm.r.3.§ (3) c)

3.1.2 Az üzletfolytonossági eljárások kidolgozása

A pénzügyi szervezet kidolgozza és üzletfolytonossági tervében vagy ahhoz kapcsolódóan dokumentálja:

a) az informatikai rendszer kiesése idején követendő üzleti helyettesítő eljárásokat,
b) az informatikai és adatkommunikációs tartalék rendszerekre való átállás, valamint a helyreállításra vonatkozó operatív eljárásokat,
c) a normál üzemre történő visszaállás operatív eljárásait,
d) az egyes eljárásokra vonatkozóan az eljárások végrehajtóit illetve a végrehajtás felelőseit,
e) az egyes kiesési esetekre vonatkozóan a belső felelősségi rendet és a külső kommunikáció rendjét.

3.1.3 Az üzletfolytonossági eljárások ellenőrzése és bevezetése

A pénzügyi szervezet, dokumentált teszteléssel meggyőződik az eljárások alkalmazhatóságáról, oktatja az eljárásokat, és felkészíti a szervezetét az eljárások alkalmazására.

3.1.4 A pénzügyi szervezet az üzletfolytonossági tervezés eredményét dokumentálja, azt a vezetőség jóváhagyja, dokumentálja, valamint azt minden – pl. üzleti, rendszertechnikai, az alkalmazott informatikai és adatkommunikációs technológiát érintő – változást követően felülvizsgálja.

Az üzletfolytonossági tervezés során az alábbiak figyelembevételét javasoljuk:

3.1.5 A pénzügyi szervezet üzletfolytonossági terve olyan forgatókönyvszerű operatív intézkedési terv, amely lehetővé teszi az eljárások gyors, hibamentes végrehajtását.

3.1.6 Az üzletfolytonossági tervet – amennyiben azt a pénzügyi szervezet célszerűnek tartja – több dokumentumban készíti el, pl. az üzletmenet folytonossági terv az üzleti helyettesítő eljárásokat, az informatikai katasztrófa helyzet elhárítási terv az informatikai rendszer működésének a helyreállítását rögzíti.

3.1.7 A pénzügyi szervezet az üzletfolytonossági eljárásai alkalmazhatóságáról – ideértve a kritikus rendelkezésre állási idő teljesülését is –, valamint a végrehajtók felkészültségéről az egyes kiesési esetek kockázataival és a megvalósítás költségeivel arányosan megválasztott teszt eljárással győződik meg, és törekszik valós gyakorlati tesztek elvégzésére.

3.1.8 A pénzügyi szervezet az üzletfolytonossági eljárásainak tesztelése során a sikeres záró teszt lényeges körülményeit – ideértve a teszt eljárások egyes lépéseit, a végrehajtás tervezett és mért időtartamait is -, az elvégzett tevékenységeket és az egyéb megállapításokat, együttesen dokumentálja.

3.1.9 A pénzügyi szervezet gondoskodik az üzletfolytonossági terv aktuális állapotban tartásáról, és azt az informatikai rendszeren kívül is, és a helyreállításhoz szükséges helyszíneken is tárolja.

3.1.10 A pénzügyi szervezet valamint a kiszervezett tevékenységet végző a szerződésükben vagy ahhoz kapcsolódóan rögzítik a pénzügyi szervezet által elfogadott visszaállási pontokat valamint kritikus helyreállítási időket. Rögzítik továbbá a kiszervezett tevékenység végzőjének kifejezett felelősségét az üzletfolytonossági tervezés elvégzésére, az üzletfolytonossági tervének már a tevékenysége megkezdését megelőzően történő elkészítésére,

üzletfolytonossági eljárásainak mindenkori alkalmazhatóságára, valamint rögzítik az eljárások tesztelésének módszerét, gyakoriságát, valamint a pénzügyi szervezet felé történő beszámolás módját.

3.1.11 A pénzügyi szervezet – a szerződésben foglaltaknak megfelelő teljesítés ellenőrzésének a keretében –meggyőződik arról, hogy a kiszervezett tevékenység üzletfolytonossági eljárásai megfelelőek-e, és biztosítják-e a pénzügyi szervezet üzletfolytonossági követelményeit.

3.2 Mentési rend

A pénzügyi szervezetnek rendelkeznie kell az informatikai rendszer szoftver elemeire vonatkozó olyan biztonsági mentésekkel és mentési renddel, ***továbbá helyreállítási tervvel,*** *amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik, továbbá a mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolnia, és gondoskodnia kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.*[8]

A pénzügyi szervezet a mentési rendjét - az üzletfolytonossági követelményekkel összhangban - az elfogadott kritikus helyreállítási idők és visszaállítási pontok figyelembe vételével úgy alakítja ki, hogy a mentések típusa, gyakorisága és példányszáma elfogadható adatvesztési kockázatot eredményezzen, valamint az archiválásra vonatkozó jogszabályi követelményeket teljesíthesse.

A pénzügyi szervezet gondoskodik továbbá arról, hogy:

a) a mentett adatok nyilvántartásba vétele megtörténjen,
b) az adatok mentése illetve archiválása mellett az adatok visszaállításához szükséges valamennyi egyéb adat, és szoftver komponens is visszaállíthatóan mentésre illetve archiválásra kerüljön, vagy mentésük illetve archivált állományuk létezzen,
c) a mentésre illetve archiválásra alkalmazott adathordozó megválasztása az adathordozó felhasználhatóságának gyártói korlátozásai – pl. adatmegőrzési idő, újraírhatóság száma, tárolási előírások stb. - figyelembe vételével történjen,
d) a mentéseket tartalmazó adathordozók kezelése a rajtuk tárolt adatok biztonsági osztályához rendelt előírások szerint (lásd 3.5.1.3 fejezet) történjen, valamint a forrásrendszerrel azonos szintű biztonságos fizikai hozzáférés védelem mellett kerüljenek megőrzésre,
e) a mentett és az archív állományok adatainak a visszatöltéséhez szükséges berendezés mindenkor a rendelkezésre álljon.

A mentési rend kialakítása során az alábbiak figyelembevételét javasoljuk a pénzügyi szervezet számára:

3.2.1 A mentések tűzbiztos védelmét a pénzügyi szervezet az alábbiak szerint biztosítja:

a) az informatikai és adatkommunikációs rendszer egyes elemei visszaállítására készített mentéseket az éles adatoktól elkülönült, zárható, és legalább 30 perces tűzállóságú önálló helyiségben, az épület egy másik tűzszakaszában, vagy az éles adatokat tartalmazó épülettől a tűzvédelmi szabályoknak megfelelő módon elválasztott másik (pl. szomszédos) épületben tárolja,

[8] Bit. 65/A.§ (6) e), Bszt.12.§ (7) e), Mpt.77/A.§ (6) e), Öpt.40/C.§ (6) e), Korm.r.3.§ (3) e), (4)

b) az üzemi informatikai rendszer teljes használhatatlanná válását követő helyreállításra szolgáló mentéseket és az archív állományokat az üzemi rendszertől földrajzilag legalább 400 méter távolságra elkülönült helyszínen - tárolja.

3.2.2 A pénzügyi szervezet mentési rendje tartalmazza az alábbi műszaki leírásokat:

a) A pénzügyi szervezet mentési rendszerének összefoglaló leírása, amely tartalmazza:

- a mentett adatok körének teljes körű meghatározását – pl. az alkalmazások-fájlszerverek adatai, üzleti- egyéb alkalmazások, rendszer környezetek, alkalmazás- és eszköz konfigurációs állományok, napló állományok, scriptek stb.,
- a mentések módját, az alkalmazott mentési szoftverek és a mentőeszközök megnevezését, a mentett állományok őrzési helyét, az egyes mentésekhez tartozó lehetséges adatvesztési eseteket – pl. az előző napi mentésből a tárgynap napközbeni tranzakciói nem állíthatók vissza,
- a mentések időpontját,
- a mentett állományok megőrzési idejét,
- a mentett állományok nyilvántartásának módját,
- az elkészített mentések olvashatóságának az ellenőrzésére alkalmazott eljárásokat, az ellenőrzés gyakoriságát.

b) Mentési eljárások, amelyek a mentések elvégzésére és annak ellenőrzésére vonatkozó operatív eljárások,

c) Visszatöltési eljárások, amelyek az egyes mentések visszatöltésére és a visszatöltés megfelelőségének az ellenőrzésére vonatkozó operatív eljárások.

d) Helyreállítási eljárások, amelyek a mentéssel érintett informatikai és/vagy adatkommunikációs rendszerek visszatöltés utáni visszaállítására és a visszaállítás megfelelősségének az ellenőrzésére vonatkozó operatív eljárások,

3.2.3 A pénzügyi szervezet a mentések operatív elvégzését az üzemeltetési utasításaiban írja elő (lásd 3.3.5 b) fejezet).

3.3 A működtetésre és a fejlesztésre vonatkozó szabályzati dokumentumok

A pénzügyi szervezetnek rendelkeznie kell az informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, a fejlesztésre vonatkozó tervekkel.[9]

Az üzleti igények folyamatos teljesítéséhez a pénzügyi szervezetnek előrelátóan fel kell mérnie az alkalmazási rendszerek fejlesztési igényeit, az informatikai rendszer kapacitás bővítési igényeit, a technológiai avulás és az új technológiák megjelenése miatti infrastruktúrafejlesztési igényeket, és ezek megvalósítását terveznie javasolt.

Az informatikai rendszer napi működtetésére vonatkozó szabályzati rendszerét – szabályzatok, műszaki- és nyilvántartási dokumentumok, feljegyzések stb. – a pénzügyi szervezet a jelen ajánlás 1.3 fejezetében leírtakkal összhangban alakítja ki.

[9] Bit. 65/A.§ (6) a), Bszt.12.§ (7) a), Mpt.77/A.§ (6) a), Öpt.40/C.§ (6) a), Korm.r.3.§ (3) a)

A dokumentumok elkészítésének javasolt szempontjai:

3.3.1 A pénzügyi szervezet informatikai tervei összhangban vannak üzleti céljaival, figyelembe veszik az informatikai- és adatkommunikációs technológiai irányokat, valamint a pénzügyi szervezet az informatikai tervezés során elkészíti legalább az alábbi dokumentumokat:

a) éves informatikai beruházási és költség tervek,
b) rövidtávú informatikai terv vagy stratégia.

3.3.2 A pénzügyi szervezet megfontolja, és kockázatai arányában dönt az informatikai- és adatkommunikációs stratégia alkotás elvégzéséről, és az alábbi dokumentumok elkészítéséről:

a) középtávú informatikai terv vagy stratégia,
b) hosszabb távú informatikai terv vagy stratégia.

3.3.3 Az informatikai tervezés eredményét a pénzügyi szervezet erre kijelölt vezetője illetve vezetői testülete jóváhagyja, és a vezetői döntés tartalmát a pénzügyi szervezet dokumentálja.

3.3.4 A pénzügyi szervezet az informatikai rendszer bevezetéséhez elkészíti, majd változások esetén módosítja az alábbi szabályzati dokumentumait:

a) adatkommunikációs rendszerének hálózati dokumentációja, amely tartalmazza legalább az alábbiakat:
    - az adathálózati rendszerének hálózati diagramja,
    - a hálózati eszközök, valamint az eszköz csatlakoztatások nyilvántartása,
    - adatátviteli összeköttetések (fizikai vonalak) műszaki nyilvántartása,
    - az adathálózat szegmentálása,
    - géptermi eszköz elhelyezési rajzok,
    - a kialakított hálózati zónák, a hálózati zónák közötti forgalmi szabályok elvi bemutatása,
    - a logikai szintű adatkapcsolatok, és az alkalmazott adatkapcsolati módok technológiai megvalósítása (pl. portok, szolgáltatások, pl. layer 3, 4-7 módok stb.),
b) futtató rendszerkörnyezet (működési architektúra, működtető környezetek, adatbázis kezelő, felügyeleti megoldás bemutatásai), rendszerenként,
c) mentési rend (mentési, visszatöltési, visszaállítási eljárások, lásd 3.2 fejezet), rendszerenként,
d) hozzáférési rend (az adatokhoz történő hozzáférési rend dokumentumai, lásd 3.7 fejezet), rendszerenként,
e) a rendszerek üzemeltetési leírásai (üzemeltetés egyes tevékenységi lépéseinek a leírása).

3.3.5 A pénzügyi szervezet napi informatikai üzemeltetéséhez elkészíti legalább az alábbi szabályzati dokumentumokat:

a) a felhasználói fiókok kezelésének rendje (a felhasználói fiókok kezelésének – létrehozás, módosítás, tiltás, engedélyezés, törlés, kiemelt jogosultságú fiókok használata, vészhelyzeti elérhetőség biztosítása – szabályai, lásd 5.3 fejezet),

b) üzemeltetési utasítások, amelyek a rendszeres üzemeltetői tevékenységekhez kapcsolódnak - pl. napi, heti, havi, éves stb. operátori/rendszergazdai, hálózat/rendszer felügyeleti, vírusvédelmi, biztonsági feladatok, stb. -, és tartalmazzák
    - a feladatok végrehajtásának és a bizonylatolásnak az előírását,
    - az ellenőrzési feladatok előírását, ideértve a naplók ellenőrzési feladatait is,
    - a feladat végrehajtásához rendelt feljegyzések elkészítését,
    - a beszámolási feladatokat,
    - valamint az alkalmazandó műszaki dokumentumokra és vezetett nyilvántartásokra történő hivatkozásokat.
c) az éles üzemi rendszerek változtatásához kapcsolódó engedélyezési és változáskezelési eljárások,
d) az adathordozók kezelésének eljárása (lásd 5.6 fejezet).

3.3.6 A pénzügyi szervezet megfontolja, és kockázataival arányosan dönt az egyes rendszerek beállítási/telepítési leírásainak szabályzati dokumentumokként történő elkészítéséről.

3.4 Alkalmazási rendszerek forráskódjai és az informatikai rendszerleírások

A pénzügyi szervezetnek rendelkeznie kell minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működését – még a szállító, illetőleg a rendszerfejlesztő tevékenységének megszűnése után is – biztosítja.[10] *Mindenkor a rendelkezésre kell állnia továbbá az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek, valamint az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének.*[11]

A pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

3.4.1 Amennyiben a pénzügyi szervezet kritikus alkalmazásait önállóan, saját fejlesztőivel maga fejleszti, illetve a fejlesztésbe külső fejlesztőket von be, saját belső változáskezelési eljárása keretében biztosítja, hogy az üzembe helyezett alkalmazási rendszerek fejlesztői dokumentációja áttekinthető formában elkészüljön, és az a forráskóddal együtt egyértelműen azonosítható módon a saját szervezetén belül archiválásra kerüljön.

3.4.2 Amennyiben a pénzügyi szervezet az alkalmazásainak a fejlesztését a szakmai irányítás megtartása mellett külső szoftverfejlesztővel végezteti, saját belső változáskezelési eljárása keretében biztosítja, hogy az üzembe helyezett alkalmazási rendszerek fejlesztői dokumentációja áttekinthető formában a pénzügyi szervezeten belül álljon elő, és az a forráskóddal együtt egyértelműen azonosítható módon archiválásra kerüljön.

3.4.3 Amennyiben a pénzügyi szervezet nem végez szoftverfejlesztést, a számára készített egyedi fejlesztések megrendelései illetve fejlesztési szerződései biztosítják, hogy:

[10] Bit. 65/A.§ (6) b), Bszt.12.§ (7) b), Mpt.77/A.§ (6) b), Öpt.40/C.§ (6) b), Korm.r.3.§ (3) b)
[11] Bit. 65/A.§ (7) a) b), Bszt.12.§ (9) a) b), Mpt.77/A.§ (7) a) b), Öpt.40/C.§ (7) a) b), Korm.r.4.§ (1) a) b)

a) a szoftverfejlesztő a szoftver átadásával egyidejűleg átadja az adatok szintaktikai szabályait és az adatok tárolási szerkezetét is tartalmazó részletes adatbázis dokumentációt,

b) abban az esetben, ha a szállító a hibajavítási- vagy az alkalmazás továbbfejlesztésére vonatkozó igényeket bármilyen okból nem teljesíti, hozzájuthasson – pl. ügyvédi letét útján – a szoftver forráskód állományához és fejlesztési dokumentációjához, és azokat a továbbiakban jogszerűen felhasználhassa.

3.4.4 A pénzügyi szervezet gondoskodik arról, hogy az alkalmazási rendszerek forráskódjaihoz illetve informatikai rendszerleírásaihoz kapcsolódóan a kiszervezett rendszerének adatai is - a kockázatai alapján elfogadott visszaállási pontok figyelembe vételével, további felhasználásra alkalmas formátumban mindenkor a rendelkezésére álljanak.

3.4.5 A szoftverfejlesztési tevékenységet folytató pénzügyi szervezet megfontolja, és kockázatai arányában döntést hoz belső fejlesztési eljárásának dokumentált szabályzati dokumentumként történő elkészítéséről, valamint abban rögzíti az elkészítendő fejlesztői dokumentációk körét.

3.5 Biztonsági osztályba sorolási rend

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az informatikai rendszer elemeinek a pénzügyi szervezet által meghatározott biztonsági osztályokba sorolási rendszerének.[12]

A kialakítás javasolt szempontjai:

3.5.1 A pénzügyi szervezet a kritikus hardver elemeinek a rendelkezésre állási követelményei szerinti biztonsági osztályba sorolási rendszerét úgy alakítja ki, hogy az egyes osztályokhoz hozzárendeli legalább az alábbi jellemzőket:

a) a hardver elem technológiai kialakítása és hibatűrő képessége - pl. belső redundanciák,

b) a javítás illetve eszköztartalékolás módja pl. helyszíni javítás helyszíni tartalék modullal vagy csereeszközzel, külső szerviz szolgáltatás igénybevétele, szerviz szolgáltatónál csereeszköz rendelkezésre tartása stb.,

c) a szolgáltatások igénybe vétele esetén a szolgáltatási idők – pl. hibajavítás kezdete, befejezése, stb.,

d) eszköz szintű (működésbeli) redundancia kialakítása – pl. magas rendelkezésre állási (high availability, HA) megoldások, terhelés megosztás, stb.

3.5.2 A pénzügyi szervezet adatainak bizalmasság szerinti biztonsági osztályokba sorolási rendszere összhangban van a bank- értékpapír- és biztosítási titokra, a személyes adatok védelmére vonatkozó jogszabályi előírásokkal, a pénzügyi szervezet adatvédelmi előírásaival, valamint a saját dolgozók személyes adatait és a különleges (személyes) adatokat[13] a legmagasabb biztonsági osztályba sorolja,

3.5.3 Az adatainak bizalmasság szerinti biztonsági osztályba sorolási rendszeréhez kapcsolódóan a pénzügyi szervezet rendelkezik az egyes biztonsági osztályokba tartozó adatok kezelésére – címkézésére, tárolására, fizikai biztonságára és hozzáférés szabályozására, továbbítására,

[12] Bit. 65/A.§ (7) c), Bszt.12.§ (9) c), Mpt.77/A.§ (7) c), Öpt.40/C.§ (7) c), Korm.r.4.§ (1) c)

[13] az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény – Infotv.

megsemmisítésére stb. – vonatkozó eljárásokkal, és az eljárások biztonsági szintje arányos az adatok bizalmassági követelményével.

3.6 Az adatok hozzáférési rendje

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az adatokhoz történő hozzáférési rend meghatározásának,[14] valamint gondoskodnia kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.[15]

A hozzáférési rend – vagy más szóhasználattal: a logikai hozzáférési rend - rögzíti mindazokat a rendszerváltozókat és beállítási értékeket, amelyek meghatározzák, hogy az adatokhoz csak az arra jogosultak, és ők is csak a számukra szükséges műveletek elvégzésére férjenek hozzá. Az egyes rendszerek[16] hozzáférési rendjét a rendszerek műszaki dokumentációja illetve önálló dokumentum tartalmazza, és a hozzáférési rendeket a pénzügyi szervezet úgy alakítja ki, hogy azok biztosítsák a mentett valamint az archivált adatállományoknak a forrás adatokkal legalább azonos szintű hozzáférés védelmét is.

A logikai hozzáférési rend tartalma

3.6.1 Rendszerenként legalább az alábbiak:

a) rendszerazonosító (hálózati név), hálózati kapcsolatok, adatkapcsolatok, portok és protokollok, a felhasználói hitelesítés módja,
b) a rendszerszintű biztonsági beállítások,
c) a helyi felhasználók, felhasználócsoportok, beépített felhasználói fiókok, fiók beállítások, helyi házirend tartalma – biztonsági házirend pl. jelszóházirend, biztonsági naplózás stb. – tartalma,
d) címtár rendszerek esetében a felhasználók, felhasználócsoportok, beépített felhasználói fiókok, fiók beállítások, hozzáférés-vezérlési listák, szervezeti egységek, közzétett (megosztott) erőforrások, a címtár objektumokhoz tartozó hozzáférési jogok, a tartományok biztonsági beállításai – pl. jelszószabályok, naplózási beállítások, stb.
e) erőforrások hozzáférési engedélyei, hozzáférés-vezérlő listák, erőforrások eseménynaplózási beállítása,
f) mappák megosztása, a megosztás paraméterei, a megosztáshoz és a fájlokhoz tartozó jogok (pl. share permissions, security, stb.),
g) alkalmazási rendszerek esetében továbbá a felhasználói csoportok (szerepkörök) és az üzleti műveletek egymáshoz rendelése (menü security), valamint az általános biztonsági beállítások – pl. jelszószabályok, naplózási beállítások, az adatkapcsolatok számára létrehozott - technikai jellegű - felhasználók rendszeren belüli kezelésének eljárása,
h) adatbázis kezelők esetében továbbá a fiók beállítások, a nem beépített szerepkörök (roles) rendszer- és objektum privilégiumai, profilok és biztonsági beállítások – pl. jelszószabályok, naplózási beállítások,

[14] Bit. 65/A.§ (7) d), Bszt.12.§ (9) d), Mpt.77/A.§ (7) d), Öpt.40/C.§ (7) d), Korm.r.4.§ (1) d)
[15] Bit. 65/A.§ (6) e), Bszt.12.§ (7) e), Mpt.77/A.§ (6) e), Öpt.40/C.§ (6) e), Korm.r.3.§ (4)
[16] alkalmazások, adatbázis kezelők, operációs rendszerek, hálózati szolgáltatást nyújtó egyéb szerverek - pl. fájl szerverek, web, ftp, proxy szerverek stb. -, az adatkommunikációs eszközök, pl. tűzfal, router stb. – operációs rendszerei

i) a kiemelt jogosultságú rendszer fiókok – pl. rendszeradminisztrátori fiókok -, valamint a technikai jellegű felhasználók és a felelősök nyilvántartása, a kezelésükre vonatkozó szabályok,

j) azoknak a felhasználói fiókoknak a listája, amelyek esetén a pénzügyi intézmény szükségesnek tartja a vészhelyzeti elérhetőség biztosítását.

A logikai hozzáférési rend karbantartása

3.6.2 A pénzügyi szervezet a rendszerek biztonsági beállításait a rendszerre vonatkozó szakmai „hardening" ajánlások, ill. a szállítótól kapott üzemeltetési kézikönyvek aktuális verziói alapján időszakosan felülvizsgálja.

3.7 Adatgazda és a rendszergazda kijelölését tartalmazó okirat

*A pénzügyi szervezetnek mindenkor rendelkezésre kell állnia az adatgazda és a rendszergazda kijelölését tartalmazó **dokumentumnak**/okiratnak.*[17]

A pénzügyi szervezet üzleti adatainak gazdája alapértelmezetten a szervezet operatív vezetője (pl. vezérigazgató), illetve a szervezet működési szabályzatában erre kijelölt vezető. Amennyiben az adatgazdai feladatok delegálásra kerülnek, a feladatokhoz rendelt adatgazda szerepkörök illetve munkakörök betöltőit a pénzügyi szervezetnek dokumentált módon kell kijelölnie. Ennek során az alábbiak figyelembevételét javasoljuk a pénzügyi szervezetek számára:

3.7.1 A pénzügyi szervezet az adatgazdai feladatokat a szabályzati rendszerében rögzíti. Az adatgazdai feladatköröket az adatok tartalmát és minőségi követelményeit ismerő szerepkörökhöz delegálja, és ezt a szabályzati rendszerében rögzíti. Az adatgazdák feladata az általuk menedzselt adatokhoz való hozzáféréshez a jogosultságok jóváhagyása és visszavonása.

3.7.2 Az adatgazdák és a rendszergazdák kijelölését a pénzügyi szervezet a kijelölést tartalmazó, a dolgozó által tudomásul vett és aláírását tartalmazó hivatalos dokumentummal végzi, amely lehet megbízás, munkaköri leírás, illetve egyéb dokumentum.

3.8 Az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződések

A pénzügyi intézménynél mindenkor rendelkezésre kell állnia az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek.[18]

Az alábbi szempontok figyelembe vételét javasoljuk a pénzügyi szervezetek számára:

3.8.1 A pénzügyi szervezet rendelkezik az általa birtokolt szoftver eszközök jogtisztaságát igazoló bizonylatokkal - szerződések, licensz számlák, licensz igazolások stb.-, és ezeket oly módon tárolja, hogy egy belső vagy külső jogtisztaságra vonatkozó vizsgálat bármikor, nehézség nélkül elvégezhető legyen.

[17] Bit. 65/A.§ (7) e), Bszt.12.§ (9) e), Mpt.77/A.§ (7) e), Öpt.40/C.§ (7) e), Korm.r.4.§ (1) e)
[18] Bit. 65/A.§ (7) f), Bszt.12.§ (9) f), Mpt.77/A.§ (7) f), Öpt.40/C.§ (7) f), Korm.r.4.§ (1) f)

3.9 A szoftvereszközök teljes körű és naprakész nyilvántartása

A pénzügyi intézménynél mindenkor rendelkezésre kell állnia az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának. [19]

Az alábbi szempontok figyelembe vételét javasoljuk a pénzügyi szervezetek számára:

3.9.1 A pénzügyi szervezet biztosítja, hogy valamennyi ügyviteli, üzleti szoftvereszközeinek – pl. a szolgáltatásnyújtáshoz kapcsolódó alapszoftverek, alkalmazási rendszerek, adatbázis kezelők, felügyeleti és biztonsági szoftvereket stb. – nyilvántartása informatikai rendszereiből bármikor nehézség nélkül előállítható, illetve ennek hiányában ezekről teljes körű nyilvántartást vezet, és ebben az esetben biztosítja a nyilvántartás naprakész állapotát.

3.9.2 A pénzügyi szervezet megfontolja, és kockázatai arányában dönt önálló szoftver nyilvántartás bevezetéséről, és a nyilvántartást rendszeres időközönként összeveti az informatikai eszközein telepített szoftvereivel.

3.10 Az egyes munkakörök betöltéséhez szükséges informatikai ismeretet meghatározó dokumentumok

A pénzügyi szervezetnek mindenkor rendelkezésre kell állnia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet meghatározó dokumentumoknak.[20]

Az alábbi szempontok figyelembe vételét javasoljuk a pénzintézetek számára:

3.10.1 A pénzügyi szervezet meghatározza az egyes munkakörök betöltéséhez szükséges informatikai – és ezen belül az informatikai biztonsági ismeretet, és ezt belső szabályzati rendszerében vagy ahhoz kapcsolódóan dokumentálja. Gondoskodik továbbá arról, hogy a munkaköröket olyan személyek töltsék be, akik birtokában vannak az előírt, naprakész ismereteknek.

4 Az informatikai biztonsági rendszer kötelezően alkalmazandó kontrolljai

4.1 Szervezeti és működési rend, a folyamatba épített ellenőrzés szabályai

Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével a pénzügyi intézménynek meg kell határoznia a szervezeti és működési rendeket, a felelősségi, nyilvántartási és tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.[21]

Az alábbi szempontok figyelembe vételét javasoljuk a pénzintézetek számára:

4.1.1 A pénzügyi szervezet meghatározza a helyettesítési rendet, az egymással összeférhetetlen informatikai feladatokat - pl. egyazon alkalmazás fejlesztése és üzemeltetése -, és biztosítja, hogy összeférhetetlen feladatokat még helyettesítés esetén se láthasson el egyazon személy.

[19] Bit. 65/A.§ (7) g), Bszt.12.§ (9) g), Mpt.77/A.§ (7) g), Öpt.40/C.§ (7) g), Korm.r.4.§ (1) g)
[20] Bit. 65/A.§ (9), Bszt.12.§ (11), Mpt.77/A.§ (9), Öpt.40/C.§ (9), Korm.r.5.§
[21] Bit. 65/A.§ (3), Bszt.12.§ (4), Mpt.77/A.§ (3), Öpt.40/C.§ (3), Korm.r.2.§ (3)

Amennyiben az összeférhetetlen feladatok szétválasztására a pénzügyi szervezetnek nincs lehetősége, kiegészítő kontrollt alkalmaz az ellenőrzés, illetve a számon kérhetőség biztosítására.

4.1.2 A pénzügyi szervezet az informatikai szervezetének felépítését és működését a szervezeti és működési szabályzatában, az informatikai munkakörökhöz rendelt feladatokat és felelősségeket a dolgozók által tudomásul vett és a tudomásul vételt igazoló aláírásukat is tartalmazó munkaköri leírásokban határozza meg.

4.1.3 A pénzügyi szervezet az üzleti működésének jellegére, nagyságrendjére figyelemmel alakítja ki informatikai szervezetét, annak működési rendjét, nyilvántartási- és a tájékoztatási szabályait.

4.1.4 A pénzügyi szervezet úgy alakítja ki az informatikai biztonsági funkciót illetve szervezetet, valamint úgy határozza meg a vonatkozó feladatokat, hogy az arányban álljon informatikai biztonsági kockázataival.

4.1.5 A pénzügyi szervezet biztosítja, hogy valamennyi munkatársa megismerje és elfogadja a rá vonatkozó informatikai biztonsági szabályokat, és ezeket képes legyen alkalmazni.

4.1.6 Az informatikai biztonságért alapértelmezetten a pénzügyi szervezet legfelső operatív vezetője a felelős, aki a feladatkört delegálhatja, és a szervezet által meghatározott informatikai és információbiztonsági ismeretekkel rendelkező informatikai biztonsági felelőst nevezhet ki, vagy bízhat meg. Az informatikai biztonsági felelős a kis szervezetek esetében lehet az informatikai terület kijelölt munkatársa, de nagyobb szervezetek esetében a pénzügyi szervezet önálló – az informatikai üzemeltetéstől szervezetileg független - informatikai biztonsági felelőst nevez ki, és döntése alapján önálló informatikai biztonsági területet hoz létre.

4.1.7 A pénzügyi szervezet biztosítja az informatikai biztonság független és rendszeres ellenőrzését. Az ellenőrzést végezheti a szervezet belső ellenőrzése, az informatikai biztonsági felelős, külső szakértő, együtt, vagy egymás között megosztva.

4.2 Informatikai ellenőrző rendszer

A pénzügyi intézménynek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működtetnie kell.[22]

A pénzügyi szervezet informatikai ellenőrző rendszerét úgy alakítja ki, hogy az biztosítsa, hogy az informatikai rendszere hibáinak észlelése és azok megszüntetése az üzletfolytonossági tervében meghatározott rendelkezésre állási időknek megfelelően megtörténhessen. Ennek során az alábbiak figyelembe vétele javasolt:

4.2.1 A pénzügyi szervezet informatikai rendszere biztonságos működtetésére saját hatáskörben, vagy külső szolgáltató igénybevételével

a) felhasználói helpdesket üzemeltet,
b) hálózat felügyeleti rendszert működtet,
c) adathálózatán – elsősorban a nem biztonságosnak tekintett szegmensekben – behatolás detektáló rendszert (intrusion detection system, IDS) működtet,

[22] Bit. /5/A.§ (4), Bszt.12.§ (5), Mpt.77/A.§ (4), Öpt.40/C.§ (4), Korm.r.3.§ (1)

d) megfontolja, és kockázatai arányában alkalmazás felügyeleti rendszert, valamint behatolás gátló rendszert (intrusion prevention system, IPS) működtet.

4.3 Üzemi környezet elkülönítése és a változtatások kezelése

A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez rendelkeznie kell olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint lehetővé teszi a megfelelő változáskövetés és változáskezelés fenntartását.[23]

A változáskezelési és változáskövetési eljárásainak a kialakításakor a pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

4.3.1 Fejlesztéseit és teszteléseit az üzemi környezettől elkülönített környezetekben végzi – pl. önálló rendszer, önálló virtuális környezetek.

4.3.2 Fejlesztői teszt környezetein éles rendszerből vett adatokat csak anonimizálást követően használ.

4.3.3 A futtató kód előállítását a pénzügyi szervezet informatikai üzemeltetője végzi, aki egyben gondoskodik a forrás- és a futtató kód azonosításáról és tárolásáról.

4.3.4 Meghatározza, hogy milyen módon és meddig van lehetőség a korábbi futtató kód visszatöltésére, illetve a korábbi működés visszaállítására.

4.4 Archiválás

A pénzügyi intézménynek rendelkeznie kell jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizzék.[24]

Az archiválási rendszere kialakításakor a pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

4.4.1 A pénzügyi szervezet a jogszabályban meghatározott nyilvántartásairól a dokumentált mentési rend alapján mentéseket készít, és azokat a jogszabályban meghatározott ideig – de legalább öt évig – bármikor visszakereshetően, helyreállíthatóan megőrzi (archív állományok),

4.4.2 A pénzügyi szervezet az adattároló berendezéseinek, rendszereinek a cseréje során gondoskodik arról, hogy a mentett és az archív adatok az újonnan üzembe állított rendszerekbe átkerüljenek, vagy gondoskodik a régi rendszerek üzemben tartásáról, illetve arról, hogy azok mindenkor üzembe állíthatóak legyenek.

[23] Bit. 65/A.§ (6) d), Bszt.12.§ (7) d), Mpt.77/A.§ (6) d), Öpt.40/C.§ (6) d), Korm.r.3.§ (3) d)
[24] Bit. 65/A.§ (6) f), Bszt.12.§ (7) f), Mpt.77/A.§ (6) f), Öpt.40/C.§ (6) f), Korm.r.3.§ (3) f)

5 Az informatikai biztonsági rendszer kockázatokkal arányosan kialakítandó védelmi kontrolljai

5.1 Az informatikai rendszer elemeinek azonosítása

A pénzügyi szervezetnek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról.[25]

A pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

5.1.1 A pénzügyi szervezet az eszközeiről – ideértve az informatikai-és adatkommunikációs működéshez kapcsolódó hardver és szoftver eszközöket, személyi hitelesítő eszközöket, stb. – műszaki célú nyilvántartást vezet, amely rögzíti legalább az alábbiakat:

a) az eszköz megnevezése, típusa, azonosítója,
b) elhelyezése – tárolási helye, vagy mobil eszközök esetében a birtokos személye,
c) hardver konfiguráció.

5.1.2 Meghatározza az egyes eszközre telepíthető szoftverek körét, és biztosítja, hogy az egyes eszközökön csak engedélyezett szoftverek legyenek telepítve,

5.1.3 Biztosítja az eszközök szoftver konfigurációjának bármikor történő megállapíthatóságát, illetve ennek hiányában az egyes eszközökön telepített szoftverekről nyilvántartást vezet (lásd 3.9.1 fejezet),

5.1.4 A kritikus üzemeltetési helyszíneire belépési jogosultsággal rendelkező személyeket azonosítóval látja el, és a belépéseket nyilvántartja,

5.2 A biztonsági rendszer védelme

A pénzügyi szervezetnek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljes körűségét biztosító ellenőrzésekről, eljárásokról.[26]

A pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

5.2.1 Internet felőli adathálózati sérülékenység vizsgálat (external network vulnerability scan) elvégzése és a kockázatokkal arányosan megválasztott szint feletti hibák kijavítása, rendszeres időközönként megismételve, negyedévente legalább egyszer,

5.2.2 Internet felől elérhető web alkalmazások sérülékenység vizsgálata (web application vulnerability scan) elvégzése és a kockázatokkal arányosan megválasztott szint feletti hibák kijavítása, üzembe állítást megelőzően, majd rendszeres időközönként megismételve, évente legalább egyszer,

[25] Bit. 65/A.§ (5) a), Bszt.12.§ (6) a), Mpt.77/A.§ (5) a), Öpt.40/C.§ (5) a), Korm.r.3.§ (2) a)
[26] Bit. 65/A.§ (5) b), Bszt.12.§ (6) b), Mpt.77/A.§ (5) b), Öpt.40/C.§ (5) b), Korm.r.3.§ (2) b)

5.2.3 Adathálózati topológia, a rendszerkomponensek változtatásaira, új eszközök rendszerbe állítására teljes körű változáskezelési eljárás működtetése, a változások jóváhagyásának a dokumentálása,

5.2.4 Valamennyi rendszerkomponens esetében a beállítások időszakos felülvizsgálata, és a nem biztonságos illetve szükségtelen szolgáltatások – pl. szkriptek, driver-ek, portok, szervizek – törlése illetve tiltása.

5.2.5 A biztonsági javító csomagok figyelemmel kísérése, és az informatikai rendszer komponensekre és szoftverekre a kockázatoktól függően, valamint előzetes teszt üzemet követően a gyártói javító csomagok installálása, vagy ezt kiváltó intézkedés megvalósítása és dokumentálása.

5.3 Felhasználói fiókok adminisztrációja

A pénzügyi szervezetnek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események).[27]

A pénzügyi szervezet az informatikai rendszerének hozzáférését felhasználói azonosítók használatához köti, és a használatot a felhasználói fiókok kezelésének rendjében szabályozza, és – ide nem értve az ügyfelek home/internet oldali hozzáférését –, annak kialakítása során az alábbiakat veszi figyelembe:

5.3.1 A felhasználói fiókok létrehozása, törlése (tiltása), illetve módosítása jóváhagyott és dokumentált módon történik, az alábbi irányelvek szerint:

a) új belépő első szintű felhasználói fiókjának a létrehozását (pl. hálózati hozzáférést biztosító felhasználói fiókok), valamint alkalmazási rendszerekben meglévő felhasználói csoportba sorolt felhasználói fiókok létrehozását, illetve ezek törlését (tiltását) a munkahelyi vezető engedélyezi, a dolgozói felvételéért felelős (vezető vagy szakterület) javaslatára vagy értesítése mellett,

b) alkalmazási rendszerekben meglévő felhasználói fiókok felhasználói csoportba vagy csoportokba sorolását, a besorolások módosítását a munkahelyi vezető és az adatgazda együttesen engedélyezi,

c) bármilyen rendszerben új felhasználói csoport fiók létrehozását, illetve, meglévő csoport fiók jogosultságainak a módosítását az adatgazda kezdeményezi, és erről tájékoztatást kap az informatikai biztonsági felelős, amennyiben a pénzügyi szervezet az informatikai biztonsági felelős szerepkört működteti,

d) egyedi rendszer jogosultsággal rendelkező felhasználói fiókok létrehozását, valamint felhasználói fiók egyedi rendszer jogosultságainak változtatásával járó módosítását, a munkahelyi vezető és az adatgazda együttesen engedélyezi, és az engedélyezésről tájékoztatást kap az informatikai biztonsági felelős, amennyiben a pénzügyi szervezet az informatikai biztonsági felelős szerepkört működteti.

5.3.2 A felhasználói fiók átvételét követően a felhasználó felelős a felhasználói fiók használatáért, valamint a mindenkori jelszó kezeléséért.

[27] Bit. 65/A.§ (5) c), Bszt.12.§ (6) c), Mpt.77/A.§ (5) c), Öpt.40/C.§ (5) c), Korm.r.3.§ (2) c)

5.3.3 A pénzügyi szervezet a felhasználói fiókok létrehozása és kiadása során biztosítja, hogy az a személy vehesse birtokba a felhasználói fiókot, akinek a részére az létre lett hozva, és – az informatikai rendszeren belüli vagy önálló nyilvántartás vezetésével - biztosítja a felhasználói fiókok és a fiókok használatáért felelős felhasználók egyértelmű egymáshoz rendelését.

5.3.4 Az informatikai rendszerekben mindenkor csak az engedélyezett felhasználói fiókok aktívak, és a pénzügyi szervezet biztosítja, hogy ennek ellenőrzése nehézség nélkül elvégezhető legyen.

5.3.5 Felhasználói fiókok többek általi közös használata csak akkor lehetséges, ha a közös használat nem jelent valós üzleti kockázatot, vagy a felhasználás által jelentett kockázatok elfogadásra kerültek, illetve ha a használó személye más módon – pl. kiegészítő kontrollokon keresztül - egyértelműen azonosítható - pl. a felhasználói fiók használata személyes felhasználói fiókkal történő belépéshez kötött, és az elérés naplózásra kerül, stb.

5.3.6 Kiemelt felhasználói fiókok valamint technikai felhasználói fiókok esetében a pénzügyi szervezet megvizsgálja a fiókok interaktív használatával végezhető műveletek kockázatait, nyilvántartja a fiókokat és azok felelőseit, és a fiókok használatának a feltételeit a kockázatokkal arányosan alakítja ki. Jelentős üzleti kockázatot jelentő esetekre biztosítja, hogy legalább két személy részvételére legyen szükség a felhasználói fiók használathoz, pl. a belépés engedélyezését két egymástól független jelszó megadásához köti. A pénzügyi szervezet osztott jelszavak alkalmazása esetében is biztosítja az egyszemélyi felelősséget és a számon kérhetőséget.

5.3.7 A jelszó szabályokat az egyes rendszerekben a felhasználói fiók használatának kockázataival arányosan határozza meg, ennek során a bank-, értékpapír-, biztosítási-, pénztár- és üzleti titkot tartalmazó kritikus rendszereknél a belső dolgozói hozzáférések esetében az alábbiakat alkalmazza:

a) a jelszó komplex (tartalmaz pl. legalább 2 kis- 2 nagybetűt, 2 számot), és hosszúsága legalább 8 karakter,
b) a felhasználói fiókok jelszava maximum 90 napos automatikus lejáratú,
c) a legutoljára használt 5 jelszóra nem beállítható,
d) azon technikai felhasználói azonosítók esetében, amelyek letiltása kritikus rendszerek működését megállítja, az automatikus lejáratást nem alkalmazza, de azt 90 naponként megváltoztatja – és ennek kötelezettségét előírja, illetve amennyiben a jelszó megváltoztatása technológiai okok miatt nem vagy csak nehezen lenne megvalósítható, a technikai felhasználói fiók jelszava komplex (pl. legalább 3 kis- 3 nagybetűt, 3 számot tartalmaz), és hosszúsága legalább 12 karakter.

5.3.8 A kritikus rendszerek esetében a felhasználói azonosítóval végzett belépés- kilépés, jelszóváltoztatás események adatait – kivéve a jelszót - naplózza.

5.3.9 Távoli hozzáférések esetében a felhasználói azonosító használata mellett legalább még egy további, a felhasználót hitelesítő faktort – pl. dinamikus kódot, tanúsítványt – is használ.

5.3.10 Amennyiben a pénzügyi szervezet PKI rendszert üzemeltet és tanúsítványokat állít elő, rendelkezik a kapcsolódó dokumentált kulcskezelési eljárással.

5.3.11 A vészhelyzeti elérés módját a felhasználói fiókok kezelésének rendjében dokumentálja, a vészhelyzetben elérhetővé tett felhasználói fiókokról egységes nyilvántartást vezet, és a pénzügyi szervezet elvégzi a vészhelyzeti elérés megfelelőségének időszakos ellenőrzését.

5.4 Naplózási rend, a bejegyzések értékelése és az események kezelése

A pénzügyi szervezetnek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.[28]

A pénzügyi szervezet a kritikus rendszerei – ideértve az adathálózati eszközöket, az informatikai biztonsági- és egyéb felügyeleti rendszereket is – naplózási beállításait a rendszerek hozzáférési rend dokumentumaiban, a napló bejegyzések ellenőrzésének szabályait a naplózási rendjében előírja, és a naplózást megvalósítja az alábbiak szerint:

5.4.1 A pénzügyi szervezet, üzemeltetési, informatikai biztonsági és üzleti területe együttesen meghatározzák, hogy az informatikai üzemeltetési infrastruktúra és az üzleti rendszerek területén melyek azok az informatikai biztonsági események, amelyeket észlelni szükséges, valamint meghatározza a detektálás alapját képező feltételeket.

5.4.2 A pénzügyi szervezet naplózási rendjében előírja az egyes napló állományok ellenőrzésének módját, gyakoriságát, időpontját, felelősét, a beszámolás módját, valamint meghatározza a felügyelni kívánt eseményeket, az értesítendők körét, az azonnali riasztás eseteit és módját.

5.4.3 A pénzügyi szervezet biztosítja az azonnali riasztást igénylő eseményekre az azonnali reagálás feltételeit.

5.4.4 A biztonsági incidensekről és a beavatkozásokról nyilvántartást vezet, ebben rögzíti azok lényeges tartalmát.

5.4.5 Megfontolja, és kockázatai arányában dönt a naplóbejegyzések központi gyűjtéséről, valamint dönt a bejegyzések központi operátori, illetve automatikus kiértékeléséről, a bevezetése során pedig tekintettel van az alábbiakra:

a) automatikus kiértékelés elindítását megelőzi teljes körű tesztelés, és a sikeres tesztelést követően elindított éles üzem bevezetéséig az operátori kiértékelés változatlan formában fennmarad.

5.5 Az adatok védelme távadatátvitel során

A pénzügyi intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről.[29]

A pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

A pénzügyi szervezet

[28] Bit. 65/A.§ (5) d), Bszt.12.§ (6) d), Mpt.77/A.§ (5) d), Öpt.40/C.§ (5) d), Korm.r.3.§ (2) d)
[29] Bit. 65/A.§ (5) e), Bszt.12.§ (6) e), Mpt.77/A.§ (5) e), Öpt.40/C.§ (5) e), Korm.r.3.§ (2) e)

5.5.1 bank-, értékpapír-, biztosítási-, pénztár- és üzleti titkok körébe tartozó adatot, távoli hálózaton – ideértve a bérelt vonalakkal kiépített magánhálózatokat is - csak rejtjelezett formában továbbít,

5.5.2 jelszavakat és egyéb személyi hitelesítő adatokat távoli hálózaton és lokális hálózaton is csak rejtjelezett formában továbbít,

5.5.3 kockázati szempontból gyenge pontoknak tekinti azokat a WIFI vezeték nélküli hálózatokat, amelyeken bank-, értékpapír-, biztosítási-, pénztár- és üzleti titkok körébe tartozó adatot továbbít, illetve amelyek a pénzügyi szervezet adathálózatára csatlakoznak,

5.5.4 kritikus tranzakciós állományok hálózati átvitele során kriptográfiai eljárással biztosítja az állomány sértetlenségének az ellenőrizhetőségét.

5.6 Az adathordozók kezelése

A pénzügyi intézménynek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodnia kell az adathordozók szabályozott és biztonságos kezeléséről.[30]

A megvalósítás során a pénzügyi szervezet számára az alábbiak figyelembe vétele javasolt:

5.6.1 A pénzügyi szervezet megfontolja és kockázatai alapján döntést hoz:

a) az adathordozók kezelésére vonatkozó önálló szabályozási dokumentum elkészítéséről,
b) az adathordozók egyedi nyilvántartásának a bevezetéséről.

5.6.2 Az adathordozók kezelése során betartja az adathordozón tárolt adatok bizalmassága szerinti biztonsági osztályra előírt kezelési előírásokat (lásd 3.5.3 fejezet).

5.6.3 Az adathordozó üzemből való kivonása esetén a bank-, értékpapír-, biztosítási-, pénztár- és üzleti titkot tartalmazó adatokat az adathordozókon visszaállíthatatlan módon törli, az adathordozót olvashatatlanná teszi, megsemmisíti, illetve szolgáltatóval megsemmisítteti.

5.7 Vírusvédelem

A pénzügyi szervezetnek a biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell a rendszer biztonsági kockázattal arányos vírus- ***és más rosszindulatú program elleni*** *védelméről.*[31]

A vírusvédelem kialakításának javasolt szempontjai:

5.7.1 A pénzügyi szervezet informatikai rendszer elemein olyan integrált végponti biztonsági programot működtet, amely alkalmas a vírusok és egyéb kártékony kódok kiszűrésére, valamint biztosítja a program naprakész állapotát, valamint naplózását. Olyan beállítások mellett üzemelteti a szoftvert, amelyek biztosítják az automatikus frissítés, valamint a teljes

[30] Bit. 65/A.§ (5) f), Bszt.12.§ (6) f), Mpt.77/A.§ (5) f), Öpt.40/C.§ (5) f), Korm.r.3.§ (2) f)
[31] Bit. 65/A.§ (5) g), Bszt.12.§ (6) g), Mpt.77/A.§ (5) g), Öpt.40/C.§ (5) g), Korm.r.3.§ (2) g)

ellenőrzések (full scan) rendszeres időszakonként – de legalább heti egy alkalommal – történő elvégzését.

5.7.2 A pénzügyi szervezet központi kezelő felülettel rendelkező végponti biztonsági programot működtet.

6 Az informatikai rendszer funkcionális alkalmasságának a követelménye

A pénzügyi szervezetnek tevékenysége ellátásához, nyilvántartásai naprakész- és biztonságos vezetéséhez rendelkeznie kell a szolgáltatások ellátásához szükséges informatikai rendszerrel. Szoftvereinek együttesen alkalmasnak kell lenniük legalább a működéshez szükséges, és jogszabályban előírt adatok nyilvántartására, üzleti működésük adatainak a pénzügyi szervezet tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra, a tárolt adatok ellenőrzésére, valamint a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.[32]

A követelmények javasolt teljesítése

6.1.1 A pénzügyi szervezet alkalmazási rendszerei eleget tesznek a vonatkozó pénzügyi-számviteli jogszabályi előírásoknak, kiemelve, hogy

a) a pénzügyi tranzakciókat idősorosan vezetik, és lezárt tranzakciók utólagos módosítását nem engedélyezik,
b) az üzleti és a biztonsággal kapcsolatos tranzakciókat egyaránt naplózzák,
c) belső jogosultsági rendszerük lehetővé teszi a pénzügyi műveleteknek szerepkörök szerinti megosztását, az összeférhetetlen szerepkörök elkülönítését, ideértve a biztonsági adminisztrációs és az üzleti műveletek elkülönítését is.

6.1.2 A pénzügyi szervezet az informatikai rendszerét időben felkészíti az országos rendszerek valamint a jogszabályi előírások változásaira, az üzleti igények teljesítésére, és a továbbfejlesztések során már a tervezés fázisában kitér a technológiai továbblépés lehetőségeire, valamint figyelembe veszi az informatikai biztonság – ideértve az üzletfolytonosság – követelményeit is.

[32] Bit. 65/A.§ (8), Bszt.12.§ (10), Mpt.77/A.§ (8), Öpt.40/C.§ (8), Korm.r.4.§ (2)

I. Melléklet

Az egyes jogszabályi kontroll követelményekkel érintett COBIT, illetve MSZ ISO/IEC 27001:2006 fejezetek.

Jogszabályi kontroll követelmény	**Szakterület és folyamat megnevezése** **COBIT 4.0**	**Folyamat megnevezése** **COBIT 5.0**	**Témakör megnevezése** **MSZ ISO/IEC 27001:2006**
Bit. 65/A.§ (1), Bszt.12.§ (1) (2), Mpt.77/A.§ (1), Öpt.40/C.§ (1), Korm.r.2.§ (1) A pénzügyi intézménynek ki kell alakítania a tevékenysége ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben meg kell határozni az információtechnológiával szemben támasztott követelményeket, a használatából adódó biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokat az informatikai vállalatirányítás, a tervezés, a fejlesztés és a beszerzés, valamint az üzemeltetés, a monitorozás és a független ellenőrzés területén.	**PO – Tervezés és szervezet** PO 6 – Tájékoztatás a vezetői célokról és irányról **AI – Beszerzés és bevezetés** AI 1 – Automatizált megoldások meghatározása **ME – Figyelemmel kísérés és értékelés** ME3 - Külső követelményeknek való megfelelés biztosítása	 APO01, APO007 BAI02 MEA03	 5.1, 5.2.2, A.5, A.6, A.8 --- 6., A.15.1, A.15.3
Bit.65/A.§ (2), Bszt.12.§ (3), Mpt.77/A.§ (2), Öpt.40/C.§ (2), Korm.r. 2.§ (2) A pénzügyi intézmény köteles az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétévente felülvizsgálni és aktualizálni.	**PO – Tervezés és szervezet** PO 9 – Az informatikai kockázatok felmérése és kezelése	 EDM03, APO01, APO12	 4.2.1-3, 4.3, 5.1, A.5, A.6
Bit.65/A.§ (3), Bszt.12.§ (4), Mpt.77/A.§ (3), Öpt.40/C.§ (3), Korm.r. 2.§ (3) Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével meg kell határozni a szervezeti és működési rendeket, a felelősségi, nyilvántartási és tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.	**PO – Tervezés és szervezet** PO 4 – Az informatikai folyamatok, szervezet és a kapcsolatok meghatározása	 APO01, APO07, APO11	 5.1, 5.2.2, A.5, A.6, A.8, 7.8

	PO 7 – Az informatikai humán erőforrások kezelése	APO07	5.2.2, A.8
Bit.65/A.§ (4), Bszt.12.§ (5), Mpt.77/A.§ (4), Öpt.40/C.§ (4), Korm.r. 3.§ (1) A pénzügyi intézménynek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működtetnie kell.	**ME – Figyelemmel kísérés és értékelés**		
	M E1 – Az informatika teljesítményének figyelemmel kísérése és értékelése	MEA01	4.2.3, 4.2.4, 7.
	ME 2 – A Belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése	MEA02	4.2.3, 6., A.15.2
	M E3 – Külső követelményeknek való megfelelés biztosítása	MEA03	6., A.15.1, A.15.3
	M E4 – Az informatikai irányítás biztosítása	EDM01-04, MEA02	5.1, A.5, 7., 8., 4.2.1-3, 4.3, 5.2, A.6
Bit.65/A.§ (5), Bszt.12.§ (6), Mpt.77/A.§ (5), Öpt.40/C.§ (5), Korm.r. 3.§ (2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról: a) a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról,	**DS – Informatikai szolgáltatás és támogatás**		
	DS 9 – Konfigurációkezelés	BAI10	---
b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljes körűségét biztosító ellenőrzésekről, eljárásokról,	**DS – Informatikai szolgáltatás és támogatás**		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 12 – A fizikai környezet biztosítása	DSS01, DSS05	az egész sztenderd, 4.2.2
	ME – Figyelemmel kísérés és értékelés		
	ME 2 – A belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése	MEA02	4.2.3, 6., A.15.2

c) a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események),	**DS – Informatikai szolgáltatás és támogatás**		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 7 – Felhasználók oktatása és képzése	APO07	5.2.2, A.8
	DS 8 – A rendkívüli események kezelése és a felhasználói támogatás működtetése	DSS02	A.13
d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére,	**AI – Beszerzés és bevezetés**		
	AI 2 **–** Alkalmazási szoftverek beszerzése és karbantartása	BAI03	A.12
	AI 3 **–** Technológiai infrastuktúra beszerzése és karbantartása	BAI03	A.12
	AI 4 –Az üzemeltetés és a használat támogatása	BAI05, BAI08	4.3
	DS – Informatikai szolgáltatás és támogatás		
	DS13 – Üzemeltetés irányítása	DSS01, DSS05, BAI09	az egész sztenderd, 4.2.2, A.7
e) a távadat-átvitel bizalmasságáról, sértetlenségéről és hitelességéről,	**DS – Informatikai szolgáltatás és támogatás**		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
f) az adathordozók szabályozott és biztonságos kezeléséről,	**DS – Informatikai szolgáltatás és támogatás**		

	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
g) a rendszer biztonsági kockázattal arányos vírusvédelméről.	**DS – Informatikai szolgáltatás és támogatás**		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 9 – Konfigurációkezelés	BAI10, DSS02	A.13
Bit. 65/A.§ (6), Bszt.12.§ (7), Mpt.77/A.§ (6), Öpt.40/C.§ (6), Korm.r.3.§ (3) A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:			
a) informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel,	**PO – Tervezés és szervezet**		
	PO1 – Informatikai stratégiai terv kidolgozása	APO02, APO05, EDM02	4.2.1, 7., 8.
	PO2 – Információ-architektúra meghatározása	APO01, APO03	5.1, A.5, A.6
	PO 3 – Technológiai irány kijelölése	APO02, APO04, EDM01	4.2.1, 5.1, A.5
	PO5 – Informatikai beruházások irányítása	APO06, APO05	---
	PO 10 – Projektek irányítása	BAI01	---
	DS – Informatikai szolgáltatás és támogatás		
	DS 13 – Üzemeltetés Irányítása	DSS01, DSS05, BAI09	az egész sztenderd, 4.2.2, A.7
	DS 6 – Költségek azonosítása és felosztása	APO06	---
b) minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy	**PO – Tervezés és szervezet**		

közvetve támogató informatikai rendszerek folyamatos és biztonságos működését - még a szállító, illetőleg a rendszerfejlesztő tevékenységének megszűnése után is - biztosítja,	PO 8 Minőségirányítás	APO11	7., 8.
	AI – Beszerzés és bevezetés		
	AI5 – Az informatikai erőforrások beszerzése	BAI03, APO10	A.12, A.6.2
	DS – Informatikai szolgáltatás és támogatás		
	DS 2 – Külső szolgáltatások igénybevételének irányítása	APO10	A.6.2
	DS 3 – Teljesítmény- és kapacitáskezelés	BAI04	---
c) a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb - a tevékenységek, illetve szolgáltatások folytonosságát biztosító - megoldásokkal,	**PO – Tervezés és szervezet**		
	PO 1– Informatikai stratégiai terv meghatározása	EDM02, APO02, APO05	4.2.1, 7., 8.
	PO 2– Információ-architektúra meghatározása	APO01, APO02, APO03	4.2.1, 5.1, A.5, A.6
	PO 5– Informatikai beruházások kezelése	APO06	---
	DS – Informatikai szolgáltatás és támogatás		
	DS 1– Szolgáltatási szintek meghatározása és betartása	APO09	---
	DS 3 – Teljesítmény- és kapacitáskezelés	BAI04	---
	DS 4 – A szolgáltatás folyamatosságának biztosítása	DSS04	4.2.4, 4.3, 8., A.14
	DS 10 – Problémakezelés	DSS03	---
d) olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását,	**AI – Beszerzés és bevezetés**		
	AI 7 – Megoldások és változtatások üzembe helyezése és bevizsgálása	BAI05, BAI07	---

	AI 6 – Változások kezelése	BAI06	---
e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. **Korm.r.3§ (4), Tpt.12.§ (8):** Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről,	**DS – Informatikai szolgáltatás és támogatás**		
	DS 4 – A szolgáltatás folyamatosságának biztosítása	DSS04	4.2.4, 4.3.8, A.14
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
f) jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizzék,	**DS – Informatikai szolgáltatás és támogatás**		
	DS 4 – A szolgáltatás folyamatosságának biztosítása	DSS04	4.2.4, 4.3, 8., A.14
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
g) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.	**DS – Informatikai szolgáltatás és támogatás**		
	DS1 – Szolgáltatási szintek meghatározása és betartása	APO09	---
	DS 4 – A szolgáltatás folyamatosságának biztosítása	DSS04	4.2.4, 4.3, 8., A.14
	DS 10 – Problémakezelés	DSS03	---
Bit. 65/A.§ (7), Bszt.12.§ (9), Mpt.77/A.§ (7), Öpt.40/C.§ (7) a), Korm.r.4§ (1) A pénzügyi intézménynél mindenkor rendelkezésre kell állnia:			
a) az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek,	**PO – Tervezés és szervezet**		
	PO 2– Információ-architektúra meghatározása	APO01, APO03	5.1, A.5, A.6

	PO 8– Minőségirányítás	APO11	7., 8.
	AI – Beszerzés és bevezetés		
	AI 1 – Automatizált megoldások meghatározása	BAI02	---
	AI 2 – Alkalmazási szoftverek beszerzése és karbantartása	BAI03	A.12
	AI 4 – Az üzemeltetés és használat támogatása	BAI05, BAI08	4.3
b) az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének,	**PO – Tervezés és szervezet**		
	PO 2 – Információ-Architektúra Meghatározása	APO01, APO03	5.1, A.5, A.6
	AI – Beszerzés és bevezetés		
	AI 1 – Automatizált megoldások meghatározása	BAI02	---
	AI 2 – Alkalmazási szoftverek beszerzése és karbantartása	BAI03	A.12
c) az informatikai rendszer elemeinek a pénzügyi intézmény által meghatározott biztonsági osztályokba sorolási rendszerének,	**PO – Tervezés és szervezet**		
	PO 2 – Információ-architektúra meghatározása	APO01, APO03	5.1, A.5, A.6
	DS – Informatikai szolgáltatás és támogatás		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
d) az adatokhoz történő hozzáférési rend meghatározásának,	**PO – Tervezés és szervezet**		
	PO 2 – Információ-architektúra meghatározása	APO01, APO03	5.1, A.5, A.6

	PO 4 – Az informatikai folyamatok, szervezet és kapcsolatok meghatározása	APO01, APO07	5.1, 5.2.2, A.5, A.6, A.8
	DS – Informatikai szolgáltatás és támogatás		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
e) az adatgazda és a rendszergazda kijelölését tartalmazó okiratnak,	**PO – Tervezés és szervezet**		
	PO 4 – Az informatikai folyamatok, szervezet és kapcsolatok meghatározása	APO01, APO07	5.1, 5.2.2, A.5, A.6, A.8
	PO7 – Az informatikai humán erőforrások kezelése	APO07	5.2.2, A.8
f) az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek,	**PO – Tervezés és szervezet**		
	PO 6 – Tájékoztatás a vezetői célokról és irányról	APO01, APO007	5.1, 5.2.2, A.5, A.6, A.8
	DS – Informatikai szolgáltatás és támogatás		
	DS 9 – Konfigurációkezelés	BAI01, DSS02	A.13
g) az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.	**DS – Informatikai szolgáltatás és támogatás**		
	DS 9 – Konfigurációkezelés	BAI01, DSS02	A.13
Bit. 65/A.§ (8), Bszt.12.§ (10), Mpt.77/A.§ (8), Öpt.40/C.§ (8), Korm.r.4.§ (2) A szoftvereknek együttesen alkalmasnak kell lenni legalább:			
a) a működéshez szükséges és jogszabályban előírt adatok nyilvántartására,	**PO – Tervezés és szervezet**		
	PO 1– Informatikai stratégiai terv meghatározása	EDM02, APO02, APO05	4.2.1, 7., 8.

	PO 8 Minőségirányítás	APO11	7., 8.
	AI – Beszerzés és bevezetés		
	AI 7 – A megoldások és változtatások üzembe helyezése és bevizsgálása	BAI05, BAI07	---
	DS – Informatikai szolgáltatás és támogatás		
	DS 1– Szolgáltatási szintek meghatározása és betartása	APO09	---
	ME – Figyelemmel kísérés és értékelés		
	ME3 - Külső követelményeknek való megfelelés biztosítása	MEA03	6., A.15.1, A.15.3
b) a pénz és az értékpapírok biztonságos nyilvántartására,	**DS – Informatikai szolgáltatás és támogatás**		
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
c) a pénzügyi intézmény tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra,	**AI – Beszerzés és bevezetés**		
	AI 2 – Alkalmazási szoftverek beszerzése és karbantartása	BAI03	A.12
	DS – Informatikai szolgáltatás és támogatás		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
d) a tárolt adatok ellenőrzéséhez való felhasználására	**AI – Beszerzés és Bevezetés**		
	AI 2 – Alkalmazási szoftverek beszerzése és karbantartása	BAI03	A.12

	DS – Informatikai szolgáltatás és támogatás		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
e) a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére	**AI – Beszerzés és bevezetés**		
	AI 2 – Alkalmazási szoftverek beszerzése és karbantartása	BAI03	A.12
.	**DS – Informatikai szolgáltatás és támogatás**		
	DS 5 – A rendszerek biztonságának megvalósítása	APO13, DSS02, DSS05	az egész sztenderd, A.13
	DS 11 – Adatok kezelése	DSS01, DSS04, DSS05, DSS06	az egész sztenderd, 4.2.2-4, 4.3, 8. A.14
Bit. 65/A.§ (9), Bszt.12.§ (11), Mpt.77/A.§ (9), Öpt.40/C.§ (9), Korm.r.5.§	**PO – Tervezés és szervezet**		
A pénzügyi intézménynek belső szabályzatában meg kell határoznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.	PO 7 – Az informatikai humán erőforrások kezelése	APO07	5.22, A.8