PÉNZÜGYI SZERVEZETEK
ÁLLAMI FELÜGYELETE
HUNGARIAN FINANCIAL
SUPERVISORY AUTHORITY

A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről

Budapest, 2007. október

TARTALOMJEGYZÉK

1. A MÓDSZERTANI ÚTMUTATÓ KIADÁSÁNAK CÉLJA

Jelen módszertani útmutató kiadásával a Pénzügyi Szervezetek Állami Felügyelete a szakági törvények (Hpt., Tpt., Mpt., Öpt., Bit) alapján működő pénzügyi intézmények informatikai rendszerének védelmének erősítését szeretné elősegíteni. Ezen belül különösen:

- a pénzügyi intézmények által a törvényi előírásoknak való minél magasabb színvonalú megfelelés elősegítését, valamint
- a pénzügyi intézmények és a Felügyelet közötti egységes értelmezés és szemléletmód kialakítását;

azáltal, hogy

- rámutat az informatikai biztonság és az informatikairányítás színvonala között fennálló szoros kapcsolatra, továbbá
- szorgalmazza a COBIT (Control Objectives for Information and related Technology) informatikairányítási eszköz hazai elterjedését.

A jelen módszertani útmutatóban a „COBIT" hivatkozások a COBIT 3. verziójára vonatkoznak és egyelőre nem a legújabb COBIT 4.0-ra vonatkozó hivatkozásokat tartalmazza. A módszertani útmutatóban foglalt elvárások követése a pénzügyi intézmények és az ügyfeleik alapvető érdekeit szolgálja, ezért az azokhoz való igazodást a Felügyelet ellenőrzései során megvizsgálja és a lényeges eltéréseket figyelembe veszi az egyes szervezetek tevékenységének értékelésekor.

2. A MÓDSZERTANI ÚTMUTATÓ FELHASZNÁLÓINAK KÖRE

A pénzügyi intézményeknél

- az informatika bármely területéért felelős vezetők,
- az informatikai biztonsággal foglalkozó szakemberek,
- a működési kockázatok elemzésével foglalkozó szakemberek,
- informatikai auditorok,
- informatikusok,
- az informatikai rendszerek felhasználói.

.

3. KAPCSOLÓDÓ JOGSZABÁLYOK

A 2004. évi törvénymódosítások nyomán

- az 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Hpt.),
- az 1997. évi LXXXII. törvény a magánnyugdíjról és a magánnyugdíjpénztárakról (Mpt.),
- az 1993. évi XCVI. törvény az Önkéntes Kölcsönös Biztosító Pénztárakról (Öpt.) és
- az 2001. évi CXX. törvény a tőkepiacról (Tpt.) (a továbbiakban összefoglalóan ágazati törvények)

a pénzügyi szervezetek informatikai rendszerének védelme tekintetében lényegében azonos[1] előírásokat tartalmaz. A biztosítókról és a biztosítási tevékenységről szóló 2003. évi LX. törvény (Bit.) egyelőre még nem fogalmaz meg hasonló értelmű előírásokat a biztosítási szektor vonatkozásában, de a kodifikációt a Pénzügyi Szervezetek Állami Felügyelete már kezdeményezte és a jelen útmutatóban leírtak követését hasznosnak tartja.

A befektetési és az árutőzsdei szolgáltatási tevékenység, az értékpapír letéti őrzés, az értékpapír letétkezelés, valamint az elszámolóházi tevékenység végzéséhez szükséges személyi, tárgyi, technikai és biztonsági feltételekről szóló 283/2001. (XII. 26.) kormányrendelet előírásait a hatálya alá tartozó intézményeknek a 2004. évi jogszabály módosításokat követően is alkalmazniuk kell.

[1] Néhány kisebb eltérés létezik ugyan, de az a jelen módszertani útmutató tartalmát nem érinti.

4. AZ ALKALMAZÁS IDŐPONTJA

A 2004. évi törvénymódosítások nyomán beiktatott jogszabályi előírások kötelező alkalmazásának kezdőnapját az alábbi táblázat mutatja:

Törvény	Informatikai rendszer védelme című paragrafus száma	A törvényi előírás kötelező alkalmazásának kezdőnapja
1996. évi CXII. törvény (Hpt.)	13/B. § Beiktatta: 2004. évi XXII. tv.	**2005. november 1. napjától** kell alkalmazni azon **pénzügyi intézmény** esetében, amely **nem tartozott** a befektetési és az árutőzsdei szolgáltatási tevékenység, az értékpapír letéti őrzés, az értékpapír letétkezelés, valamint az elszámolóházi tevékenység végzéséhez szükséges személyi, tárgyi, technikai és biztonsági feltételekről szóló **283/2001. (XII. 26.) Korm. rendelet hatálya alá** és e törvény hatálybalépésekor már működött, illetve a törvény hatálybalépését megelőzően érvényesen nyújtotta be alapítási engedély iránti kérelmét. 2004.05.06-án már működő, a befektetési és az árutőzsdei szolgáltatási tevékenység, az értékpapír letéti őrzés, az értékpapír letétkezelés, valamint az elszámolóházi tevékenység végzéséhez szükséges személyi, tárgyi, technikai és biztonsági feltételekről szóló **283/2001. (XII. 26.) Korm. rendelet hatálya alá tartozó pénzügyi intézménynek legkésőbb 2005. január 1-jétől** kell megfelelnie a Hpt. 13/B. §-ában foglaltaknak.
1997. évi LXXXII. törvény (Mpt.)	77/A. § Beiktatta: 2004. évi CI. tv.	2006.01.01.
1993. évi XCVI. törvény (Öpt.)	40/C. § Beiktatta: 2004. évi CI. tv.	2006.01.01.
2001. évi CXX. törvény (Tpt.)	101/A. § Beiktatta: 2004. évi XXII. tv.	2004.05.06-án már működő, a befektetési és az árutőzsdei szolgáltatási tevékenység, az értékpapír letéti őrzés, az értékpapír letétkezelés, valamint az elszámolóházi tevékenység végzéséhez szükséges személyi, tárgyi, technikai és biztonsági feltételekről szóló **283/2001. (XII. 26.) Korm. rendelet hatálya alá tartozó szolgáltatónak**, elszámolóházi tevékenységet végző szervezetnek legkésőbb **2005. január 1-jétől** kell megfelelnie a Tpt. 101/A. §-ában foglaltaknak.

A módszertani útmutatóban foglaltak követése a jelen útmutató kiadásának napjától kezdődően javasolt.

5. HATÁLY

A módszertani útmutató a Hpt., a Tpt., az Mpt. és az Öpt. hatálya alá tartozó pénzügyi szervezeteknél működtetett informatikai rendszerekre terjed ki. A jelen módszertani útmutató kiadásával a 3/2005. évi módszertani útmutató hatályát veszti.

A Bit 65. §. b) pontjában leírtak szerint: „A biztosítási tevékenység engedélyezésének és a tevékenység folytatásának feltétele: *b)* a folyamatos nyilvántartási, adatfeldolgozási és adatszolgáltatási rendszer kiépítése, illetve a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv" valamint a Bit. 66. §. (1) a) pontja szerint a biztosítónak képesnek kell lennie a "működés megkezdéséhez szükséges személyi és tárgyi feltételek biztosítására". Bár a Bit. nem rendelkezik részletesen a fentiek megvalósításának feltételeiről, azonban a fentiek teljesítése érdekében az alábbi témakörökre vonatkozó javaslatokat fogalmazunk meg.

Annak ellenére, hogy a biztosítási szektorra a témában nincsenek kötelező érvényű jogszabályi előírások, a Felügyelet a Bit. hatálya alá tartozó intézmények számára is javasolja az útmutatóban leírt, az informatikai rendszerek védelmében kapcsolatos felügyeleti elvárások követését.

6. AZ INFORMATIKAI BIZTONSÁG ÉS AZ INFORMATIKAIRÁNYÍTÁS KAPCSOLATA

A globalizálódó világban az új információ-technológiai lehetőségek az informatikai biztonságot veszélyeztető, korábban nem ismert működési kockázatok megjelenésével párosulnak. Nem vezet eredményre, ha az informatikai biztonságot csupán különböző *biztonsági* intézkedések életbe léptetésével vagy valamely *biztonsági* szabvány adaptálásával kívánjuk megteremteni. Az üzleti célkitűzéseket szolgáló, gazdaságos informatikai biztonság sokkal inkább a nemzetközileg elismert *informatikairányítási* gyakorlat alkalmazásával érhető el, amely szem előtt tartja az informatikai rendszerek szabályszerű, kontrollált és biztonságos fejlesztését, fenntartását és üzemeltetését.

7. A COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY) NYÍLT SZABVÁNY

Az *informatikairányítás* világszerte egyre szélesebb körben elismert *eszköze*, egyben nyílt szabványa a COBIT, amely rendszerbe foglalja az információ, az információ technológia és az ezzel kapcsolatos kockázatok kontrollálására alkalmas gyakorlatot. Hasznosítja az informatikairányítás korábbi eredményeit, ugyanakkor épít a korszerű vállalatirányítási módszerekre is. Hangsúlyozza, hogy az informatikának az üzleti célkitűzéseket kell szolgálnia. A COBIT alkalmazásával az üzleti területi vezetők, a működési kockázatokkal foglalkozó szakemberek, az informatikusok és az auditorok egységes szemléletben, közös fogalmi rendszert használva, hatékonyan tudnak együttműködni. Ezek az ismérvek a COBIT-ot kifejezetten érdemessé teszik a pénzügyi intézményekben való alkalmazásra. A pénzügyi intézmény informatikai rendszerének védelmére vonatkozó törvényi előírások és a COBIT megfeleltetését az I. sz. melléklet tartalmazza. A megfeleltetés a két anyag között természetesen – keletkezésük, készítőik, céljuk, felhasználási körük stb. különbözősége miatt – nem lehet teljesen egyértelmű és megfellebbezhetetlen, de célja mindenképpen a jogszabálynak a nemzetközi gyakorlat alapján kialakított és karbantartott COBIT szabványhoz való igazítása és annak teljes lefedése. A nem egyértelmű megfeleltetés következtében tehát a COBIT bizonyos fejezetei több jogszabályi pontnál is megjelennek.

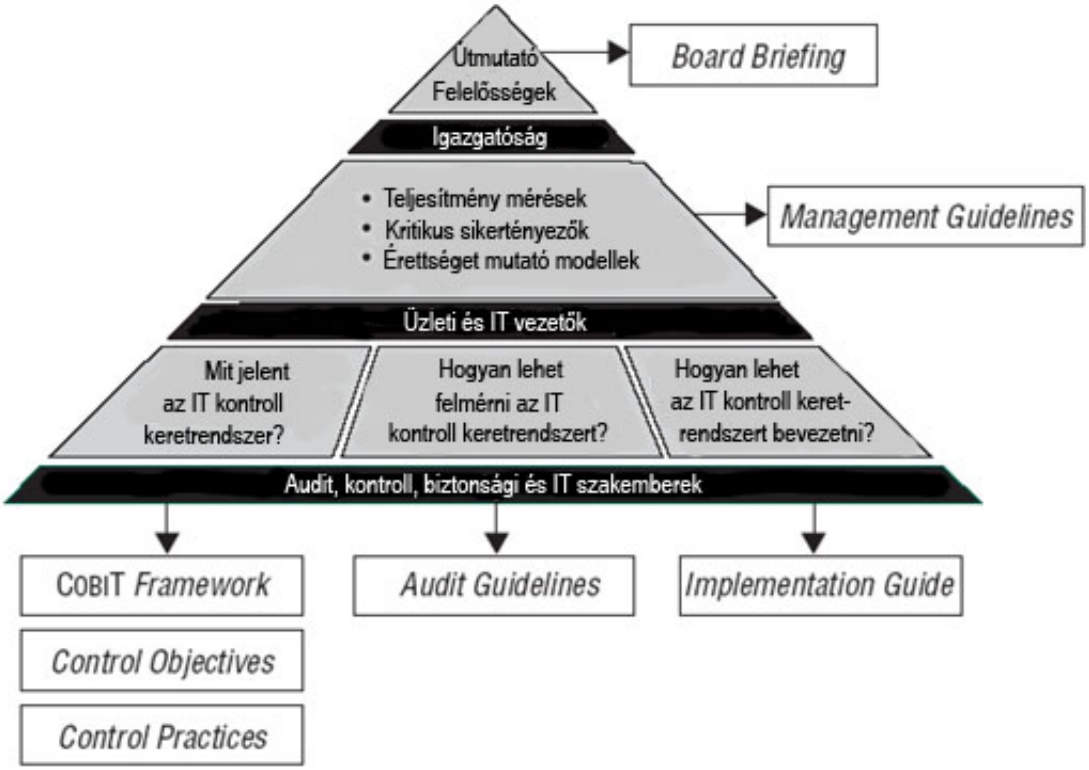
7.1 A COBIT TÖRTÉNETE

A szabványban megtestesülő kutatások motorja a világszerte kb. 35000 tagot számláló ISACA (Information Systems Audit and Control Association), amelynek társintézménye, a COBIT-ot kiadó IT Governance Institute (USA) 1998-ban alakult. Eddig három COBIT kiadás jelent meg: 1996-ban, 1998-ban és 2000-ben. Folyamatosan továbbfejlesztik. 2003-ban megjelent egy internetes változata, továbbá egy egyszerűsített, bevezető verzió is. A COBIT növekvő nemzetközi elfogadottságához jelentősen hozzájárul részletesen kidolgozott auditálási módszertana is. A Felügyelet informatikai

ellenőrei az ISACA tagjai és már több éve COBIT szemléletben végzik a pénzügyi szervezetek informatikai rendszerének vizsgálatát és erre épül a jelenleg használt vizsgálati módszertanuk is.

7.2 A COBIT KÉZIKÖNYVEK ÁTTEKINTÉSE

Az informatikairányítás és ennek eszköze, a COBIT ma már tekintélyes számú szakkönyvben van dokumentálva. Az alábbi ábra[2] az alapkönyvek közötti eligazodást segíti elő.



A COBIT kézikönyvek témacsoportokra bontását és elérhetőségét a II. sz. melléklet tartalmazza.

[2] Forrás: COBIT Security Baseline (Copyright © 2004 IT Governance Institute)

8. A JOGSZABÁLYI ELŐÍRÁSOK ÉRTELMEZÉSE ÉS A KAPCSOLÓDÓ FELÜGYELETI ELVÁRÁSOK

Az alábbiakban a törvényi előírások egyes pontjait érintve további értelmező megjegyzéseket, javaslatokat teszünk, azonban hangsúlyozzuk, hogy **legfőbb célunk a rendszeresen karbantartott és az informatikairányítás gyakorlatában bevált eljárásokat és módszereket leíró COBIT módszertan használatának elősegítése**, amelynek egyes részei már magyar nyelven is elérhetők (pl. http://www.isaca.hu). A jogszabályi előírások egyes kiemelt részeinek magyarázatát az eddig felmerült kérdések megválaszolására koncentráltuk és a jogszabály egyes pontjaiban használt rövidítések magyarázatát a III. számú mellékletben soroltuk fel.

Az informatikai rendszer védelme minden esetben a pénzügyi intézmény vezetésének a felelőssége és ez a felelősség nem átháríthatő (azonban megfelelő körülmények biztosítása esetén delegálható). A pénzügyi intézmény külső szervezeteket is megbízhat (pl.: kiszervezés keretében) a védelmi rendszer kialakításával, működtetésével és a működés ellenőrzésével, de a teljes kontrollkörnyezet megfelelőségének biztosítása ez esetben is a vezetőség feladata marad.

1. Mpt. 77/A. § (1) bekezdés, Öpt. 40/C. § (1) bekezdés, Tpt. 101/A. § (1) bekezdés, Hpt. 13/B. § (1) bekezdés

A pénzügyi szervezetnek ki kell alakítania a tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.

A „szabályozási rendszer”-el kapcsolatban a Felügyelet javasolja a pénzügyi intézménynek, hogy készítse el és folyamatosan aktualizálja az informatikára vonatkozó legfőbb szabályozásokat. A Felügyelet javasolja továbbá, hogy a pénzügyi intézmény alakítsa ki a szabályozási rendszer hierarchiáját, amelyhez a Felügyelet célszerűnek tartja az „irányelvek – szabályzatok – eljárásrendek” hármas tagozódási struktúra követését. A szabályozások mennyiségére, formai követelményeire vonatkozóan nincsenek elvárások, azonban a szabályozások és a napi gyakorlatban végrehajtott feladatok összhangját biztosítani kell. A szabályozási rendszerből ki kell derülnie, a szabályozások hatályba léptetésének ideje (módosított szabályzat érvénybeléptetési ideje), aktualizáltságának foka, hatókörének és megismertetésének mértéke. A szabályozási rendszer tartalmazza legalább az Informatika biztonsági politikát, az Informatika biztonsági szabályozást, az informatikai rendszerek üzemeltetési rendjét, a Hozzáférések- és jogosultságok kezelését, a Vírusvédelmi szabályozást, a Mentések- és archiválások rendjét, a Kockázatok elemzésének és kezelésének módszerét (dokumentált módszertant, amely alapján a kockázatelemzést elvégzik), a Változások kezelését, a szabályzatok készítésének és kiadásának menetét, formai követelményét, illetve az alkalmazottak általi elérhetőség és megismertetés követelményeit.

Az „irányelveket – szabályzatokat – eljárásrendeket” rendszeresen, évente legalább egyszer, vagy az üzleti, illetve a működési környezetben történt jelentős változások esetén felül kell vizsgálnia a pénzügyi intézmény vezetésének és szükség esetén módosítani kell azokat. A vezetésnek emellett figyelemmel kell kísérnie azt is, hogy időszerűek-e az alkalmazott irányelvek, és ki kell alakítani egy megfelelő rendszert és eljárást a normák, alapelvek, célkitűzések, irányelvek és eljárások időszakos felülvizsgálatára és jóváhagyására vonatkozóan.

Minden informatikai felhasználóval meg kell ismertetni a rá vonatkozó informatikához kapcsolódó biztonsági szabályokat, és gondoskodni kell arról, hogy minden felhasználó teljes mértékben megértse a biztonsági szabályok fontosságát. Az oktatásnak azt az üzenetet kell közvetítenie, hogy az informatika biztonsága a pénzügyi intézmény egészének, vagyis minden dolgozónak közös érde-

ke, amelyért mindenki felelős.

Az „információ technológiával szemben támasztott követelmények” értelmezésében a Felügyelet javasolja, a már a bevezetőben említett COBIT kézikönyvek, illetve a jelen módszertani útmutatóban megfogalmazottak figyelembe vételét. Az informatikai rendszerek menedzselése érdekében kontroll környezetét a pénzügyi intézmény a jogszabály által hivatkozott, a COBIT alapját képező - és a jogszabályban is nevesített - főbb területekre vonatkozóan alakítsa ki.

Kiszervezés esetén a szabályzatok elkészítése, módosítása a szerződésben rögzítettek szerint történik (vagy a pénzügyi intézmény, vagy a szolgáltató végzi), de mindkét félnek gondoskodnia kell a releváns szabályzatok saját magánál történő érvénybe helyezéséről és a felhasználók megfelelő tájékoztatásáról.

A jogszabály ezen pontjának teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO6 - Vezetői célok és irányvonal közlése” , a „PO8 - Külső követelmények betartása” és az „AI1 – Automatizált megoldások meghatározása” fejezeteinek figyelembe vételét.

2. **Mpt. 77/A. § (2) bekezdés, Öpt. 40/C. § (2) bekezdés, Tpt. 101/A. § (2) bekezdés, Hpt. 13/B. § (2) bekezdés**

A pénzügyi szervezet köteles az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétévente felülvizsgálni és aktualizálni.

Az informatika biztonsági kockázatok kezelése érdekében javasolt egy olyan kockázatelemzési módszertan kiválasztása, amely az informatikai biztonsági kockázatok szisztematikus felmérését és menedzselését teszi lehetővé. A kockázatfelmérésnek, elemzésnek és menedzselésnek igazodnia kell a pénzügyi intézmény legkritikusabb üzleti folyamataihoz és ki kell terjednie a tervezés, a fejlesztés, a beszerzés, az üzemeltetés, a kiszervezés és az ellenőrzés területére is. A munkadokumentumok elkészítése és a menedzselt kockázatonként a védelmi intézkedések bemutatása fontos a kockázatfelmérés és elemzés megfelelőségének megítéléséhez. Kiszervezés esetén a kockázatelemzésnek minden olyan rendszerelemre ki kell terjedni a kiszervezési szolgáltatónál is, amely a szolgáltatáshoz kapcsolódik és e nélkül a szolgáltatás megfelelősége nem biztosítható.

A kockázatelemzési módszertan rendszeres elvégzését belső szabályozás szintjén fogalmazza meg és annak megfelelően járjon el (szabályzataiban dokumentálja a módszertant a megismerhetőség az ellenőrizhetőség és az újbóli végrehajthatóság miatt). A kockázatok felmérését és elemzését új rendszerek üzembe helyezését követően, a környezeti változásokat figyelembe véve, illetve előre meghatározott rendszerességgel (lehetőleg évente) hajtsa végre. A kockázatelemzést minden rendszerre (szoftver és hardver) el kell végezni.

A jogszabály ezen pontjának értelmezéséhez a Felügyelet célszerűnek tartja a COBIT „PO9 - Kockázatok értékelése” fejezetének alkalmazását.

3. **Mpt. 77/A. § (3) bekezdés, Öpt. 40/C. § (3) bekezdés, Tpt. 101/A. § (3) bekezdés, Hpt. 13/B. § (3) bekezdés**

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.

A „szervezeti működési rendek, a felelősségi, nyilvántartási és tájékoztatási szabályok”-kal kapcsolatban a Felügyelet javasolja az informatikai részleg szervezeti felépítésének és kapcsolatainak meghatározását, dokumentálását és folyamatos karbantartását (SZMSZ, szervezeti ábrák, munkaköri leírások, stb.). A személyek feladatait és felelősségi köreit világosan meg kell határozni és az összeférhetetlenséget el kell kerülni (lásd a IV. számú mellékletet). Szét kell választani a feladatokat és felelősségi köröket, olyan módon, hogy ne legyen lehetőség arra, hogy egyetlen személy kezében összpontosuljon valamely kritikus eljárás irányítása, végrehajtása és ellenőrzése, amely visszaélésre ad lehetőséget. A legfontosabb összeférhetetlenségi probléma a rendszergazdai, a fejlesztői és az üzemeltetői feladatkörök megfelelő elkülönítése és az un. szoftverkönyvtárosi kontroll funkció kialakítása az IT szervezetben. A vezetésnek gondoskodnia kell arról, hogy a szervezet minden alkalmazottja tisztában legyen az információs rendszerekkel kapcsolatos feladataival és felelősségével. Minden alkalmazottnak megfelelő hatáskört kell biztosítani ahhoz, hogy végre tudja hajtani a rá bízott feladatokat, és tájékoztatni kell arról, hogy milyen mértékű ellenőrzési és biztonsági felelősséggel tartozik.

A vezetésnek ki kell neveznie egy „informatika biztonsági felelőst”, aki a szervezet informatikai eszközeinek fizikai és logikai biztonságáért egyaránt felelős és közvetlenül a szervezet felső vezetőjének számol be munkájáról. A vezetésnek ki kell dolgoznia egy eljárást az adatok tulajdonosainak (adatgazda) és kezelőinek hivatalos kijelölésére vonatkozóan és gondoskodnia kell arról, hogy minden informatikai eszköznek (adatok és rendszerek) legyen egy kijelölt tulajdonosa (adatgazda), aki dönt az osztályozásról és hozzáférési jogosultsági szintekről. Az adatgazda a nyilvántartó rendszerek esetében nem informatikus, hanem egy felhasználó, aki általában a leginkább érintett funkcionális terület vezetője (számlavezetés, könyvelés, stb.). Az informatikai kiszolgáló alkalmazásoknak adatgazdája informatikus (Windows domain rendszer, Active Directory, adatátviteli hálózat vezérlő alkalmazás, naplógyűjtő és elemző alkalmazás stb.).

A szükséges dolgozói létszámot rendszeres időközönként felül kell vizsgálni annak érdekében, hogy helyettesítések esetére is megfelelő számú és a munkakörre előírt képzettségű dolgozóval rendelkezzen az informatikai részleg. A vezetésnek gondoskodnia kell az informatikai munkaköri leírások kidolgozásáról és rendszeres aktualizálásáról. A munkaköri leírásokban világosan rögzíteni kell mind a hatásköröket, mind a felelősségi köröket, beleértve az adott munkakör ellátásához szükséges képzettség és gyakorlat meghatározását is. A pénzügyi intézménynél a munkakörökhöz szükséges informatikai képzettség és gyakorlat meghatározását belső szabályzatban kell meghatározni, nem a munkaköri leírásokban.

Kiszervezés esetén a kiszervezési szolgáltatónak is meg kell felelnie a pénzügyi szervezetre vonatkozó törvényben foglaltaknak a kiszervezéssel érintett területeken.

A jogszabály ezen pontjának értelmezéséhez a Felügyelet célszerűnek tartja a COBIT „PO4 – Az informatikai részleg szervezeti felépítésének és kapcsolatainak meghatározása” és a „PO7 – Emberi erőforrások kezelése” fejezeteinek figyelembe vételét.

4. Mpt. 77/A. § (4) bekezdés, Öpt. 40/C. § (4) bekezdés, Tpt. 101/A. § (4) bekezdés, Hpt. 13/B. § (4) bekezdés

A pénzügyi szervezetnek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működtetnie kell.

Az informatikai ellenőrző rendszer alatt nem egy adott célalkalmazást kell érteni, hanem az informatikairányítás működését felügyelő kontrollkörnyezet kiépítettségét és működését, amelybe beletartoznak mindazon irányelvek, folyamatok, eljárások, gyakorlatok, napi rutinok, eszközök, emberi erőforrások és szervezeti struktúrák, amelyek ezt lehetővé teszik.

A vezetésnek mérnie kell (a külső és belső szolgáltatási szint megállapodásokban meghatáro-

zott teljesítménymutatók, illetve kritikus sikertényezők alapján) a kulcsalkalmazások terén az informatikai részleg által nyújtott szolgáltatásokat és össze kell hasonlítania azokat a tervezett szintekkel. Az informatikai részleg teljesítményét rendszeres jelleggel, folyamatosan értékelni kell. A vezetésnek rendszeres időközönként meg kell vizsgálnia, hogy a felhasználók milyen mértékben elégedettek az informatikai részleg szolgáltatásaival. Jelentéseket kell készíteni a vezetés számára a kitűzött szervezeti célok megvalósításának irányában történt előrelépések áttekintéséhez és a kockázatok csökkentése érdekében végrehajtott lépések megítéléséhez. Figyelemmel kell kísérni azt, hogy a belső ellenőrzési eljárások eredményesen működnek-e a szervezet szokásos eljárásrendjén belül. Az áttekintések alapján meg kell tenni a szükséges vezetői intézkedéseket és lépéseket.

A belső ellenőrzési eljárások akkor működnek eredményesen, ha a preventív kontrollok gyorsan felderítik és kijavítják a hibákat, ellentmondásokat, még mielőtt azok befolyásolnák a rendszer üzemszerű működését, illetve a szolgáltatásnyújtást.

Gondoskodni kell az üzemeltetési biztonság és a belső ellenőrzés rendszeres felülvizsgálatáról, és ennek kapcsán önértékelés vagy független ellenőrzés formájában meg kell vizsgálni, hogy a biztonsági és belsőellenőrzési eljárások a meghatározott, illetve alkalmazott biztonsági és belső ellenőrzési követelményeknek megfelelően működnek-e, vagy sem. A vezetésnek, felügyeleti feladatai keretében, fel kell tárnia a sebezhető pontokat és a biztonsági problémákat.

A kritikus fontosságú új informatikai szolgáltatások bevezetése előtt a vezetésnek független szakértői tanúsítást / hitelesítést / értékelést kell szereznie az érintett rendszerek biztonsági és belső ellenőrzési eljárásaira vonatkozóan. A szolgáltatás bevezetését követően rendszeres időközönként meg kell újítani a korábban szerzett szakértői tanúsítást / hitelesítést / értékelést. Külső szolgáltatók szolgáltatásainak igénybe vétele (kiszervezés) előtt a vezetésnek független szakértői tanúsítást / hitelesítést / értékelést kell szereznie az adott szolgáltató biztonsági és belső ellenőrzési eljárásairól. A szolgáltatás bevezetését követően rendszeres időközönként (az informatikai architektúra lényeges változásait követően) meg kell újítani a korábban szerzett szakértői tanúsítást / hitelesítést / értékelést. A független szakértő lehet a pénzügyi intézmény belső ellenőre is, ha rendelkezik mindazokkal a szakmai, műszaki, technikai ismeretekkel, képességekkel és tapasztalatokkal, amelyek az ilyen jellegű feladatok hatékony, eredményes ellátásához szükségesek.

A vezetésnek ki kell dolgoznia egy, az ellenőrzési területre vonatkozó szabályzatot, amelyben fel kell vázolni a feladatait, hatáskörét, beszámolási kötelezettségét és a számon kérhetőség módját. A szabályzatot rendszeres időközönként felül kell vizsgálni. Az ellenőrnek függetlennek kell lennie a vizsgált részlegtől (tényleges és érzékelt függetlenség), hogy objektív ellenőrzést tudjon végezni.

A jogszabály ezen pontjának értelmezéséhez a Felügyelet célszerűnek tartja a COBIT „M1 – Eljárások felügyelete”, az „M2 – Belső ellenőrzés megfelelőségének felmérése”, az „M3 – Független értékelés végeztetése” és az „M4 – Független audit elvégeztetése” fejezeteinek figyelembe vételét.

5. **Mpt. 77/A. § (5) bekezdés, Öpt. 40/C. § (5) bekezdés, Tpt. 101/A. § (5) bekezdés, Hpt. 13/B. § (5) bekezdés**

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az a)-g) pontokban meghatározottakról.

Az ágazati törvények hivatkozott paragrafusainak (2) bekezdésében említett kockázatelemzésre alapozva kell teljesíteni az e ponthoz tartozó előírásokat.

6. **Mpt. 77/A. § (5) bekezdés a) pont, Öpt. 40/C. § (5) bekezdés a) pont, Tpt. 101/A. § (5) bekezdés a) pont, Hpt. 13/B. § (5) bekezdés a) pont**

***A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon kell gondoskodni* a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról.**

Az informatikai eszközök és rendszerek (hardver és szoftver eszközök, a szervereken és munkaállomásokon lévő alkalmazások, rendszertechnikai és adatkapcsolati ábrák stb.) teljes körű és naprakész nyilvántartásának rendelkezésre kell állnia (ez az alapja a már említett kockázatelemzésnek). Az informatikai részleg vezetésének gondoskodnia kell arról, hogy a konfiguráció-nyilvántartás minden egyes tétel aktuális státuszát tartalmazza, a múltbeli változtatások jelzésével együtt. Nyomon kell követni a konfiguráció-elemek változásait is a változáskezelési szabályzatnak megfelelően (pl. új elemek, 'fejlesztés alatt', stb.). Megfelelő eljárások révén gondoskodni kell arról, hogy csak engedélyezett és azonosítható konfiguráció-elemek kerüljenek be beszerzéskor a (konfiguráció) leltárba és selejtezéskor (értékesítéskor) ki a leltárból. Rendszeresen ellenőrizni kell az informatikai részleg által vezetett konfiguráció-nyilvántartás meglétét és a bejegyzések konzisztenciáját. Például a szoftvereket nyilvántartásba kell venni és megfelelő engedéllyel kell rendelkezni használatukra vonatkozóan.

Kiszervezés esetén a kiszervezett szolgáltatónál is minden olyan eszközre ki kell terjedni a nyilvántartásnak, amely bármilyen módon érintve van az adott pénzügyi intézménynek végzett szolgáltatás kapcsán.

A jogszabály ezen pontjának értelmezéséhez a Felügyelet célszerűnek tartja a COBIT „DS9 – Konfiguráció kezelése" fejezetének figyelembe vételét.

7. **Mpt. 77/A. § (5) bekezdés b) pont, Öpt. 40/C. § (5) bekezdés b) pont, Tpt. 101/A. § (5) bekezdés b) pont, Hpt. 13/B. § (5) bekezdés b) pont**

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

Az informatikai rendszerek biztonsága kapcsán ügyelni kell arra, hogy a biztonsági intézkedések összhangban legyenek az üzleti/ szervezeti követelményekkel. Ez magában foglalja az IT kockázatelemzést, az informatikai biztonsági tervet; az informatikai biztonsági terv végrehajtását; az informatikai biztonsági terv aktualizálását az informatikai konfiguráció változásainak megfelelően; a változtatási kérelmek hatásainak kiértékelését informatikai biztonsági szempontból; az informatikai biztonsági terv végrehajtásának felügyeletét; és az informatikai biztonsági eljárások hozzáigazítását a többi szabályhoz és eljáráshoz.

Korlátozni kell a számítástechnikai erőforrások használatát és az erőforrásokhoz történő hozzáférést a megfelelő azonosítási, hitelesítési és hozzáférési jogosultság ellenőrzési eljárások révén (még az informatikai részleg esetében is) és meg kell akadályozni a jogosulatlan felhasználói hozzáférést. A vezetésének olyan biztonsági eljárásokat kell kialakítania, amelyek – az informatika biztonsági politikával összhangban – ellenőrzik a tranzakciókat továbbító másik fél valódiságát, hitelességét, amelyek segítségével ellenőrizhető a tranzakciók hitelessége és a rendszerbe bejelentkező felhasználó személyének valódisága. Gondoskodni kell arról (ahol ez szükséges), hogy a tranzakciókat egyik fél se tagadhassa le, és olyan ellenőrzési eljárások működjenek, amelyek biztosítják a tranzakciók kezdeményezésének, fogadásának, elindításának és végrehajtásának letagadhatatlanságát. Gondoskodni kell arról, hogy a bizalmas tranzakciók adatainak cseréje megbízható csatornákon keresztül történjen. A bizalmas információk közé tartoznak a biztonsági eljárásokhoz kapcsolódó információk, a bizalmas tranzakciók adatai, a jelszavak és a kriptográfiai kulcsok. A biztonsági eljárásokhoz kapcsolódó összes hardvert és szoftvert meg kell védeni a jogosulatlan hozzáférésekkel szemben sértetlenségük és titkos kódjaik megőrzése érdekében. Emellett a szervezetnek lehetőleg

titokban kell tartania a biztonsági rendszer felépítését, de nem szabad a biztonságot a rendszer-terv titkosságára építeni.

A vezetésnek gondoskodnia kell a pénzügyi és más bizalmas információk hitelesítéséhez, illetve tárolásához használt kártyák és egyéb fizikai berendezések sértetlenségéről, figyelembe véve az azokhoz kapcsolódó eszközöket, berendezéseket, alkalmazottakat és érvényesség-ellenőrzési módszereket is.

Megfelelő intézkedéseket kell hozni az informatikai eszközök fizikai védelme és az eszközökhöz történő hozzáférés ellenőrzése céljából, beleértve az informatikai eszközök telephelyen kívül történő felhasználását is. A fizikai biztonság és hozzáférés ellenőrzését a rendszer elemeinek összekapcsolásához használt kábelezési egységekre, a segítő szolgáltatásokra (pl.: elektromos áramforrások), a mentésekhez használt adat-hordozókra és a rendszer működéséhez szükséges minden egyéb elemre ki kell terjeszteni. Hozzáférési jogot csak az arra felhatalmazott személyek kaphatnak. Megfelelő eljárások keretében gondoskodni kell arról, hogy külső személyek, vagyis akik nem tagjai az informatikai részleg üzemeltetési csoportjának, csak a fenti csoport valamely tagjának kíséretében léphessenek be a kulcsfontosságú számítógépes helyiségekbe (szerverszoba, kommunikációs kapcsolóberendezések, stb.). A látogatásokról naplót kell vezetni, amelyet rendszeres időközönként ellenőrizni kell. Az informatikai részleg vezetésének gondoskodnia kell arról, hogy megfelelő védelmi intézkedések és eljárások legyenek érvényben a környezeti veszélyforrásokra (pl. tűz, por, elektromosság, túlzott hőmérséklet, illetve páratartalom stb.) vonatkozóan. A vezetésnek rendszeres időközönként fel kell mérnie a szünetmentes tápegységek és generátorok iránti igényeket a kritikus programok biztonságos működése érdekében.

Kiszervezés esetén a szolgáltatónak is biztosítania kell a fenti feltételeket.

Az ezen pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS5 – A rendszer biztonságának megvalósítása" és a „DS12 – Létesítmények kezelése" fejezetek alkalmazását.

8. **Mpt. 77/A. § (5) bekezdés c) pont, Öpt. 40/C. § (5) bekezdés c) pont, Tpt. 101/A. § (5) bekezdés c) pont, Hpt. 13/B. § (5) bekezdés c) pont**

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

A vezetésnek olyan eljárásokat kell kialakítania, amelyek gondoskodnak arról, hogy kellő időben megtörténjenek a szükséges intézkedések a felhasználói jogosultságok kérésével, rögzítésével, kiadásával, felfüggesztésével és lezárásával kapcsolatban (szabályzat). Ezzel összefüggésben ki kell dolgozni egy hivatalos engedélyezési eljárást, amelynek keretében az adatok, illetve a rendszer tulajdonosa (adatgazda) engedélyezi a hozzáférést (hozzáférési szintek). A külső felek hozzáférésének biztonságát szerződés szintjén is meg kell határozni és ennek kapcsán, ki kell térni az adminisztrációhoz és az adatok bizalmas kezeléséhez kapcsolódó követelményekre is. Kiszervezés esetén a felek között megkötött szerződésben ki kell térni a kockázatok és az információs rendszerekhez és hálózatokhoz kapcsolódó biztonsági ellenőrzések és eljárások kérdésére. A rendszeres időközönként (alkalmazás vagy szervezeti, működési struktúra lényeges változásakor) felül kell vizsgálni és meg kell erősíteni a hozzáférési jogokat (de legalább negyedévente javallott).

A 3. pontban jelölt informatika biztonsági felelősnek gondoskodnia kell arról, hogy a biztonságot érintő eseményekről nyilvántartást vezessenek, továbbá arról, hogy a rendszer a biztonsági intézkedések *megsértésére utaló jelzésekről* azonnal értesítse az összes, belső és külső, érintett felet és kellő időben megtegyék a szükséges válaszlépéseket. Az informatika biztonsági felelősnek gondoskodnia kell a biztonsági rendszer működéséhez és a biztonsági előírások megsértéséhez *kapcsolódó esetek* nyilvántartásáról, jelentéséről, átvizsgálásáról, a jogosulatlan hozzáférések és hozzáférési

kísérletek azonosítása és feltárása érdekében.

A vezetésnek ki kell alakítania egy megfelelő eljárást, amely elrendeli, hogy az adatok tulajdonosainak (adatgazdáknak) osztályozniuk kell az adatokat bizalmassági fokuk szerint, formális döntés keretében, az adatosztályozási rendszer előírásai alapján (hozzáférési szintek a felhasználók funkciói alapján).

Lehetőség szerint gondoskodni kell arról, hogy a felhasználók azonosítását és hozzáférési jogait, valamint a rendszerek és az adatgazdák azonosítását egyetlen, központi rendszer kezelje az átfogó hozzáférési jogosultság ellenőrzés hatékony és egységes megvalósítása érdekében.

A felhasználói jogosultságok adminisztrálása kapcsán rendszerenként kell meg határozni felhasználói funkciócsoportonként (könyvelő, számlavezető, pénztáros stb.) a kiosztható jogokat és lehetőség szerint a felhasználók csak a csoportok jogait kaphassák meg. A jogosultság engedélyeken szerepelnie kell az engedélyező aláírásának, vagy elektronikus engedélyezés esetén a rendszer által biztosított (bizonyítható) módon adott engedélynek. Az engedélyező lapokat (elektronikus vagy papír) úgy kell kialakítani, hogy abból egyértelműen kiderüljön az engedélyezett jog. Az engedélyezett jogokat nyilvántartásba kell venni (jogosultság nyilvántartó rendszer). A nyilvántartás egy historikus adatokat tároló rendszer, amelyben egy adott felhasználó minden joga, ami az informatikai rendszerben van lekérdezhető. A rendszerekben lévő felhasználói jogoknak meg kell felelni az engedélyekben és a jogosultság nyilvántartó rendszerben tárolt adatoknak. A szabályzat és a nyilvántartás elkészítésekor figyelembe kell venni a kiemelt jogú felhasználókat (rendszergazdák, technikai felhasználók), a rendszerek alkotóelemeinek (operációs rendszer, adatbázis kezelő, alkalmazás stb.) sokrétűségét és az adminisztrációnak mindezekre ki kell terjedni. A jogosultságok változtatásának naplózását a rendszerekben aktiválni kell, és olyan eljárást kell kialakítani, amely biztosítja a felhasználói jogok változásának, változtatásának ellenőrzését.

Az ezen pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS5 – A rendszer biztonságának biztosítása", a „DS7 – Felhasználók képzése" és a „DS8 – Informatikai felhasználók segítése" fejezetekben leírtak figyelembe vételét.

9. **Mpt. 77/A. § (5) bekezdés d) pont, Öpt. 40/C. § (5) bekezdés d) pont, Tpt. 101/A. § (5) bekezdés d) pont, Hpt. 13/B. § (5) bekezdés d) pont**

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon kell gondoskodni 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,

Az informatikai beszerzések során, figyelembe kell venni a megfelelő „biztonsági környezet" kialakításának szempontjait, amely összhangban van az előzetes kockázatelemzéssel. Megfelelő eljárások révén gondoskodni kell arról, hogy az üzemeltetési naplókban rögzítésre kerüljenek azok a szükséges kronológiai információk, amelyek lehetővé teszik az adatfeldolgozási folyamatok és a feldolgozáshoz kapcsolódó és azt segítő egyéb tevékenységek idősorrendjének rekonstruálását, áttekintését és kivizsgálását. Gondoskodni kell továbbá a kritikus rendszerek eseményeinek naplózásáról, a naplóállományok rendszeres ellenőrzéséről és mentéséről.

A fejlesztési életciklus módszertanban (változáskezelés) elő kell írni megfelelő eljárások és módszerek alkalmazását az új informatikai rendszer-fejlesztési projektek specifikációjának kidolgozásakor, amelyek gondoskodnak a szükséges naplózásról. A vezetésnek gondoskodnia kell arról, hogy a meglévő rendszerek jelentősebb módosítása esetén is az új rendszerek kifejlesztésére vonatkozó fejlesztési előírások szerint kelljen eljárni.

A fejlesztés, illetve módosítás alatt álló rendszerek alapvető biztonsági és belső ellenőrzési aspektusait a rendszer koncepcionális szintű megtervezésével egy időben kell meghatározni annak

érdekében, hogy a biztonsági szempontokat a tervezés lehető legkorábbi szakaszában be lehessen építeni.

A pénzügyi intézménynek ki kell alakítania azokat a megfelelő eljárásokat, amelyek biztosítják, ahol szükséges, hogy az alkalmazási programok olyan funkciókat is tartalmazzanak, amelyek rutinszerűen ellenőrzik a szoftver által elvégzett feladatokat, segítve ezzel az adatok sértetlenségének megőrzését, és amelyek gondoskodnak az adatok épségének helyreállításáról a tranzakciók visszagörgetése, illetve más eszközök révén.

Figyelmet kell fordítani a rendszer-szoftverek paramétereinek megfelelő beállítására és aktualizálására.

A rendszerek által készített naplók biztonsági szempontú elemzését folyamatosan, dokumentált módon kell végezni. Több rendszer, vagy nagyobb szervezet esetén a naplóelemzés megfelelő informatikai támogatásának biztosítása szinte elengedhetetlen a megfelelő színvonalú és költséghatékony munkához.

Az ezen pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „AI2 – Alkalmazási szoftverek beszerzése és karbantartása", az „AI3 – Technológiai infrastruktúra beszerzése és karbantartása", az „AI4 – Informatikai eljárások kifejlesztése és karbantartása" valamint a „DS13 – Üzemeltetés irányítása" fejezetekben leírtak figyelembe vételét.

10. **Mpt. 77/A. § (5) bekezdés e) pont, Öpt. 40/C. § (5) bekezdés e) pont, Tpt. 101/A. § (5) bekezdés e) pont, Hpt. 13/B. § (5) bekezdés e) pont**

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon kell gondoskodni a távadat-átvitel bizalmasságáról, sérthetetlenségéről és hitelességéről.

A vezetésnek gondoskodnia kell a bizalmas információk adattovábbítás és szállítás közben történő megvédéséről, a jogtalan hozzáférések, a módosítások és a téves kézbesítések megakadályozásáról. Az Interneten illetve más nyilvános hálózatokon keresztül történő adattovábbítások kapcsán a vezetésnek ki kell alakítania olyan eljárásokat, szabályokat, illetve számítástechnikai, hálózati protokollokat, amelyek gondoskodnak a bizalmas üzenetek sértetlenségének, bizalmasságának és letagadhatatlanságának megőrzéséről. A szervezethez kívülről érkező információk hitelességét és sértetlenségét megfelelő módon ellenőrizni kell, bármilyen kritikus fontosságú lépés megtétele előtt. Az adatok továbbításakor gondoskodni kell a megfelelő titkosításról illetve a biztonságos protokollok (HTTPS, SSL, SSH, stb.) alkalmazásáról.

Figyelembe véve azt a tényt, hogy egyre kevésbé lehet támaszkodni a hagyományos értelemben vett földrajzi és időbeli határokra, a vezetésnek megfelelő eljárásokat és szabályokat kell kialakítania a bizalmas és kritikus elektronikus tranzakciók sértetlenségének és hitelességének biztosítása érdekében. Minden külső hálózattal kapcsolatos információ-áramlást ellenőrzés alatt kell tartani mindkét irányban. Az Internethez illetve más nyilvános hálózatokhoz történő kapcsolódás vonatkozásában megfelelő védelmet (pl. tűzfalakat, behatolás védelmi eszközöket, stb.) kell kialakítani a belső erőforrásokhoz történő jogtalan hozzáférések illetve a szolgáltatások ellehetetlenítését célzó támadások (pl. Denial of Service) megakadályozása érdekében.

A jogszabály ezen pontjának értelmezéséhez a Felügyelet célszerűnek tartja a COBIT „DS5 – Rendszer biztonságának biztosítása" és a „DS11 – Adatok kezelése" fejezetekben leírtak alkalmazását.

11.) **Mpt. 77/A. § (5) bekezdés f) pont, Öpt. 40/C. § (5) bekezdés f) pont, Tpt. 101/A. § (5) bekezdés f) pont, Hpt. 13/B. § (5) bekezdés f) pont**

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos

módon kell gondoskodni az adathordozók szabályozott és biztonságos kezeléséről.

Az adathordozók szabályozott és biztonságos kezelése érdekében, a kockázatelemzés alapján, megfelelő adattárolási szabályokat kell kialakítani, figyelembe véve a visszakereshetőséggel kapcsolatos követelményeket, a költség-hatékonyságot és a biztonsági alapelveket is. Meg kell határozni a dokumentumok, adatok, programok, jelentések és üzenetek (bejövő és kimenő), valamint az ezek rejtjelezéséhez és hitelesítéséhez használt adatok (kulcsok, tanúsítványok) megőrzési idejét és tárolási feltételeit. A vezetésnek gondoskodnia kell az adatokat tartalmazó tároló szisztematikus leltározásáról és arról, hogy a leltározás során talált eltérések időben rendezésre kerüljenek, továbbá megfelelő intézkedéseket kell hozni a tárolt adathordozók sértetlenségének megőrzése érdekében. A vezetésnek gondoskodnia kell arról, hogy létezzen egy olyan eljárásrend és szabályzat, amely az adathordozó-tároló tartalmának védelmét szolgálja. Külön szabályokat és előírásokat kell kidolgozni a mentési adathordozók külsején megjelenő azonosító címkékre, az adathordozók tárolására és fizikai mozgatásuk nyomon követésére annak érdekében, hogy mindig el lehessen velük számolni. Ki kell jelölni az adathordozó könyvtár (mágnesszalagok, cserélhető szalag kazetták illetve egyéb cserélhető adathordozó elemek, lemezek, CD, DVD) kezeléséért felelős személyeket.

Az ezen pontban leírtak teljesítése érdekében a Felügyelet javasolja a COBIT „DS11 – Adatok kezelése" fejezetekben leírtak alkalmazását.

12. **Mpt. 77/A. § (5) bekezdés g) pont, Öpt. 40/C. § (5) bekezdés g) pont, Tpt. 101/A. § (5) bekezdés g) pont, Hpt. 13/B. § (5) bekezdés g) pont**

A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon kell gondoskodni a vírusvédelméről.

A rossz szándékú szoftverek vonatkozásában, mint amilyenek a számítógépes vírusok vagy a "trójai programok", a vezetésnek megfelelő megelőző, észlelési és korrekciós mechanizmusokat, válaszlépéseket és jelentési eljárásokat kell kidolgoznia. A vezetésnek gondoskodnia kell arról, hogy a szervezet egészére kiterjedően megfelelő eljárások kerüljenek kialakításra a számítógépes vírusokkal szembeni védelem érdekében. A fenti eljárásoknak a vírus-védelemre, a vírusok felderítésére, a megfelelő válaszlépésekre és a jelentési kötelezettségekre egyaránt ki kell terjedniük. Olyan szabályokat kell kialakítani és bevezetni, amelyek korlátozzák a személyes és az engedély nélküli szoftverek használatát. A szervezetnek víruskereső és vírusirtó szoftvereket kell használnia minden olyan munkaállomáson és szerveren, amelyek alkalmasak vírusok futtatására. Az informatikai részleg vezetésének rendszeres időközönként ellenőriznie kell, hogy a szervezet személyi számítógépeire nem lettek-e telepítve engedély nélküli szoftverek.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS5 – Rendszer biztonságának biztosítása" és a „DS9 – Konfiguráció kezelése" című fejezetekben leírtak figyelembe vételét.

13. **Mpt. 77/A. § (6) bekezdés, Öpt. 40/C. § (6) bekezdés, Tpt. 101/A. § (6) bekezdés, Hpt. 13/B. § (6) bekezdés**

A pénzügyi szervezetnek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább az a)-g) pontokban meghatározottakkal.

Az ágazati törvények hivatkozott paragrafusainak (1) bekezdésében említett kockázatelemzésre alapozva kell kiépíteni a védelmi intézkedéseket, de a „rendelkeznie kell legalább a következőkkel"

kitétel minimum követelményeket határoz meg, így a (6) bekezdés alpontjaiban szereplő meghatározások minimum feltételek.

14. **Mpt. 77/A. § (6) bekezdés a) pont, Öpt. 40/C. § (6) bekezdés a) pont, Tpt. 101/A. § (6) bekezdés a) pont, Hpt. 13/B. § (6) bekezdés a) pont**

A pénzügyi szervezetnek rendelkeznie kell informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel.

Az informatikai részlegnek egységes szabványos eljárásokat kell kialakítania az informatikai rendszerek üzemeltetésére vonatkozóan (a hálózati üzemeltetést is beleértve), és megfelelően dokumentálnia kell azokat. Minden alkalmazott informatikai megoldást és platformot a fenti eljárásoknak megfelelően kell működtetni. Az eljárások eredményességét és betartását rendszeres időközönként ellenőrizni kell. Az informatikai részleg vezetésének gondoskodnia kell arról, hogy az üzemeltető személyzet megfelelő ismeretekkel és gyakorlottsággal rendelkezzen az indítási eljárás és a többi üzemeltetési feladat dokumentálása, rendszeres tesztelése és szükség szerinti módosítása terén. Az informatikai részleg vezetésének gondoskodnia kell arról, hogy a szolgáltatási szint megállapodásokban (SLA-k) kitűzött célok teljesítése érdekében a munkafolyamatok, eljárások és feladatok a lehető leghatékonyabb módon legyenek megszervezve, maximális áteresztőképességet és kihasználtságot biztosítva. Megfelelő eljárásokat kell kialakítani a munkafolyamatok előírt ütemezésétől történő eltérések megállapítására, kivizsgálására és jóváhagyására vonatkozóan. Megfelelő eljárások révén gondoskodni kell arról, hogy a feldolgozás az operátori műszakváltás alatt is folyamatos legyen, és ennek érdekében meg kell határozni a munkafeladatok átadására, az állapot jelentésének aktualizálására és a feladatokért viselt felelősségről szóló jelentésekre vonatkozó szabályokat. Megfelelő eljárások révén gondoskodni kell arról, hogy az üzemeltetési naplókban rögzítésre kerüljenek azok a szükséges kronológiai információk, amelyek lehetővé teszik az adatfeldolgozási folyamatok és a feldolgozáshoz kapcsolódó és azt segítő egyéb tevékenységek idősorrendjének rekonstruálását, áttekintését és kivizsgálását. A vezetésnek gondoskodnia kell a speciális nyomtatványok és a bizalmas jellegű output eszközök megfelelő fizikai védelméről. Távműködtetés esetén külön eljárásokat kell kidolgozni a távműködtető munkaállomásokhoz történő csatlakozás, illetve leválás meghatározására és végrehajtására vonatkozóan. Minden alkalmazásnak el kell készíteni az üzemeltetési utasítását.

A vezetés felel azért, hogy olyan hosszú- és rövid távú tervek kerüljenek kidolgozásra és végrehajtásra, amelyek megfelelnek a pénzügyi intézmény hosszú távú célkitűzéseinek és rövid távú céljainak. Az informatikai tervezési eljárásnak figyelembe kell vennie a kockázat-elemzések eredményeit, az üzleti, a környezeti, a technológiai és az emberi erőforrásokhoz kapcsolódó kockázatokat, valamint az időszerű és szükséges változások átvezetésének módját.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO1 – Informatikai stratégiai terv kidolgozása", a „PO2 – Információ-architektúra meghatározása", a „PO3 – Technológiai irány meghatározása", a „PO5 – Informatikai beruházások kezelése", a „PO10 – Projektek irányítása", a „DS6 – Költségek megállapítása és felosztása" valamint a „DS13 – Üzemeltetés irányítása" című fejezetekben leírtak figyelembe vételét.

15. **Mpt. 77/A. § (6) bekezdés b) pont, Öpt. 40/C. § (6) bekezdés b) pont, Tpt. 101/A. § (6) bekezdés b) pont, Hpt. 13/B. § (6) bekezdés b) pont**

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.

A vezetésnek gondoskodnia kell arról, hogy meghatározásra kerüljenek az informatikai rendszerek rendelkezésre állására és teljesítményére vonatkozó üzleti követelmények, és azok alapján kerüljenek kidolgozásra a rendelkezésre állásra vonatkozó feltételek és követelmények. A vezetésnek gondoskodnia kell egy olyan megfelelő rendelkezésre állási terv kidolgozásáról, amely biztosítja, figyelemmel kíséri és ellenőrzi informatikai szolgáltatások rendelkezésre állását, valamint gondoskodni kell a rendkívüli eseményekről kellő időben megfelelő részletességű jelentés készüljön.

A pénzügyi intézmény rendszerfejlesztési módszertanában meg kell határozni a programok dokumentációjára vonatkozó szabványokat és az informatikai rendszer-fejlesztési, illetve módosítási feladatok részeként kifejlesztett szoftverek teszt-követelményeire, valamint a tesztelés ellenőrzésére, dokumentációjára és fenntartására vonatkozó szabványokat. A pénzügyi intézmény rendszerfejlesztési életciklus módszertanában meg kell határozni, hogy milyen esetekben szükséges a régi és új rendszerek párhuzamos futtatása, illetve elő kell írni azt, hogy minden informatikai rendszerfejlesztési, megvalósítási, illetve módosítási projekt során meg kell őrizni az elvégzett tesztek dokumentált eredményeit.

A vezetésnek gondoskodnia kell arról, hogy a külső szolgáltatók által biztosított szolgáltatások köre pontosan legyen meghatározva és a szállítókkal meglévő technikai és szervezeti kapcsolat megfelelően legyen dokumentálva. A vezetésnek megfelelő eljárások keretében gondoskodnia kell arról, hogy a külső szolgáltatókkal kialakított kapcsolatokat olyan írásbeli szerződések szabályozzák, amelyeket még a munkák megkezdése előtt hivatalosan megkötöttek. Ettől eltérni rendkívüli helyzet esetében lehet, melyre a vonatkozó szabályzat térjen ki! A vezetésnek gondoskodnia kell arról, hogy a külső szolgáltatói kapcsolatok esetében olyan biztonsági megállapodások (pl. titoktartási megállapodások) kerüljenek kidolgozásra és megkötésre, amelyek megfelelnek az általános üzleti normáknak, valamint a jogi és szabályozási követelményeknek, az anyagi, pénzügyi felelősségre vonatkozó követelményeket is beleértve. A vezetésnek gondoskodnia kell a külső szolgáltatók által nyújtott szolgáltatások teljesítésének folyamatos figyeléséről a szerződésben foglaltak betartásának ellenőrzése céljából.

A vezetésnek ki kell alakítania egy megfelelő eljárást a külső rendszerfejlesztőkkel történő kapcsolat biztosítására az elfogadási, az átadás/átvétel kritériumai, a változtatások kezelése, a fejlesztés során jelentkező problémák megoldása, a felhasználói szerepek, a technikai berendezések, a műszaki környezet, a fejlesztő-eszközök, a szoftverek, a szabványok és az eljárások területén.

Külső fejlesztő alkalmazása esetén a szerződésben rendelkezni kell arról, hogy a fejlesztett szoftver reprodukciójához szükséges információkat (forráskódját, adatbázis definícióját, stb.) letétbe kell helyezni, és a fejlesztő társaság megszűnése esetén a pénzügyi intézmény az informatikai rendszerének folyamatos működése érdekében hozzájusson.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS2 – Külső szolgáltatások kezelése", a „DS3 – Teljesítmény és kapacitás kezelése" valamint a „PO11 – Minőségirányítás" című fejezetekben leírtak figyelembe vételét.

16.) **Mpt. 77/A. § (6) bekezdés c) pont, Öpt. 40/C. § (6) bekezdés c) pont, Tpt. 101/A. § (6) bekezdés c) pont, Hpt. 13/B. § (6) bekezdés c) pont**

A pénzügyi szervezetnek rendelkeznie kell 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,

Az informatikai részleg vezetésének az üzletmenet-folytonossági terv alapján ki kell dolgoznia egy informatikai folyamatossági keretrendszert, amely meghatározza a feladatokat és felelősségi

köröket, az alkalmazandó kockázat-alapú megközelítési módszert valamint az informatikai folyamatossági terv dokumentálására és jóváhagyására vonatkozó szabályokat és struktúrákat. A vezetésnek gondoskodnia kell arról, hogy az informatikai folyamatossági terv összhangban álljon az üzletmenet-folytonossági tervvel. Az informatikai részleg vezetésének megfelelő eljárásokat kell kidolgoznia a változtatások szabályozására vonatkozóan annak érdekében, hogy a folyamatossági terv mindig naprakész legyen és igazodjon az üzleti/szervezeti követelményekhez. A folyamatossági terv eredményességének megőrzése érdekében a vezetésnek rendszeres időközönként értékelnie kell a terv megfelelőségét, illetve akkor, amikor jelentősebb változások történnek a szervezetben, az üzletvitelben vagy az informatikai infrastruktúrában. A katasztrófa-elhárítási módszertan keretében gondoskodni kell arról, hogy minden érintett fél rendszeres időközönként megfelelő képzést kapjon arra vonatkozóan, hogy rendkívüli esemény illetve katasztrófa esetén milyen szabályok szerint kell eljárni. A folyamatossági módszertanban gondoskodni kell arról, hogy a felhasználók megfelelő alternatív feldolgozási eljárásokat alakítsanak ki, amelyeket használhatnak addig, amíg az informatikai részleg teljes mértékben helyre nem állítja a rendszert a bekövetkezett leállást, illetve katasztrófát követően. A folyamatossági tervben meg kell határozni a katasztrófa-helyzet utáni helyreállításhoz szükséges kritikus fontosságú alkalmazási programokat, külső szolgáltatókat, operációs rendszereket, munkatársakat és készleteket, adatállományokat és a katasztrófa utáni visszaállításhoz szükséges időt. A vezetésnek gondoskodnia kell arról, hogy a folyamatossági módszertan alternatív tartalék telephelyek és hardverek meghatározását is előírja és egy végleges alternatíva is ki legyen választva. Amennyiben szükséges, szerződés keretében kell szabályozni az ilyen jellegű szolgáltatásokat. A helyreállításra és folyamatos üzletvitelre vonatkozó tervek kapcsán gondoskodni kell a kritikus back-up adathordozók, dokumentációk és egyéb informatikai erőforrások külső tárolásáról. A külső helyen tárolandó back-up erőforrások körének meghatározásába be kell vonni az üzleti folyamatokért felelős vezetőket és az informatikai részleg dolgozóit is.

A szolgáltatások meghatározása érdekében a felső vezetésnek meg kell határoznia egy olyan megfelelő keretrendszert, amely segíti a formális szolgáltatási-szint megállapodások (SLA-k) kidolgozását és meghatározza azok minimális tartalmát (rendelkezésre állás, megbízhatóság, teljesítmény, kapacitás, szolgáltatási díjak, változáskezelés, stb.). A felhasználóknak és az informatikai részlegnek írásbeli megállapodást kell kötniük, amelyben mennyiségi és minőségi vonatkozásban is meg kell határozniuk a szolgáltatási szintet. Megfelelő eljárások révén gondoskodni kell arról, hogy az érintett felek közötti kapcsolatokból (pl. titoktartási megállapodásokból) eredő kötelezettségek teljesítésének módja és felelőssége megfelelően meghatározásra kerüljön, koordinálva legyen és tájékoztatást kapjon arról minden érintett osztályt. Az informatikai részleg vezetésének ki kell neveznie egy szolgáltatási szint-felelőst, akinek figyelemmel kell kísérnie a meghatározott szolgáltatási kritériumok teljesítését. A vezetésnek rendszeres idő-közönként felül kell vizsgálnia a szolgáltatási-szint megállapodásokat és meg kell újítania a külső szolgáltatókkal megkötött szerződéseket.

Az informatikai részleg vezetésének ki kell alakítania egy megfelelő probléma-kezelő rendszert, amely gondoskodik a működés során tapasztalt nem szokásos események (rendkívüli esetek, problémák, hibák, stb.) nyilvántartásáról, elemzéséről és megfelelő időben történő megoldásáról. A vész-helyzetekben alkalmazandó program eljárások megváltoztatását azonnal tesztelni kell, jóvá kell hagyatni és jelentést kell készíteni az esetről. Jelentősebb probléma esetén ún. 'rendkívüli esemény jelentést' kell készíteni. A vezetésnek ki kell alakítania megfelelő probléma felterjesztési/ továbbítási eljárásokat (az illetékesek felé) a feltárt problémák lehető leghatékonyabb módon és megfelelő időben történő megoldása érdekében. A fenti eljárásokban meg kell határozni az ezzel kapcsolatos prioritásokat. Az eljárás keretében dokumentálni kell az informatikai folyamatossági terv beindulására vonatkozó döntés-előkészítő eljárást is. A problémakezelő rendszer keretében ki kell alakítani olyan megfelelő ellenőrzési naplókat, amelyek lehetővé teszik a problémák mögött meghúzódó okok felderítését a rendkívüli eseményből kiindulva az okokig, és vissza.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS1 – Szolgáltatási szintek meghatározása", a „DS4 – Folyamatos működés biztosítása" és a „DS10 – Rendkívüli események kezelése" című fejezetekben leírtak figyelembe vételét.

17. **Mpt. 77/A. § (6) bekezdés d) pont, Öpt. 40/C. § (6) bekezdés d) pont, Tpt. 101/A. § (6) bekezdés d) pont, Hpt. 13/B. § (6) bekezdés d) pont**

A pénzügyi szervezetnek rendelkeznie kell olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását.

A szervezet rendszerfejlesztési metodikájának részeként ki kell alakítani egy megfelelő eljárást a felhasználói szoftverek teljesítményének méretezésére, optimalizálására az új és jelentős mértékben módosított, megváltoztatott szoftverek üzemeltetéséhez szükséges erőforrások előrejelzése érdekében. Az elért előrehaladás mérésére - az érintett felek által jóváhagyott - megvalósítási tervet kell kidolgozni. A végrehajtási tervnek az alábbi kérdésekre kell kitérnie: helyszín előkészítése, eszközök beszerzése és telepítése, felhasználók képzése, operációs rendszer módosításainak telepítése, üzemelési eljárások bevezetése és áttérés. A szervezet rendszerfejlesztési metodikájában elő kell írni, hogy a régi rendszer szükséges elemeit minden egyes informatikai rendszer-fejlesztési, megvalósítási illetve módosítási projekt esetében át kell emelni az új rendszerbe az erre vonatkozóan előre kidolgozott tervek szerint.

Migráció illetve adatkonverzió esetén a vezetésnek elő kell írnia olyan adat-átalakítási terv elkészítését, amely meghatározza az átalakítandó adatok összegyűjtésének és ellenőrzésének módszereit és emellett feltárja és megoldja az átalakítás során talált hibákat (adat-átalakítás és konverzió).

A rendszergazdának és az informatikai részleg vezetésének tesztelési stratégiákat és terveket kell készíteniük. Az érintett felhasználói osztályok dolgozói és az informatikai részleg üzemeltetési csoportja számára a kidolgozott oktatási tervben foglaltaknak megfelelő képzést kell biztosítani. A vezetésnek gondoskodnia kell arról, hogy a változtatásokat a valós környezetben történő üzembeállítás előtt külön környezetben tesztelje egy a (rendszer-építőktől) független tesztelési csoport a hatás- és kapacitás-elemzésnek megfelelően. Az átvételi tesztelést a jövőbeni működési környezethez hasonló környezetben kell végrehajtani.

Szoftverváltozások esetén az új illetve módosított rendszerek végleges elfogadási, átvételi illetve minőségbiztosítási tesztelési eljárásának részeként a tesztelési eredményeket formálisan is jóvá kell hagynia az érintett felhasználói osztály(ok) és az informatikai részleg vezetésének. A vezetésnek elő kell írnia, hogy az üzemeltetési részleg és a felhasználói osztályok vezetőinek formálisan is el kell fogadniuk a teszt-eredményeket és a rendszerek biztonsági szintjét, az elfogadott kockázati szinttel együtt. A vezetésnek ki kell dolgoznia és végre kell hajtania azokat a formális eljárásokat, amelyek szabályozzák a rendszer átadását a rendszerfejlesztéstől kezdve a tesztelésen keresztül az üzembe helyezésig. A vezetésnek elő kell írnia, hogy az új rendszer csak, sikeres teszteredményeket követően, a rendszer tulajdonosának engedélyével helyezhető üzembe. Az egyes alkalmazások eltérő rendeltetésű környezeteit (fejlesztési, tesztelési, üzemeltetési) külön kell választani és gondoskodni kell azok korrekt védelméről.

A pénzügyi intézmény rendszerfejlesztési szabályozási rendszerében elő kell írni, hogy a megvalósítást követően az informatikai rendszerre vonatkozó üzemeltetési-követelmények (ún. kapacitás, áteresztőképesség, stb.) megvizsgálása alapján értékelni kell, hogy a rendszer megfelel-e a felhasználói igényeknek, vagy sem.

A pénzügyi intézmény életében bekövetkező változásokat kezelni kell. A változások (adatok, hardver, szoftver, infrastruktúra, technológia, emberi erőforrások, stb.) kezelésre vonatkozóan formális szabályokat és hivatalos eljárásokat kell definiálni, valamint a változáskezelési feladatok menedzselése érdekében javasolt külön felelős(öke)t kijelölni (változásmenedzser). A vezetésnek elő kell írnia, hogy a változtatásokra, a rendszerkarbantartásokra és a szállítói (által végzendő) karbantartásokra vonatkozó kéréseket előre meghatározott formában kell benyújtani és annak megfelelően kell eljárni. A változtatási kéréseket kategorizálni kell, majd meg kell határozni prioritási fokukat. A sürgős esetekre vonatkozóan külön szabályozást kell kidolgozni. A változtatások kérelmezőit tájékoztatni kell kérelmük státuszáról.

Ki kell alakítani egy olyan eljárást, amely gondoskodik a változtatási kérelmek strukturált módon történő értékeléséről és figyelembe veszi az üzemben lévő rendszert és annak funkcionalitását érintő összes lehetséges – kockázatelemzés során figyelembevett – következményt. A vezetésnek gondoskodnia kell arról, hogy a változáskezelés, a szoftvermenedzselés és terítés megfelelően igazodjon az átfogó konfiguráció-kezelési rendszerhez. Az alkalmazási rendszerben végrehajtott változások megfigyelésére szolgáló rendszert automatizálni kell annak érdekében, hogy rögzítésre kerüljenek a nagy és bonyolult informatikai rendszereken elvégzett módosítások.

Az informatikai vezetésnek meg kell határoznia a sürgősségi (pl. vészhelyzet) változtatások paramétereit és az ilyen változtatások szabályozásának menetét, amennyiben azok kívül esnek a bevezetés előtti műszaki, üzemelési és vezetői értékelés normál eljárásán. A sürgősségi változtatásokat nyilván kell tartani és előzetesen jóvá kell hagynia az informatikai vezetésnek.

A változtatási eljárásra vonatkozó szabályokban elő kell írni, hogy amennyiben végrehajtásra kerül valamilyen rendszerváltoztatás, az ahhoz kapcsolódó dokumentációt és eljárásokat is aktualizálni kell. A vezetésnek gondoskodnia kell a karbantartó személyzet által elvégzendő munkák kijelöléséről és megfelelő felügyeletéről. Ezen felül szabályozni kell hozzáférési jogaikat is az automatizált rendszerekhez történő jogosulatlan hozzáférés elkerülése érdekében.

A vezetésnek olyan szabályokat kell kialakítania és bevezetnie az új szoftver verziók bevezetésére vonatkozóan, amelyek a jóváhagyásra és elfogadásra, a szoftver csomag kialakítására, a tesztelésre, az átadásra, stb. egyaránt kiterjednek. Megfelelő belső ellenőrzési intézkedéseket kell kialakítani annak érdekében, hogy az egyes szoftverelemek sértetlenül a megfelelő helyre kerüljenek a megfelelő időben, és mindez megfelelően ellenőrizhető legyen (pl. az ellenőrzési naplón keresztül).

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „AI5 – Rendszerek üzembe helyezése és jóváhagyása" valamint az „AI6 – Változások kezelése" című fejezetekben leírtak figyelembe vételét.

18. **Mpt. 77/A. § (6) bekezdés e) pont, Öpt. 40/C. § (6) bekezdés e) pont, Tpt. 101/A. § (6) bekezdés e) pont, Hpt. 13/B. § (6) bekezdés e) pont**

A pénzügyi szervezetnek rendelkeznie kell 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. Ezen mentéseket környezeti kockázati szempontból elkülönítetten és védett módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.

A vezetésnek ki kell dolgoznia egy megfelelő stratégiát az adatok mentésére és helyreállítására vonatkozóan, amely kitér az üzleti követelmények áttekintésére, valamint a helyreállítási terv kidolgozására, megvalósítására, tesztelésére és dokumentálására is. Megfelelő eljárások keretében gondoskodni kell arról, hogy a mentések megfeleljenek a fenti követelményeknek. Megfelelő eljárások keretében gondoskodni kell arról, hogy a mentési műveletek a meghatározott mentési stratégiával összhangban kerüljenek végrehajtásra, továbbá rendszeres időközönként ellenőrizni kell a mentések használhatóságát. Az informatikai adathordozókra vonatkozó mentési előírások keretében gondoskodni kell az adatállományok, a szoftverek és a kapcsolódó dokumentációk megfelelő tárolásáról, mind a szervezet telephelyén, mind azon kívül. A mentéseket biztonságos helyen kell őrizni és rendszeres időközönként ellenőrizni kell a tárolási hely fizikai hozzáférhetőségét, valamint az adatállományok és egyéb elemek biztonságát, meg kell győződni az elmentett adatok és rendszerek visszatölthetőségéről az esetleges szoftver és hardverkörnyezet megváltozása esetén.

Az adatgazdáknak kell meghatározniuk az adatok besorolását és megosztását, valamint azt, hogy szükség van-e, és ha igen mikor, a programok és fájlok megőrzésére, archiválására, illetve

törlésére.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS11 – Adatok kezelése" című fejezetében leírtak figyelembe vételét.

19. **Mpt. 77/A. § (6) bekezdés f) pont, Öpt. 40/C. § (6) bekezdés f) pont, Tpt. 101/A. § (6) bekezdés f) pont, Hpt. 13/B. § (6) bekezdés f) pont**

A pénzügyi szervezetnek rendelkeznie kell jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig (pénztárak esetében az adott tag tagsági jogviszonyának megszűnését követő 5 évig), bármikor visszakereshetően, helyreállíthatóan megőrizzék.

A vezetésnek megfelelő szabályok és eljárások kialakításával gondoskodnia kell arról, hogy az adatok archiválására a jogi és üzleti követelményeknek megfelelően kerüljön sor, továbbá gondoskodni kell az archivált adatoknak az eredetivel megegyező megfelelő védelméről és nyilvántartásáról.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS11 – Adatok kezelése" című fejezetében leírtak figyelembe vételét.

20. **Mpt. 77/A. § (6) bekezdés g) pont, Öpt. 40/C. § (6) bekezdés g) pont, Tpt. 101/A. § (6) bekezdés g) pont, Hpt. 13/B. § (6) bekezdés g) pont**

A pénzügyi szervezetnek rendelkeznie kell a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (6) bekezdés c) pontjához fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS1 – Szolgáltatási szintek meghatározása", a „DS4 – Folyamatos működés biztosítása" és a „DS10 – Rendkívüli események kezelése" című fejezetekben leírtak figyelembe vételét.

21. **Mpt. 77/A. § (7) bekezdés, Öpt. 40/C. § (7) bekezdés, Tpt. 101/A. § (7) bekezdés, Hpt. 13/B. § (7) bekezdés**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az a)-g) pontokban meghatározottaknak.

A „mindenkor rendelkezésre kell állnia" a Felügyelet értelmezésében azt jelenti, hogy a pénzügyi szervezetnek már az engedélyezéskor, illetve az üzleti tevékenység folytatása során folyamatosan rendelkeznie kell ezekkel a minimális feltételekkel .

22. **Mpt. 77/A. § (7) bekezdés a) pont, Öpt. 40/C. § (7) bekezdés a) pont, Tpt. 101/A. § (7) bekezdés a) pont, Hpt. 13/B. § (7) bekezdés a) pont**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az általa fejlesztett, megrendelésére

készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (4) bekezdéséhez, (5) bekezdés a) pontjához, illetve (6) bekezdés a)-b) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „AI1 – Automatizált megoldások meghatározása", az „AI2 – Alkalmazói szoftverek beszerzése és karbantartása", az „AI4 – Informatikai eljárások kifejlesztése és karbantartása", a „PO2 – Információ architektúra meghatározása" és a PO11 – Minőségirányítás" című fejezetekben leírtak figyelembe vételét.

23. **Mpt. 77/A. § (7) bekezdés b) pont, Öpt. 40/C. § (7) bekezdés b) pont, Tpt. 101/A. § (7) bekezdés b) pont, Hpt. 13/B. § (7) bekezdés b) pont**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak ((6) bekezdés a)-b) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „AI2 – Alkalmazói szoftverek beszerzése és karbantartása", a „PO2 – Információ architektúra meghatározása", az „AI1 – Automatizált megoldások meghatározása" és az „AI2 – Alkalmazói szoftverek beszerzése és karbantartása" című fejezetekben leírtak. Figyelembe vételét.

24. **Mpt. 77/A. § (7) bekezdés c) pont, Öpt. 40/C. § (7) bekezdés c) pont, Tpt. 101/A. § (7) bekezdés c) pont, Hpt. 13/B. § (7) bekezdés c) pont**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az informatikai rendszer elemeinek a pénzügyi szervezet által meghatározott biztonsági osztályokba sorolási rendszeréne.

Az ebben a pontban elvártak megegyeznek az az ágazati törvények hivatkozott paragrafusainak (5) bekezdés c) pontjához fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO2 – Információ architektúra meghatározása" és a „DS5 – A rendszerek biztonságának megvalósítása" című fejezetekben leírtak figyelembe vételét.

25. **Mpt. 77/A. § (7) bekezdés d) pont, Öpt. 40/C. § (7) bekezdés d) pont, Tpt. 101/A. § (7) bekezdés d) pont, Hpt. 13/B. § (7) bekezdés d) pont**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az adatokhoz történő hozzáférési rend meghatározásának.,

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak ((5) bekezdés a) és c) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT a „PO2 – Információ architektúra meghatározása”, a „PO4 – Az informatikai részleg szervezeti felépítésének és kapcsolatainak meghatározása” és a „DS5 – A rendszerek biztonságának megvalósítása” című fejezetekben leírtak figyelembe vételét.

26. **Mpt. 77/A. § (7) bekezdés e) pont, Öpt. 40/C. § (7) bekezdés e) pont, Tpt. 101/A. § (7) bekezdés e) pont, Hpt. 13/B. § (7) bekezdés e) pont**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az adatgazda és a rendszergazda kijelölését tartalmazó okiratnak.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (3) bekezdéséhez fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO4 – Az informatikai részleg szervezeti felépítésének és kapcsolatainak meghatározása” és a „PO7 – Emberi erőforrások kezelése” című fejezetekben leírtak figyelembe vételét.

27.) **Mpt. 77/A. § (7) bekezdés f) pont, Öpt. 40/C. § (7) bekezdés f) pont, Tpt. 101/A. § (7) bekezdés f) pont, Hpt. 13/B. § (7) bekezdés f) pont**

A pénzügyi szervezetnél mindenkor rendelkezésre kell állnia az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (1) bekezdéséhez és az (5) bekezdés a)-b) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO6 – Vezetői célok és irányvonal közlése” és a „DS9 – Konfiguráció kezelése” című fejezetekben leírtak figyelembe vételét.

28. **Mpt. 77/A. § (7) bekezdés g) pont, Öpt. 40/C. § (7) bekezdés g) pont, Tpt. 101/A. § (7) bekezdés g) pont, Hpt. 13/B. § (7) bekezdés g) pont**

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

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (5) bekezdés a) pontjához fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS9 – Konfiguráció kezelése” című fejezetben leírtak figyelembe vételét.

29. **Mpt. 77/A. § (8) bekezdés, Öpt. 40/C. § (8) bekezdés, Tpt. 101/A. § (8) bekezdés, Hpt. 13/B. § (8) bekezdés**

A pénzügyi szervezetnél a szoftvereknek együttesen alkalmasnak kell lenniük legalább a bekezdésben meghatározottaknak.

:

Az ebben a pontban elvártak a szoftverekre vonatkozóan tartalmaznak minimum feltételeket.

30. **Mpt. 77/A. § (8) bekezdés a) pont, Öpt. 40/C. § (8) bekezdés a) pont, Tpt. 101/A. § (8) bekezdés a) pont, Hpt. 13/B. § (8) bekezdés a) pont**

A pénzügyi szervezetnél a szoftvereknek együttesen alkalmasnak kell lenniük a működéshez szükséges és jogszabályban előírt adatok nyilvántartására.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (1) bekezdéséhez és a (6) bekezdés c)-d) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO1 – Informatikai stratégiai terv kidolgozása”, a „PO8 – Külső követelmények betartásának biztosítása”, a PO11 – Minőségirányítás”, az „AI5 – Rendszerek installálása és jóváhagyása” valamint a „DS1 – Szolgáltatási szintek meghatározása” című fejezetekben leírtak figyelembe vételét.

31. **Mpt. 77/A. § (8) bekezdés b) pont, Öpt. 40/C. § (8) bekezdés b) pont, Tpt. 101/A. § (8) bekezdés a) pont, Hpt. 13/B. § (8) bekezdés d) pont*)***

A pénzügyi szervezetnél a szoftvereknek együttesen alkalmasnak kell lenniük a tárolt adatok ellenőrzéséhez való felhasználására.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (5) bekezdés f) pontjához és a (6) bekezdés e)-f) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „DS11 – Adatok kezelése” című fejezetben leírtak figyelembe vételét.

32. **Mpt. 77/A. § (8) bekezdés c) pont, Öpt. 40/C. § (8) bekezdés c) pont, Tpt. 101/A. § (8) bekezdés f) pont, Hpt. 13/B. § (8) bekezdés e) pont*)***

A pénzügyi szervezetnél a szoftvereknek együttesen alkalmasnak kell lenniük a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (5) bekezdés b)-c) és d) pontjaihoz fűzött megjegyzésekkel.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „AI2 – Alkalmazói szoftverek beszerzése és karbantartása”, a „DS5 – A rendszer biztonságának megvalósítása” valamint a „DS11 – Adatok kezelése” című fejezetekben leírtak figyelembe vételét.

33**. Tpt. 101/A. § (8) bekezdés b-d) pont, Hpt. 13/B. § (8) bekezdés b)-c) pont**

A pénzügyi szervezetnél a szoftvereknek együttesen alkalmasnak kell lenniük a pénz és az érték-

papírok biztonságos nyilvántartására, a befektetési és árutőzsdei szolgáltatások tárgyának elkülönített naprakész nyilvántartására, valamint az országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra.

Az ebben a pontban elvártak megegyeznek az ágazati törvények hivatkozott paragrafusainak (5) és (6) bekezdéséhez fűzött megjegyzésekkel.

34**. Mpt. 77/A. § (9) bekezdés, Öpt. 40/C. § (9) bekezdés, Tpt. 101/A. § (9) bekezdés, Hpt. 13/B. § (9) bekezdés**

A pénzügyi szervezet belső szabályzatában meg kell határozni az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.

A pénzügyi intézménynél a munkakörökhöz szükséges informatikai képzettség és gyakorlat meghatározását belső szabályzatban kell meghatározni és nemcsak a munkaköri leírásokban. Minden dolgozónak részt kell vennie egy az informatikai biztonság alapelveit – munkakörének megfelelő szinten – ismertető tanfolyamon, amelyet rendszeres jelleggel meg kell tartani és amelyen belül kiemelt figyelmet kell fordítani a biztonsági kérdések tudatosítására és a rendkívüli események kezelésére. Az ebben a pontban elvártak kapcsolódnak a 3. ponthoz fűzött megjegyzésekhez.

Az ebben a pontban leírtak teljesítése érdekében a Felügyelet célszerűnek tartja a COBIT „PO7 – Emberi erőforrások kezelése" című fejezetben leírtak figyelembe vételét.

A módszertani útmutatóban megfogalmazott véleménynek jogi ereje, kötelező tartalma nincs, az elvárások a nemzetközi ajánlásokon és legjobbnak tartott gyakorlaton alapulnak.

I. sz. melléklet: A törvényi előírások és a COBIT megfeleltetése

I. MELLÉKLET: A TÖRVÉNYI ELŐÍRÁSOK ÉS A COBIT MEGFELELTETÉSE

Az informatikai rendszer védelmére vonatkozó törvényi előírások összefoglalása[3]	**Szakterület és folyamat megnevezése a COBIT-ban**
(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 ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.	**PO – TERVEZÉS ÉS SZERVEZET** PO 6 – VEZETŐI CÉLOK ÉS IRÁNYVONAL KÖZLÉSE PO 8 – KÜLSŐ KÖVETELMÉNYEK BETARTÁSÁNAK BIZTOSÍTÁSA **AI – BESZERZÉS ÉS BEVEZETÉS** AI 1 – AUTOMATIZÁLT MEGOLDÁSOK MEGHATÁROZÁSA
(2) A pénzügyi intézmény köteles az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább kétévente felülvizsgálni és aktualizálni.	**PO – TERVEZÉS ÉS SZERVEZET** PO 9 – KOCKÁZATOK ÉRTÉKELÉSE
(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 RÉSZLEG SZERVEZETI FELÉPÍTÉSÉNEK ÉS KAPCSOLATAINAK MEGHATÁROZÁSA PO 7 – EMBERI ERŐFORRÁSOK KEZELÉSE
(4) A pénzügyi intézménynek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működtetnie kell.	**M – FELÜGYELET** M 1 – ELJÁRÁSOK FELÜGYELETE M 2 – BELSŐ ELLENŐRZÉS MEGFELELŐSÉGÉNEK FELMÉRÉSE M 3 – FÜGGETLEN ÉRTÉKELÉS VÉGEZTETÉSE M 4 – FÜGGETLEN ELLENŐRZŐ VIZSGÁLAT (AUDIT) VÉGEZTETÉSE
(5) 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 – KONFIGURÁCIÓ KEZELÉSE
b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljes körűségét biztosító ellenőrzésekről, eljárásokról,	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 12 – LÉTESÍTMÉNYE KEZELÉSE **M – FELÜGYELET** M 2 – BELSŐ ELLENŐRZÉS MEGFELELŐSÉGÉNEK FELMÉRÉSE
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 RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 7 – FELHASZNÁLÓK KÉPZÉSE DS 8 – INFORMATIKAI FELHASZNÁLÓK SEGÍTÉSE
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 AI 3 – TECHNOLÓGIAI INFRASTUKTÚRA BESZERZÉSE ÉS KARBANTARTÁSA AI 4 – INFORMATIKAI ELJÁRÁSOK KIFEJLESZTÉSE ÉS KARBANTARTÁSA

[3] Hivatkozás a Hpt., a Tpt., az Mpt és az Öpt előírásaira, amelyeknek ismerete és alkalmazása hasznos lehet a biztosítóknál is.

I. sz. melléklet: A törvényi előírások és a COBIT megfeleltetése

e) a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről,	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 11 – ADATOK KEZELÉSE
f) az adathordozók szabályozott és biztonságos kezeléséről,	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 11 – ADATOK KEZELÉSE
g) a rendszer biztonsági kockázattal arányos vírusvédelméről.	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 9 – KONFIGURÁCIÓ KEZELÉSE
(6) 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** PO 3 – TECHNOLÓGIAI IRÁNY MEGHATÁROZÁSA PO 10 – PROJEKTEK IRÁNYÍTÁSA **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 13 – ÜZEMELTETÉS IRÁNYÍTÁSA DS 6 – KÖLTSÉGEK MEGÁLLAPÍTÁSA ÉS FELOSZTÁSA
b) 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,	**PO – TERVEZÉS ÉS SZERVEZET** PO 11 MINŐSÉGIRÁNYÍTÁS **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 2 – KÜLSŐ SZOLGÁLTATÁSOK KEZELÉSE DS 3 – TELJESÍTMÉNY ÉS KAPACITÁS KEZELÉSE
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 KIDOLGOZÁSA PO 2– INFORMÁCIÓ-ARCHITEKTÚRA MEGHATÁROZÁSA PO 5– INFORMATIKAI BERUHÁZÁSOK KEZELÉSE **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 1– SZOLGÁLTATÁSI SZINTEK MEGHATÁROZÁSA DS 3 – TELJESÍTMÉNY ÉS KAPACITÁS KEZELÉSE DS 4 – A FOLYAMATOS MŰKÖDÉS BIZTOSÍTÁSA DS 10 – A PROBLÉMÁK ÉS RENDKÍVÜLI ESEMÉNYEK KEZELÉSE
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 5 – RENDSZEREK INSTALLÁLÁSA ÉS JÓVÁHAGYÁSA AI 6 – VÁLTOZÁSOK KEZELÉSE
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. 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 FOLYAMATOS MŰKÖDÉS BIZTOSÍTÁSA DS 11 – ADATOK KEZELÉSE
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 FOLYAMATOS MŰKÖDÉS BIZTOSÍTÁSA DS 11 – ADATOK KEZELÉSE
g) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 4 – A FOLYAMATOS MŰKÖDÉS BIZTOSÍTÁSA

I. sz. melléklet: A törvényi előírások és a COBIT megfeleltetése

	DS 10 – A PROBLÉMÁK ÉS RENDKÍVÜLI ESEMÉNYEK KEZELÉSE
(7) 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 PO 11– MINŐSÉGIRÁNYÍTÁS **AI – BESZERZÉS ÉS BEVEZETÉS** AI 1 – AUTOMATIZÁLT MEGOLDÁSOK MEGHATÁROZÁSA AI 2 – ALKALMAZÁSI SZOFTVEREK BESZERZÉSE ÉS KARBANTARTÁSA AI 4 – INFORMATIKAI ELJÁRÁSOK KIFEJLESZTÉSE ÉS KARBANTARTÁSA
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 **AI – BESZERZÉS ÉS BEVEZETÉS** AI 1 – AUTOMATIZÁLT MEGOLDÁSOK MEGHATÁROZÁSA AI 2 – ALKALMAZÁSI SZOFTVEREK BESZERZÉSE ÉS KARBANTARTÁSA
c) az informatikai rendszer elemeinek a pénzügyi intézmény által meghatározott biztonsági osztályokba sorolási rendszerének,	**PO – TERVEZÉS ÉS SZERVEZET** PO 2 – INFORMÁCIÓ-ARCHITEKTÚRA MEGHATÁROZÁSA **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA
d) az adatokhoz történő hozzáférési rend meghatározásának,	**PO – TERVEZÉS ÉS SZERVEZET** PO 2 – INFORMÁCIÓ-ARCHITEKTÚRA MEGHATÁROZÁSA PO 4 – AZ INFORMATIKAI RÉSZLEG SZERVEZETI FELÉPÍTÉSÉNEK ÉS KAPCSOLATAINAK MEGHATÁROZÁSA **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA
e) az adatgazda és a rendszergazda kijelölését tartalmazó okiratnak,	**PO – TERVEZÉS ÉS SZERVEZET** PO 4 – AZ INFORMATIKAI RÉSZLEG SZERVEZETI FELÉPÍTÉSÉNEK ÉS KAPCSOLATAINAK MEGHATÁROZÁSA
f) az alkalmazott szoftver eszközök jogtisztaságát bizonyító szerződéseknek,	**PO – TERVEZÉS ÉS SZERVEZET** PO 6 – VEZETŐI CÉLOK ÉS IRÁNYVONAL KÖZLÉSE **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 9 – KONFIGURÁCIÓ KEZELÉSE
g) az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 9 – KONFIGURÁCIÓ KEZELÉSE
(8) 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 KIDOLGOZÁSA PO 8 – KÜLSŐ KÖVETELMÉNYEK BETARTÁSÁNAK BIZTOSÍTÁSA PO 11 MINŐSÉGIRÁNYÍTÁS **AI – BESZERZÉS ÉS BEVEZETÉS** AI 5 – RENDSZEREK INSTALLÁLÁSA ÉS JÓVÁHAGYÁSA **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 1– SZOLGÁLTATÁSI SZINTEK MEGHATÁROZÁSA
b) a pénz és az értékpapírok biztonságos nyilvántartására,	**DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 11 – ADATOK KEZELÉSE
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 **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 11 – ADATOK KEZELÉSE
d) a tárolt adatok ellenőrzéséhez való felhasználására	**AI – BESZERZÉS ÉS BEVEZETÉS** AI 2 – ALKALMAZÁSI SZOFTVEREK BESZERZÉSE ÉS KARBANTARTÁSA

I. sz. melléklet: A törvényi előírások és a COBIT megfeleltetése

	DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 11 – ADATOK KEZELÉSE
e) a biztonsági kockázattal arányos logikai védelemre és a sérthetetlenség védelmére.	**AI – BESZERZÉS ÉS BEVEZETÉS** AI 2 – ALKALMAZÁSI SZOFTVEREK BESZERZÉSE ÉS KARBANTARTÁSA **DS – INFORMATIKAI SZOLGÁLTATÁS ÉS TÁMOGATÁS** DS 5 – A RENDSZER BIZTONSÁGÁNAK MEGVALÓSÍTÁSA DS 11 – ADATOK KEZELÉSE
(9) A pénzügyi intézménynek belső szabályzatában meg kell határoznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.	**PO – TERVEZÉS ÉS SZERVEZET** PO 7 – EMBERI ERŐFORRÁSOK KEZELÉSE

II. sz. melléklet: A COBIT kézikönyvek csoportosítása, elérhetőség

II. MELLÉKLET: A COBIT KÉZIKÖNYVEK CSOPORTOSÍTÁSA, ELÉRHETŐSÉG

II.1. INFORMATIKAIRÁNYÍTÁS (IT GOVERNANCE)

Cím	Ingyenes letöltés az internetről (ISACA web profile létesítése nélkül)	Megvásárolható az alábbi Internet címen
Board Briefing on IT Governance	http://www.isaca.org/downloads	http://www.isaca.org/bookstore
IT Governance Executive Summary	http://www.isaca.org/downloads	
Information Security Governance: Guidance for Boards of Directors and Executive Management	http://www.isaca.org/downloads	http://www.isaca.org/bookstore
IT Governance Implementation Guide	nem lehetséges	http://www.isaca.org/bookstore

II.2. EGYSZERŰSÍTETT COBIT KEZDŐKNEK

Kézikönyv és felmérő program	Ingyenes letöltés az internetről (ISACA web profile létesítése után)	Megvásárolható az alábbi Internet címen
COBIT Quickstart	nem lehetséges	http://www.isaca.org/quickstart

II.3. COBIT ALAPKÖNYVEK

Cím	Ingyenes letöltés az internetről (ISACA web profile létesítése után)	Megvásárolható az alábbi Internet címen
COBIT And Related Products Brochure	http://www.isaca.org/ Tovább: Governance / COBIT / Obtain COBIT	
COBIT Executive Summary Magyar fordításban: COBIT Összefoglaló áttekintés	http://www.isaca.org/ Tovább: Governance / COBIT / Obtain COBIT http://www.pszaf.hu/	 http://www.isaca.hu/
COBIT Framework Magyar fordításban: COBIT Keretrendszer	http://www.isaca.org/ Tovább: Governance / COBIT / Obtain COBIT http://www.pszaf.hu/	http://www.isaca.org/bookstore http://www.isaca.hu/
COBIT Control Objectives Magyar fordításban: COBIT Kontroll célkitűzések	http://www.isaca.org/ Tovább: Governance / COBIT / Obtain COBIT http://www.pszaf.hu/	http://www.isaca.org/bookstore http://www.isaca.hu/
COBIT Management Guidelines	http://www.isaca.org/ Tovább: Governance / COBIT / Obtain COBIT	http://www.isaca.org/bookstore
COBIT Audit Guidelines	Csak ISACA tagoknak: http://www.isaca.org/ Tovább:	http://www.isaca.org/bookstore

II. sz. melléklet: A COBIT kézikönyvek csoportosítása, elérhetőség

	Governance / COBIT / Obtain COBIT	
COBIT Implementation Tool Set Magyar fordításban: COBIT Alkalmazási módszerek	http://www.isaca.org/ Tovább: Governance / COBIT / Obtain COBIT http://www.pszaf.hu/	http://www.isaca.org/bookstore http://www.isaca.hu/

II.4. A COBIT CÉLKITŰZÉSEK MEGVALÓSÍTÁSA

Cím	Ingyenes letöltés az internetről (ISACA web profile létesítése után)	Megvásárolható az alábbi Internet címen
COBIT Control Practices	nem lehetséges	http://www.isaca.org/bookstore

II.5. A COBIT INTERNETES VÁLTOZATA (A CONTROL PRACTICES BEÉPÍTÉSÉVEL)

Cím	Ingyenes letöltés az internetről (ISACA web profile létesítése után)	Éves előfizetés az alábbi Internet címen
COBIT Online	nem lehetséges	http://www.isaca.org/cobitonline

II.6. EGYÉB COBIT

Cím	Ingyenes letöltés az internetről (ISACA web profile létesítése után)	Megvásárolható az alábbi Internet címen
COBIT Security Baseline	http://www.isaca.org/downloads	http://www.isaca.org/bookstore
	Ingyenes letöltés az internetről (ISACA web profile létesítése nélkül)	
COBIT Mapping: Overview of International IT Governance	http://www.isaca.org/downloads	
IT Control Objectives for Sarbanes-Oxley	http://www.isaca.org/downloads	http://www.isaca.org/bookstore

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

III. MELLÉKLET: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA.

Adat
Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

Adatállomány
Valamely informatikai rendszerben lévő adatok logikai vagy fizikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

Adatgazda: az a személy, aki élve a pénzügyi intézmény által biztosított jogosultságával adatot minősít, illetve osztályba sorol és felelős az általa minősített adat kezeléséért.

Adatbázis
Elektronikus formában, digitálisan tárolt információk összessége.

Adatbiztonság
Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatfeldolgozás
Az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adatfeldolgozó
Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Adatkezelés
Az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is.

Adatkezelő
Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adattovábbítás
Ha az adatot meghatározott harmadik személy vagy alkalmazás számára hozzáférhetővé teszik.

Adattörlés
Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem lehetséges.

Adatvédelem
Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik.

Adminisztratív védelem
Szervezési és szabályozási úton megvalósított védelem.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Alapfenyegetettségek
A fenyegetések általánosított csoportosítása. Ide soroljuk: a bizalmasság, a hitelesség, a sértetlenség, a letagadhatatlanság, a rendelkezésre állás és a funkcionalitás sérülését vagy elvesztését.

Alkalmazás: alkalmazáson a pénzügyi intézmény valamely üzleti célja megvalósítása vagy megvalósulásának támogatása érdekében elkülönülő, saját néven egységbe szervezett hardver-szoftver-kommunikációs erőforrásainak együttesét értjük. Az alkalmazásokra az ember-számítógép együttműködés jellemző. Az alkalmazáshoz tartozónak tekintjük a tevékenységet támogató/hordozó, meghatározott üzleti-, banki-, szervezeti-, stb. cél elérése érdekében a pénzügyi szervezet teljes informatikai rendszerére alapozva kidolgozott technológiát ("know-how"-t) valamint a beépített elméleti modellt az alkalmazás dokumentációjával együtt.

Alkalmazói program (alkalmazói szoftver)
Olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja.

Alkalmazási (éles) (rendszer) környezet: a pénzügyi intézmény informatikai rendszerébe tartozó mindazon komponensek összessége, amelyet az adott alkalmazás rendeltetésszerű működtetése érdekében érvényes eredményt/tranzakciót előállító módon bevon. Az éles környezet működési eredményének érvényessége az a körülmény, amely éles ellentétben áll az összes többi környezet (fejlesztő, teszt) eredményeinek jellegével.

Alkalmazás Felhasználó: Az a pénzügyi intézmény, amely az alkalmazást saját üzletei céljai megvalósításába - szállító és vagy szolgáltató esetleges közreműködésével — bevonja.

Alkalmazás Szállító: Az alkalmazás fejlesztője/gyártója/közvetítője, licencének kibocsátója, aki az alkalmazás hibák kiküszöbölésére vagy a megváltozó igények kielégítésére rendszerverziókat állít elő.

Alkalmazás Szolgáltató: Az alkalmazáshoz tartozó IT erőforrásokat a felhasználó pénzügyi intézmény elvárásai szerint IT szolgáltatásként hozzáférhetővé tévő szervezeti egység (esetleg szerződő cég). A szolgáltató feladata a felhasználó felhatalmazása alapján a szállító által rendelkezésre bocsátott verziók érvényre juttatása, vagyis a verzióváltás. A felhasználó, a szállító és a szolgáltató lehet ugyanaz a cég is.

Átlagos helyreállítási idő
A hibák behatárolására és megszüntetésére fordított kényszerű leállások átlagos ideje.

Archiválás: Az alkalmazás (tágabb értelemben az informatikai rendszer) egy-egy környezetének (tehát nem csak adattartalmának) különleges mentése. Különleges, mivel az archivált és a visszamaradó rendszernek is logikailag épnek, visszaállíthatónak kell lennie. Az archiválás — ellentétben a mentéssel — általában nem elsősorban biztonsági, hanem hatékonyság javító üzemviteli intézkedés (legtöbbször a visszamaradó környezet/rendszer felgyorsítása érdekében).

Backup rendszer
Az informatikai biztonság megvalósítása során az adatok rendelkezésre állását lehetővé tevő másolatokat őrző rendszer. Rendszerint minimális tartalékkal rendelkező informatikai rendszert is értenek alatta.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

BCP
Business Continuity Planning (lásd *Üzletmenet folytonosság tervezés*).

Bizalmasság: (szervezeti állapot) A pénzügyi intézmény olyan állapota, amely biztosítja, hogy az adatokhoz csak azok a meghatalmazottak férhessenek hozzá, akiknek a szervezet ehhez jogot adott. (adat tulajdonság) A *~bizalmasság* a kezelőrendszer által az adatokhoz rendelt tulajdonság, amely jelzi/kifejezi az adat osztályba sorolásának megfelelő védelmi intézkedések teljesülését. Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

Biztonság: olyan szervezeti állapot, melyben az adott szervezetnek a lehető legkisebb veszélyekkel kell számolnia, szolgáltatásait a vállalt/előírt feltételekkel és korlátozások nélkül képes nyújtani, a feladatait, funkcióinak ellátását illetően érdemi hatást gyakorló veszteség nem éri, a lehetséges fenyegetettségek bekövetkezési valószínűségéből és a lehetséges kárértékekből származtatott kockázat a szervezet számára elfogadhatóan alacsony, és a kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elviselhető tartományban marad. A védeni kívánt informatikai rendszer olyan, az adott intézmény számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét bizalmasságát és hitelességét erősítik.

Biztonsági auditálás
Az informatikai rendszerre vonatkozó feljegyzések és tevékenységek független átvizsgálása, a rendszer ellenőrzések megfelelőségének vizsgálata, a kialakított szabályzatok és a működtetési eljárások megfelelőségének elérése, a biztonság gyenge pontjainak felfedése az ellenőrzésben, a szabályzatokban és az eljárásokban ajánlott biztonsági változtatások céljából.

Biztonsági esemény
Az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, amelynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet.

Biztonsági igény
Olyan elvárás, vagy elérendő célkitűzés, amely abban az esetben áll fenn, ha egy vagy akár több kockázat elfogadhatatlanul magas és ezért valamit az informatikai rendszer védelme érdekében tenni kell.

Biztonsági kockázat (informatikai kockázat): valószínűségi mérték, amely az informatikai rendszer működését veszélyeztető valamely körülmény bekövetkezési valószínűségével , illetve a bekövetkezéskor várható kár nagyságával egyaránt arányos. Rendre élőmunka igényben, időben, pénzben vagy ezek együttesében fejezhető ki.

Biztonsági környezet
A jogszabályok, a gazdasági szervezet belső szabályai, és elvárásai, szokások, szakértelem és tudás, amelyek meghatározzák azt a környezetet, amelyben az erőforrásokat az intézmény használni akarja.

Biztonsági követelmények
A kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Biztonsági mechanizmus
Olyan eljárás, módszer vagy megoldási elv – ami lehet számítástechnikai műszaki tartalmú is –, amely valamilyen biztonsági követelmény(eke)t valósít meg.

Biztonsági osztályba sorolás
Az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó védelmi szintet meghatározó besorolása, osztályozása.

Biztonsági rés
Az informatikai rendszer védelme érdekében a legkülönbözőbb területeken kell intézkedéseket hozni. A megelőző, elővigyázatossági intézkedések érinthetik az építészeti, a műszaki, a szervezési és a személyi kérdéseket. Az intézkedéseket egymással össze kell hangolni, és egy informatikai biztonsági szabályozási rendszerben kell összefoglalni. Tudatában kell lenni annak, hogy – mint általában – egyetlen informatikai rendszer biztonsága sem lehet száz százalékos. Tökéletes megoldás nem létezik. Az értelemszerűen fennmaradó maradványkockázatokat azonban ismerni kell, és figyelembe kell venni. A szabályozási rendszer kidolgozásakor a cél ezen maradványkockázatok elviselhető szintre szorítása. A védelmi igény mértéke függ a bevezetendő informatikai rendszer tulajdonságaitól és a bevezetés környezetétől is.

CA
Certification Authority (lásd *Hitelesítés Szolgáltató*).

Cracker
Az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal betörő személy.

CRAMM
CCTA Risk Analysis and Management Method. Az Egyesült Királyság Central Computer and Telecommunication Agency szervezete által kidolgozott kockázatelemzési és kezelési módszertan.

Demo szoftver
Számos licence köteles szoftver gyártója ingyenesen vagy csekély költség ellenében (demonstrációs azaz demo) próbaverziókat bocsát ki. E szoftverek célja a bemutatás, tesztelés és kipróbálás, ennek megfelelően funkcionalitásuk sok esetben nem teljes, és használatuk általában időkorláthoz kötött. Ezeket a szoftververzziókat tilos üzleti célra felhasználni.

Disztributív mentés
Az a mentési megoldás, ha az egy csoportba tartozó felhasználók a saját számítógépeiken a saját adatbázisukról helyileg készítenek másolatot.

DRP
Disaster Recovery Planning (lásd *Katasztrófahelyzet elhárítás tervezés*).

Digitális aláírás (Lásd *Elektronikus aláírás*.)

Egyenszilárdság
A biztonság az intézmény tevékenységét teljesen átfogja, és annak minden pontján azonos erősségű.

Egyszeri javítási idő
Az informatikai rendszer egyszeri javítási ideje, amely a hiba észlelésétől az informatikai rendszer normál üzembe való visszatéréséig tart.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Elektronikus aláírás
Az informatikai rendszerben kezelt adathoz rendelt, kódolással előállított olyan jelsorozat, amely az adat hitelességének és sértetlenségének bizonyítására használható.

Elérhetőség
Az az állapot, amikor az információ feldolgozás során valamely informatikai alkalmazás szolgáltatásai az adott helyen és az adott időben igénybe vehetők.

Ellenőrzési nyom
Az informatikai tevékenységek rögzítésére szolgál, amelynek alapján az illegális, illetve nem megfelelő tevékenységek feltárásra, jelentésre kerülhetnek.

Elöregedési időszak
Egy informatikai termék életgörbéjének utolsó szakasza, amelyben a meghibásodási tényező ismét növekszik, a rendszerelemek minősége pedig az irreverzibilis változások miatt romlik.

Érték
Az információk és feldolgozásuk értéke abból vezethető le, hogy azok milyen jelentőséggel rendelkeznek a felhasználó által támasztott követelmények kielégítése szempontjából. Az informatikai rendszerelemek értéke pedig azon információk és feldolgozásuk értékéből származtatható, amelyek az adott rendszerelem igénybevételével megvalósuló eljárásokban részt vesznek.

Fejlesztői (rendszer) környezet: az alkalmazás szállító / fejlesztő szervezet informatikai rendszerébe tartozó mindazon komponensek összessége, amelyet egy adott pénzügyi jellegű rendeltetésű alkalmazás előállítása érdekében állítanak össze. Fejlesztő környezet érvényes eredményt/tranzakciót előállító módon nem működhet.

Feladatelhatárolás
Az informatikai rendszer használatához és üzemeltetéséhez kapcsolódó biztonságkritikus munkakörök szétválasztása.

Felelősségre vonhatóság
Olyan tulajdonság, amely lehetővé teszi, hogy egy adott folyamat tevékenységei egyértelműen az adott folyamatra legyenek visszavezethetők.

Felhasználó
Az a személy, szervezet vagy csoport, aki (amely) egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.

Felhasználói hitelesítés
A felhasználó hitelességének ellenőrzése (a belépéskor minden felhasználó ellenőrzése), és különböző azonosító eszközök (pl.: jelszó, chip-kártya, biometrikus azonosítás stb.) alkalmazása.

Felhasználói program (felhasználói szoftver) (Lásd *Alkalmazói program*.)

Fenyegetés
A biztonság megsértésének lehetősége.

Fenyegetettség
Olyan állapot, amelyben az erőforrások felfedésre, módosításra vagy elpusztításra kerülhetnek.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Fenyegetettség elemzés
Valamennyi jelentős informatikai fenyegető tényező meghatározása.

Fenyegető tényező
Olyan körülmény vagy esemény, amely az adat, illetve információ valamely informatikai rendszerben történő feldolgozásának rendelkezésre állását, sértetlenségét, bizalmasságát vagy hitelességét, illetve az informatikai rendszernek és a rendszer elemeinek működőképességét fenyegetheti. A fenyegető tényezők közé soroljuk nemcsak a személyektől eredő támadásokat, amelyek valamely informatikai rendszer ellen irányulnak, hanem valamennyi szélesebb értelemben vett fenyegetést, mint például véletlen eseményeket, külső tényezők általi behatásokat és olyan körülményeket, amelyek általában magának az informatikának a sajátosságaiból adódnak. (Példaként említhetjük a tüzet, az áramkimaradást, az adatbeviteli hibát, a hibás kezelést, a hardver tönkremenetelét, a számítógépes vírusokat és a különböző programhibákat.)

Féreg program
Olyan programtörzs, amely az informatikai hálózaton keresztül terjed, jut el egyik informatikai rendszerből a másikba, és fejt ki kártékony hatását.

Fizikai biztonság
Erőforrások szándékos és véletlen fenyegetései elleni fizikai védelemre használt intézkedések, illetve az anyagi térben megvalósuló szándékos vagy véletlen támadások elleni védelem.

Fizikai védelem
(Lásd *Fizikai biztonság*.)

Folyamatosság
Az üzleti tevékenységek zavarmentes rendelkezésre állása.

Folytonos védelem
Olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

Freeware szoftver
Olyan ingyenesen, licence kötelezettség nélkül használható szoftver, amelynek alkotói lemondtak a szerzői jogi védelemről.

Funkcionalitás
Az informatikai rendszerelem (beleértve az adatokat is) olyan tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a kezelési céloknak megfelel, és használható.

Gyenge pont
Az informatikai rendszerelemek olyan részei vagy tulajdonságai, amelyek révén a fenyegető tényezők hatásainak ki vannak téve.

Hacker
Az informatikai rendszerbe informatikai eszközöket használva, kifejezetten ártó szándék nélküli betörő személy.

Hálózat
Számítógépek (vagy általánosabban informatikai rendszerek) összekapcsolása, és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Hálózati együttműködés
Eszközök közötti együttműködés azonos kommunikációs szabványok alapján.

Hash-függvény
Olyan transzformáció, amely egy tetszőleges hosszú szöveg egyedi, az adott szövegre jellemző fix hosszúságú digitális sűrítményét készíti el.

Hasznos élettartam
Egy informatikai termék életgörbéjének középső, egyenletes szakasza, amelyen belül a meghibásodási tényező gyakorlatilag állandó.

Háromgenerációs elv
Az informatikai rendszer megvalósításához, és az adatok rendelkezésre állásának biztosításához szükséges olyan megoldás, amely a legutolsó három mentésből állítja vissza az informatikai rendszer működőképességét.

Helyreállítás
A katasztrófa következtében megsérült erőforrások eredeti állapotának biztosítása, eredeti helyen.

Hibamentes működés valószínűsége
Annak a valószínűsége, hogy adott időszakaszban, előírt működési és környezeti feltételek mellett, nem következik be meghibásodás.

Hitelesítés Szolgáltató
(CA – Certification Authority) Olyan mindenki által megbízhatónak tartott, szakosodott szervezet, amely tanúsítványokat adhat ki kliensek és szerverek számára.

Hitelesség: Egy adat hiteles, ha minden kétséget kizáróan megállapítható annak előállítója és az a tény, hogy az az előállítás óta változatlan maradt. A hitelesség tehát az adat (és az adathordozó) tulajdonsága, amellyel igazolhatjuk, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

Hozzáférés
Olyan eljárás, amely valamely informatikai rendszer használója számára – jogosultságának függvényében - meghatározott célra, helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait, elérhetővé tesz a rendszerben adatokként tárolt információkat. Ez az eljárás bekövetkezhet például névmegadáson keresztül valamely adatszerűségre nézve, és lehetővé tehet olvasást, írást vagy akár törlést is.

Hozzáférés ellenőrzés
Az informatikai erőforrásokhoz való jogosulatlan hozzáférések elhárítása, beleértve az erőforrások jogosulatlan használatának megakadályozását is.

Hozzáférés ellenőrzési lista
Az informatikai erőforrásokhoz való hozzáférésre jogosult entitások és hozzáférési jogaik jegyzéke.

Humánbiztonság
Az erőforrások bizalmasságának és/vagy sértetlenségének és/vagy rendelkezésre állásának sérelmére – az intézménnyel munkaviszonyban álló vagy az intézménynél bármely szerződés alapján tevé-

kenységet folytató vagy külső személyek által – elkövethető szándékos vagy véletlen humántámadások elleni védettség.

Illegális szoftver
Az a szerzői jog védelme alatt álló szoftvertermék, amelynek a legalitás igazolásához szükséges dokumentumok (licence, számla, szállítólevél, ajándékozási szerződés stb.) nem mindegyike áll rendelkezésre, valamint a szoftver használata nem felel meg a licence szerződés előírásainak.

Illetéktelen személy
Olyan személy, aki az adat megismerésére nem jogosult.

Informatika
A számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

Informatikai biztonság: A pénzügyi intézmény informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljeskörű, folytonos és a kockázatokkal arányos.

Informatika-biztonsági felelős
Olyan személy, aki a pénzáton belüli biztonság megvalósításáért felel. Részt vesz az informatika biztonsági politika és szabályozás kidolgozásában, oktatásában, aktualizálásában, felelős annak ellenőrzésében és betartatásában.

Informatika-biztonsági terv
Olyan az éves informatikai terv részét képező költségvetési és egyéb erőforrásokra vonatkozó, az IT biztonsággal kapcsolatos hardver-, szoftver-, oktatási-, szabályozási- és egyéb dokumentumok.

Informatikai rendszer: A hardver-, szoftver- kommunikációs eszközök és ezek kezelő/kiszolgáló szervezeteinek olyan együttese, amelyet a pénzügyi intézmény üzletpolitikájával összhangban céljai megvalósítására használ.

Informatikai katasztrófa
Egy olyan nem kívánt esemény, amely az adattovábbító, -tároló és -feldolgozó képesség elvesztését okozza hosszabb időre.

Informatikai katasztrófahelyzet
Az az állapot, amikor egy rendszer utolsó működőképes állapotát a megállapított helyreállítási időn belül nem lehet visszaállítani.

Informatikai katasztrófa utáni helyreállítási terv
Eljárás vagy tevékenység lépések sorozata annak biztosítására, hogy a szervezet kritikus információ feldolgozó képességeit katasztrófa után, a szükséges aktuális adatokkal helyre lehessen állítani elfogadhatóan rövid idő alatt.

Informatikai rendszer

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Információs, ügyviteli, üzletviteli vagy folyamatot, szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, valamint az ezeket kiszolgáló emberi erőforrások és a kapcsolódó folyamatok összessége.

Informatikai rendszerelem
Az informatikai rendszer olyan jól elkülöníthető egysége, amely annak bevezetéséhez/kiépítéséhez szükséges és amelyet a fenyegető tényezők érintenek.

Informatikai rendszerelemzés
Olyan vizsgálat, amelyet valamely informatikai rendszer beszerzése és bevezetése előtt valósítanak meg, hogy a vele szemben támasztott követelményeket rögzítsék. Alapja az informatikai rendszer bevezetésének a célja, valamint a bevezetés környezete.

Informatikai vészhelyzet
Egy olyan nem kívánt állapot, amely az intézmény rendelkezésére álló informatikai biztonsági rendszer szabályainak előírásszerű betartásával és végrehajtásával, a meghatározott erőforrások felhasználásával meghatározott időn belül megoldható.

Információ
Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott olyan megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg. Az információ általános értelemben a valóság folyamatairól és dologi viszonyairól szóló felvilágosítás.

Információrendszer
Információk meghatározott célú, módszeres gyűjtésére, tárolására, feldolgozására (bevitelére, módosítására, rendszerezésére, aggregálására) továbbítására, fogadására, megjelenítésére, megsemmisítésére stb. alkalmas rendszer. Ha ez a rendszer számítógéppel támogatott, akkor számítógépes információrendszerről (informatikai rendszerről) beszélünk.

Információvédelem
Az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.

Irányelvek
A szervezet vezetése által is elfogadott, követett és kommunikált általános szabályok ismertetése. A szabályozási struktúra legfelsőbb szintje, amelynek részletes megvalósítása a szabályozási struktúra további elemeiben (utasítások, körlevelek, szabályzatok, eljárásrendek, kézikönyvek, stb.) találhatók meg.

Jogosultság
A lehetőség megadása az informatikai rendszerben végzendő tevékenységek végrehajtására.

Jogosultsággal rendelkező felhasználó
Egy olyan felhasználó, aki jogosult egy tevékenység végrehajtására.

Kár
Azon érték csökkenése, amelyet valamely objektum jelent egy informatikai rendszer alkalmazásában és amely akkor következik be, ha valamely fenyegető tényező kifejti hatását.

Katasztrófa

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Az informatikai rendszer folyamatos és rendeltetésszerű működésének megszakadása.

Katasztrófahelyzet elhárítás tervezés
Az informatikai rendszer rendelkezésre állásának megszűnése, nagy mértékű csökkenése utáni visszaállításra vonatkozó tervezés. (DRP – Disaster Recovery Planning)

Kezdeti időszak
Egy informatikai termék életgörbéjének eleje, amelyre a meghibásodási tényező fokozatos csökkenése jellemző.

Klienskategória
Az adott intézmény kliensszámítógépeinek konfigurációját leszabályozó olyan kategóriarendszer, amely elősegíti, hogy a felhasználók számítógépein az optimális működéshez szükséges szoftverek és csak azok legyenek telepítve.

Klienskonszolidáció
A klienskategóriákra alapuló olyan folyamat, amely az adott intézmény minden kliensszámítógépét egységessé teszi, így könnyítve meg a nyilvántartást és a hatékony szoftvergazdálkodást.

Kockázat
Az informatikai fenyegetettség mértéke, amely valamely fenyegető tényezőből ered és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze.

Kockázatelemzés
Olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési gyakoriságát.

Kockázatkezelés
Védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak.

Kockázatmenedzsment
(Lásd *Kockázatkezelés*.)

Kockázatarányos védelem: az a védelem, mely a kockázatokat a releváns fenyegetettségek bekövetkezési valószínűsége és a fenyegetettség bekövetkezésekor keletkező kár függvényeként kezeli, és ahol a védelemre fordított erőforrások értéke arányos a védendő értékek nagyságával, illetve kockázatcsökkentő képességével.

Környezeti biztonság
Az informatikai erőforrások rendelkezésre állásának és sértetlenségének a természeti katasztrófákkal szembeni védettsége.

Kötelező hozzáférés-védelem
A szubjektumokhoz, és az objektumokhoz egy jelző (címke) van rendelve, azok titokvédelmi osztályozása szerint A hozzáférés akkor engedélyezhető, ha a szubjektum titokvédelmi osztályozása uralkodik az objektum titokvédelmi osztályozása felett.

Közérdekű adat

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat.

Központi mentés
Az a mentési eljárást, amikor egy hálózatos rendszerben a szétszórt, vagy a hálózat egy-egy csomópontjában található adatokat egy kijelölt csomóponti számítógépen tárolják, vagy erre átmozgatják, és ezen a számítógépen készül a mentés.

Kriptoanalízis (kriptográfiai bevizsgálás)
A rejtjeles üzenet illetéktelenek által, azaz a dekódolási eljárás ismerete nélkül, vagy annak részleges ismeretében az eredeti üzenet visszaállításának kísérlete.

Kriptográfia
Mindazoknak a matematikai eljárásoknak, algoritmusoknak és biztonsági rendszabályoknak a kutatása és alkalmazása, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.

Kriptológia
A kriptoanalízis és a kriptográfia elméletének és gyakorlatának együttese.

Kritikus helyreállítási idő: Az az időtartam, ameddig az intézmény szolgáltatás nyújtása (bármilyen okból) anélkül szünetelhet, hogy emiatt komoly anyagi vagy erkölcsi veszteség érné. Egy-egy alkalmazáshoz (tágabb értelemben az egész informatikai rendszerhez) rendelt időtartam, méghozzá maximálisan megengedett időtartam, mely időtartamú alkalmazás, illetve rendszer-kiesést a pénzügyi intézmény feladataira, kötelezettségeire is tekintettel még eltűr anélkül, hogy általa elviselhetőnek ítélt veszteségeket meghaladó anyagi és/vagy nem anyagi jellegű kár érné.

Különleges adat
A faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre, az egészségi állapotra, a kóros szenvedélyre, a szexuális életre, valamint a büntetett előéletre vonatkozó személyes adatok.

Legális szoftver
Az a szerzői jog védelme alatt álló szoftvertermék, amelynek legalitásának igazolásához minden szükséges dokumentum (licence, számla, szállítólevél, ajándékozási szerződés stb.) rendelkezésre áll, valamint a használata a szoftver licence szerződés előírásainak megfelelő módon történik.

Logikai bomba
A vírus olyan része, illetve szerkezete, amelyik időhöz, esemény bekövetkezéséhez, logikai változó adott értékéhez kötött módon aktivizálódik.

Logikai védelem
Az informatikai rendszerekben informatikai eszközökkel megvalósított védelem.

Mentés, Mentési rend: Az alkalmazás (tágabb értelemben az informatikai rendszer) egy-egy környezetének (tehát nem csak adattartalmának) alkalmas hordozóra történő másolása a mentett környezet épségének megbontása nélkül.
A mentés általában biztonsági érdekből, a mentett környezet visszaállításának céljával készül. A mentési rend a mentett környezet elemeinek meghatározásából, a mentés körülményeinek előírásából áll, ide sorolva a mentett környezet állapotának megszabását, a mentés időpontjának- vagy időszakának előírását, a mentés periodicitásának megszabását, kezelési / őrzési / tárolási előírásokat, a tárolási helyre vonatkozó előírásokat, az alkalmazandó jelzéseket/nyilvántartásokat, frissítési szabályokat, stb. A mentési utasítás célja a későbbi sikeres felhasználás/visszaállítás garantálása.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Maradványkockázat
Az tudatosan felvállalt kockázat, amely alapvetően – kis mértékben – annak ellenére is fennmarad, hogy a fenyegető tényezők ellen intézkedések eredményesen végrehajtásra kerültek.

Megbízható működés
Az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.

Megbízhatóság
A megbízhatóság műszaki értelemben egy informatikai rendszerelemnek vagy rendszernek az a jellemzője, amely megadja, hogy az üzemeltetési feltételek fenntartása esetén milyen mértékben várható el annak hibátlan, rendeltetésszerű működése.
A megbízhatóság matematikai értelemben egy statisztikai fogalom, amely annak a valószínűségét adja meg, hogy egy rendszerelem, vagy rendszer jellemzői az előírt határok közé esnek.

Meghibásodási tényező
Az informatikai rendszer (vagy rendszerelemek) megbízhatóságát jellemző olyan mutatószám, amely megadja, hogy adott időpont után, kis időegységen belül, az informatikai rendszerelemnek mekkora a meghibásodás valószínűsége, feltéve, hogy az adott időpontig az eszköz nem hibásodott meg.

Meghibásodások közötti átlagos működési idő
Az informatikai rendszerek megbízhatóságának jellemzésére gyakran használt mennyiségi mutató, a két egymást követő meghibásodás közötti hibátlan működés átlagos ideje.

Meg nem kerülhetőség
Annak biztosítása, hogy egy védelmi intézkedést nem lehet más úton kijátszani.

Megoldás (desifrírozás)
A rejtjeles üzenet legális címzettje által, a dekódolási eljárás ismeretében az eredeti üzenet visszaállítása.

Megszemélyesítés
Egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel.

Mentés
Az az informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt, vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.

Mentési médium
Az az adathordozó (a legtöbbször mágneses elven működő szalagos egység), amelyen a mentések által duplikált adattartalmat tárolják.

Mentő eszköz
Minden olyan informatikai berendezés, amely segítségével az informatikai rendszerben meglévő adatbázisokról elektronikus másolat készíthető.

Mentő szoftver

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Olyan szoftver, amely az operációs rendszer és a mentő eszköz közötti kapcsolatért felelős, továbbá ennek a feladata biztosítani, hogy az adatbázis duplikációját speciális körülmények között is el lehessen a mentési médiumra készíteni.

Minősítés
Az a döntés, amelynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik.

Működőképesség
A rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal. Ezen állapot fenntartásának alapfeladatait a rendszeradminisztrátor (rendszergazda) látja el.

Működési zavar, rendkívüli esemény: Az IT rendszer működési folyamatában beálló rendellenesség, szabálytalanság. Eltérés a rendeltetésszerű működéstől.

Naplózás
A felhasználói jogosultságok rögzítésére, dokumentálására szolgáló, és a számonkérést biztosító funkció a hozzáférés-védelemben.

Négy szem elv
Olyan tevékenység, amelyet csak két személy, egymást ellenőrizve végezhet.

Nyilvános Kulcsú Infrastruktúra
A Hitelesítés Szolgáltatónak nemzetközi feltételeket, szabványokat kielégítő biztonságos rejtjelzési módszereit, a személyzetre, a fizikai és az informatikai környezetre kiterjesztő infrastruktúrája.

Nyilvános kulcsú rendszer
Olyan kriptográfiai rendszer, amelynek a résztvevői közös algoritmust használnak a rejtjelzésre és a megoldásra. A rejtjelző algoritmusnak két – a használótól függő – kulcsa van. Ezek egyikét (nyilvános kulcs) a nevükkel együtt nyilvánosságra hozzák, a másikat pedig titokban tartják (titkos kulcs). A kulcsok egyikét a rejtjelzésre, a másikat a megoldásra használják.

Nyilvánosságra hozatal
Az adatnak meghatározhatatlan körben, mindenki részére biztosított megismerhetővé, hozzáférhetővé tétele.

Papíralapú információhordozó
Az információk valamennyi olyan megjelenítési változatának meghatározására szolgál, amelyek papíron állnak rendelkezésre és amelyek az informatikai rendszer használatával, illetve üzemeltetésével összefüggésben vannak.

Passzív fenyegetés
Az információ jogosulatlan nyilvánosságra hozásának veszélye az informatikai rendszer állapotának változása nélkül.

PKI
Public Key Infrastructure (lásd *Nyilvános Kulcsú Infrastruktúra*).

Probléma
Olyan egyedi, jelentős hatású zavaró esemény, amely hatása nagymértékben rontja a felhasználók számára nyújtott informatikai szolgáltatás minőségét.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Program
Olyan eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.

Próbaverzió
(Lásd *Demo szoftver*..)

Public Key Cryptosystem
(Lásd *Nyilvános kulcsú rendszer*.)

Rejtjelzés
Nyílt üzenet kódolása kriptográfiai eljárással, eszközzel vagy módszerrel. A rejtjelzés eredménye a rejtjeles üzenet.

Rendelkezésre állás: Az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai állandóan, illetve egy meghatározott időben hozzáférhetők és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

Rendszer
Az egymással valamilyen meghatározható kapcsolatban álló elemek összessége.

Rendszerelemek
Az adatokat „körülvevő", az informatikai rendszer részét képező elemek.

Rendszerprogram (rendszerszoftver)
Olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardverei használhatók legyenek és az alkalmazói programok működjenek. (A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.)

Rendszerszervezés
Az intézményben végbemenő folyamatok, valamint irányításuk és ellenőrzésük szervezése.

Rendszergazda: az a szervezeti egység vagy személy, amely vagy aki az adott rendszer üzleti elvárás szerinti működtetéséért felelős.

Rendszer leírás: célszerűen használható, de nem pontos összefoglaló fogalom, amely a pénzügyi jellegű rendeltetésű alkalmazás (informatikai rendszer) vagy az ezekhez tartozó rendszerelem dokumentációját jelöli. A pontos megjelölés a pénzügyi intézmény (vagy alkalmazás szolgáltató vagy alkalmazás szállító) belső ellenőrzési rendszerében előírt, szabványos specifikáció, rendszer/modul terv, fejlesztési dokumentum, tesztelési jegyzőkönyv, üzemeltetési utasítás, felhasználói utasítás, stb. lenne.

Rendszer modell: absztrakt elgondolás, amely a pénzügyi jellegű rendeltetésű alkalmazás folyamatainak-, műveleteinek leírásából, az ezeket kiszolgáló adatmodell meghatározásából, a csatlakozó szervezeti-, emberi- gépi tevékenységek vezérlési rendjéből, adatáramlási rendjéből, ellenőrzési/működtetési kritériumaiból áll, ide sorolva a csatlakozó rendszerek interfészeinek-, valamint a működőnek feltételezett rendszer technológiai leírását is.

Sebezhetőség
A veszélyforrás képezte támadás bekövetkezése esetén az erőforrások sérülésének lehetősége.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Sebezhetőségi ablak
Az informatikai szolgáltatás megszakadását követő időtartam, amelyet normális működési rendjének és tevékenységének megszakadása nélkül képes az intézmény elviselni.

Sértetlenség: Az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, ép, módosulatlan. Informatikai rendszer tulajdonság, amely adott, ha a rendszerben kezelt adatokat, illetve az adatkezelést megvalósító összes többi rendszer komponenst csak az arra jogosultak és csak dokumentáltan változtatják meg, emellett minden egyéb (véletlen vagy szándékos) módosulás kizárt, — vagyis az adatok és feldolgozási folyamataik pontosak és teljesek.

Shareware szoftver
Időszakosan ingyenesen használható szoftver. Korlátozott funkcionalitás, regisztrálási illetve fizetési kötelezettség jellemzi.

Szabály alapú biztonsági politika
Valamennyi használó számára kötelező, általános szabályokon alapuló informatikai biztonsági politika. Ezen szabályok rendszerint az elérendő erőforrások érzékenységének összehasonlítására, a használói vagy a használói csoportok nevében tevékenykedő entitások megfelelő jellemzőinek ismeretére épülnek.

Számítógépes bűnözés
Haszonszerzés vagy károkozás céljából, az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányuló, informatikai eszközök útján elkövetett cselekmények.

Számonkérhetőség
Annak biztosítása, hogy az informatikai rendszerben végrehajtott tevékenységek a későbbi ellenőrizhetőség céljára rögzítésre kerüljenek.

Személyes adat
A meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés.

Szoftver
Valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

Szoftvergazdálkodás alapelvei
A szoftverbeszerzés és terítés alapvető elemei mint például a következők: 1., Kizárólag legális (jogtiszta) szoftvereket lehet használni. 2., Csak azokat a szoftvereket szabad a számítógépekre telepíteni, amelyek a munkavégzéshez feltétlenül szükségesek. 3., Minden dolgozó számára biztosítani kell a munkája hatékony és eredményes elvégzéséhez szükséges szoftverkörnyezetet. 4., Egységesség, a konfigurációk könnyű menedzselhetősége.

Szoftverkönyvtáros
Az a személy, aki az összes program és adatfájl őrzéséért, megóvásáért és fenntartásáért felel. A változás menedzselés egyik fontos eleme, amely biztosítja a fejlesztési és üzemeltetési funkciók szétválasztását.

Szoftverleltár
Annak dokumentált leírása, hogy az intézmény informatikai rendszerébe tartozó minden egyes számítógépen és szoftver futtatására alkalmas eszközön milyen szoftverek találhatók.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Szoftverpark
Az adott intézmény informatikai rendszerében használt szoftverek összessége.

Szükséges tudás elve
Az érzékeny információ tulajdonosa részéről az információk elérésére, birtoklására, és azokon tevékenység végrehajtására vonatkozó jogosultságok meghatározása egy felhasználó részére, annak hivatali kötelezettségei függvényében.

Teszt (rendszer) környezet: Az alkalmazás szolgáltató szervezet/cég informatikai rendszerébe tartozó mindazon komponensek összessége, amelyet egy adott pénzügyi jellegű rendeltetésű alkalmazás ellenőrzése érdekében állítanak össze. Teszt környezet érvényes eredményt/tranzakciót előállító módon nem működhet.

Támadás
Valamely személy (tettes) akciója azzal a szándékkal, hogy valamely informatikai rendszert veszélyeztessen és károkat okozzon.

Támadási potenciál
A sikeres támadás esélyét fejezi ki.

Teljeskörű védelem
Teljeskörűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.

Tetszőleges hozzáférés-védelem
Egy szubjektum a hozzáférési engedélyét más szubjektumoknak továbbadhatja.

Titokvédelem
Az adatvédelem körébe tartozó adatok, és az egyéb erőforrások bizalmasságának védelmi körülményeinek megteremtése.

Titkos személyi információk
Minden olyan, az egyes ügyfelekről az intézmény rendelkezésére álló tény, információ vagy adat, amely az ügyfél személyére, adataira, vagyoni és pénzügyi helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi és/vagy üzleti kapcsolataira, valamint az adott intézménnyel fennálló kapcsolatára vonatkozik.

Trójai program
Olyan rosszindulatú programtörzs, amelyeket készítője illegálisan épített be az általa tervezett programba és a felhasználó szándéka ellenére és tudta nélkül hajt végre illegális feladatokat (pl.: adattörlés, illegális lemezművelet, program-megsemmisítés stb.).

Tűzfal
Egy olyan számítástechnikai eszköz, amely fizikailag, és logikailag elválaszt egy hálózatot egy másiktól.

Üzemi készenléti tényező (Rendelkezésre állás)
Annak a valószínűsége, hogy az adott informatikai rendszerelem valamely időpontban működőképes lesz.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Üzemi szoftver
Az informatikai rendszer működésének ellenőrzésére, felügyeletére szolgáló szoftver.

Üzleti titok
A működéshez, az üzletmenethez és a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.

Üzletmenet folytonosság tervezés
Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. (BCP – Business Continuity Planning)

Vagyonbiztonság
Az intézmény olyan állapota, amelyben az értékrendszer erőforrásainak rendelkezésre állása, bizalmassága és sértetlenségének fenyegetettsége gyakorlatilag minimális.

Veszélyforrás
Ide sorolható mindaz, aminek támadás formájában történő bekövetkezésekor a rendszer működésében nem kívánt állapot jön létre, illetve az erőforrások biztonsága sérül.

Védelmi intézkedés
A fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési vagy technikai eszközökkel tett intézkedés.

Védelmi mechanizmusok
Olyan informatikai védelmi intézkedések, amelyeket informatikai biztonsági szabványok határoznak meg, a hardver és szoftver gyártó cégek pedig termékeik előállítása során építik be és szolgáltatják a felhasználók részére.

Visszatöltés
Az a folyamat, amelynek során a mentett adatokat tartalmazó médiumról a mentő eszköz segítségével a sérült adathalmaz utolsó ép állapotának leginkább megfelelő adatstruktúrát visszaállítják.

Vírus
Olyan rosszindulatú programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl.: konkrét időpont, szabad lemezterületi helyek száma stb.) trójai faló hatást indít el.

Vírusvédelmi rendszer
A vírusvédelmi rendszer és a hozzá kapcsolódó védelmi mechanizmusok feladata az informatikai rendszerhez kapcsolódó vírusok felkutatása, működésük, aktív vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint – megsemmisítésük.

Védelem zártsága: Zárt a védelem, ha az összes releváns kockázatot figyelembe veszi.

Védelem teljes(körű)sége: Teljes körű a védelem, ha az illető informatikai rendszer összes elemére kiterjed.

III. sz. melléklet: A JOGSZABÁLYBAN ALKALMAZOTT FOGALMAK DEFINÍCIÓJA

Verzió: Az IT rendszer egy adott konkrét (jól meghatározott) állapota, amely a szállító, a szolgáltató és a felhasználó számára — az együttműködésük szabta korlátokon belül — azonos értelemmel bír.

Verziószám: Az alkalmazás adott verziójának azonosítására használt szöveges megjelölés. Legtöbbször számok és írásjelek kombinációja. A verziószám kiosztása általában a rendszerszállító feladata. A szokásos használat szerint az IT rendszer nevének említése a verziószám nélkül az illető terméket jelöli (tehát az összes verziót általában), míg a verziószámmal együttes említés a termék egy adott állapotát jelöli.

Verzióváltás: Külső vagy belső okok által indokolt új/módosított IT rendszerváltozat létrejöttének és bevezetésének folyamata a kezdeményezéstől a mindennapi használatig. A verzióváltás kitüntető eleme az alkalmazás kódjának megváltozása, amely szemben áll az át paraméterezés okozta rendszermódosításokkal (lásd még Változás kezelés).

Változáskezelés: Az informatikai erőforrásokban (adatok, infrastruktúra, technológia, hardver, szoftver, személyzet, szabályozás, stb.) bekövetkező változások, szabályozott keretek közötti nyilvántartása, menedzselése, ellenőrzése. A változáskezelési feladatok elvégzésének felelőse a változásmenedzser.

Zavaró esemény
Azok a váratlan jelenségek, amelyek károsan hatnak az informatikai szolgáltatásokra.

Zárt védelem
Zártnak nevezik az informatikai rendszer védelmét, ha az összes releváns fenyegetést figyelembe veszi.

IV. sz. melléklet: ÖSSZEFÉRHETETLEN FELADATOK ÉS FELELŐSSÉGEK A COBIT SZERINT

IV. MELLÉKLET: ÖSSZEFÉRHETETLEN FELADATOK ÉS FELELŐSSÉGEK A COBIT SZERINT

Összeférhetetlen feladatok és felelősségek (COBIT szerint)

	Felhasználó	IT ellenőr	Fejlesztő	Szoftver könyvtáros	Felh. támogató	Rendszer admin.	Hálózati admin	Adatbázis admin.	Operátor	IT biztonsági felelős
Felhasználó			X	X	X		X	X	X	
IT ellenőr			X	X	X	X	X	X	X	
Fejlesztő	X	X		X	X	X	X	X	X	X
Szoftver könyvtáros	X	X	X		X	X	X			X
Felh. támogató	X	X	X	X		X	X	X		X
Rendszer admin.		X	X	X	X			X	X	
Hálózati admin	X	X	X	X	X			X	X	
Adatbázis admin.	X	X	X		X	X	X			
Operátor	X	X	X			X	X	X		X
IT biztonsági felelős			X	X	X				X	

Az **X** jelöli az összeférhetetlen feladatokat és felelősségeket
Zöld szín: összefoglalva üzemeltetés