Állami Számvevőszék

MÓDSZERTAN

az információs rendszerek kontrolljainak ellenőrzéséhez

2004. február

Állami Számvevőszék

H-1052 Budapest,
Apáczai Csere János utca 10.
Levélcím: 1364 Budapest, Pf. 54.
Telefon: (36 1) 484 9100
Fax: (36 1) 338 4710

Módszertan az informatikai rendszerek kontrolljainak ellenőrzéséhez

2004. február

A módszertant készítették: **Fülöp Istvánné**
Borsos Ferenc
Weltherné Szolnoki Dóra
Szabó Balázs

Előszó

Az Állami Számvevőszék megújult középtávú stratégiája kiemelt figyelmet szentel a hagyományos pénzügyi ellenőrzés, az elszámolások megbízhatóságának minősítése, az átláthatóság érvényesítése mellett a közgazdasági értékelést és a döntés-előkészítést segítő, a teljesítményre, a hatékonyságra összpontosító kontrolltevékenységre. E célok elérése érdekében újszerű feladatot jelent, hogy – az eddigi munkálatokat felgyorsítva – a Számvevőszék teljes mértékben alkalmassá váljon az informatikai rendszerek megbízható és szabályszerű működésének ellenőrzésére.

A módszertan első, 2001-ben elkészült kiadásával elsődleges célnak tekintettük, hogy a számvevők a nemzetközileg elfogadott sztenderdek alapján, a legjobb gyakorlat alkalmazásával értékelhessék a számítógépes rendszerekben tárolt és kezelt adatok megbízhatóságát, sértetlenségét és rendelkezésre állását, illetve mindezek pénzügyi beszámolóra gyakorolt hatásait.

A módszertan a gyakorlatban is sikeresen beépült a számvevőszéki vizsgálatokba, az informatikai rendszerek kontrolljainak ellenőrzése szerves részévé vált az Állami Számvevőszék pénzügyi-szabályszerűségi ellenőrző tevékenységének.

A három év alatt összegyűjtött és elemzett tapasztalatok alapján aktuálissá vált a módszertan felülvizsgálata, korszerűsítése, és – az ÁSZ módszertani kiadványsorozatának részeként – a jelenlegi, második kiadás elkészítése. Az összeállítás során hasznosítottuk a Budapesti Közgazdaságtudományi és Államigazgatási Egyetem szakértőinek első kiadással kapcsolatban adott konstruktív és előremutató véleményét, és mindenekelőtt a számvevők gyakorlati tapasztalataiból leszűrt következtetéseket.

Az átdolgozás elsősorban az informatikai környezet és tevékenység megismerésének folyamatát és az általános kontrollokat taglaló részt érinti – egyfelől a technika korszerűsödéséhez való igazodás eredményeképpen, másfelől abból a szándékból kiindulva, hogy a megfogalmazások pontosabbak és egyértelműbbek legyenek, valamint az ellenőrök és ellenőrzöttek számára egyaránt könnyebben kezelhető és áttekinthetőbb kérdőíveket alakítsunk ki. Jelentősen bővítettük továbbá – az első kiadásban csak vázlatosan tárgyalt – működésfolytonossági tervek kontrolljainak és ellenőrzésének leírását.

A módszertan közreadása lehetőséget nyújt egyúttal arra is, hogy az érdeklődők megismerhessék és véleményt formálhassanak a számvevőszéki ellenőrzések során követett eljárásokról, illetve az alkalmazott módszerekről. Ezzel is munkánk nyitottságát, a hivatásunkhoz kapcsolódó bizalmat kívánjuk erősíteni. Mindezeken túlmenően a módszertan segítséget nyújthat a költségvetési gazdálkodó intézmények pénzügyi és informatikai vezetői számára is az informatikai rendszerek kockázatainak felmérésében és a hatékony belső kontroll-mechanizmusok kialakításában.

Az informatika területén nemzetközi és hazai tekintetben egyaránt gyors fejlődéssel számolhatunk. Ezért elengedhetetlen, hogy a nemzetközileg elfogadott sztenderdek változásait követve, azok hazai feltételekre történő adaptálásával a jövőben is folyamato-

san karbantartsuk és korszerűsítsük az informatikai ellenőrzés módszertanát. A módszertan továbbfejlesztésének következő nagyobb lépéseként tervezzük az alkalmazási kontrollok részletesebb – azaz már konkrét pénzügyi-számviteli informatikai rendszerekre épülő – kifejtését, lehetőséget biztosítva egyes, az államigazgatásban gyakran alkalmazott gazdasági szoftverek mélyebb megismerésére és ellenőrzésére.

Tartalomjegyzék

Bevezetés

Az informatikai rendszerek kontrolljainak ellenőrzéséhez készült módszertan az Állami Számvevőszék pénzügyi ellenőrzési módszertanának integráns részét képezi. A módszertan alapelve, hogy a számvevők részére olyan elvi, gyakorlati és eljárási útmutatást adjon, amelynek segítségével az ellenőrzés ezen speciális formáját elvégezhetik, illetve a vizsgálati eljárások során felismerik azokat az eseteket, amikor informatikai szakértő alkalmazására van szükség a pénzügyi ellenőrzés folyamatában való továbblépéshez.

A módszertan alkalmazásával az ellenőr felmérheti az informatikai terület vizsgálatának kockázatait, támpontot kap az eredendő kockázat, és a belső kontroll kockázat értékeléséhez – amelynek eredményei a továbbiakban kihatnak a teljes pénzügyi ellenőrzés folyamatára.

A módszertan célja, hogy segítséget nyújtson az ellenőr számára annak megítélésében, hogy az informatikai környezetben előállított pénzügyi beszámoló adatai és a beszámoló előállításához felhasznált elektronikus bizonyítékok

- teljesek,
- sértetlenek és
- megbízhatóak legyenek, valamint
- rendelkezésre állásuk biztosított-e.

A módszertan kidolgozása során az INTOSAI (International Organization of Supreme Audit Institutions) Auditing Standards idevonatkozó útmutatásait vettük alapul, amelyek kimondják:

> 3.3.4 „A számítógépesített számviteli vagy más információs rendszerek esetében az ellenőrnek kell meghatároznia, hogy a belső kontrollok megfelelően működnek-e, biztosítva az adatok sértetlenségét, megbízhatóságát és teljességét."
>
> 3.5.2 „… Ha a számítógépes alapú rendszer adatai az ellenőrzés fontos részét képezik, és az adatok megbízhatóságának nagy jelentősége van az ellenőrzési célok megvalósíthatóságában, akkor az ellenőröknek meg kell győződniük ezen adatok megbízhatóságáról és tárgyhoz tartozásáról."

A vizsgálati szempontok és eljárások kialakítása során továbbá figyelembe vettük a Számvitelről szóló 2000. évi C. törvény 169.§-ának követelményeit, amely az elektronikus formában őrzött bizonylatokra vonatkozóan előírja, hogy „az alkalmazott módszer biztosítsa a bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét."

A szervezet informatikai kontroll-mechanizmusainak vizsgálata tehát arra a kérdésre ad választ, hogy az informatikai környezetben előállított adatok érzékenyek-e az informa-

tikai rendszerben rejlő kockázatokra, fenyegetettségekre. Azaz végső soron a vizsgált szerv informatikai vonatkozású, eredendő és belső kontroll kockázatainak elemeiről, és ezen keresztül az adatok biztonságáról alkothat képet az ellenőr. Ennek eredményeként az informatikai kontroll-mechanizmusok vizsgálata olyan tényeket is feltárhat, amelyek a pénzügyi ellenőrzés megközelítését, végrehajtását befolyásolják.

Hasonlóképpen ahhoz, ahogyan a módszertanban bemutatott informatikai ellenőrzés célja a pénzügyi ellenőrzés céljaiból vezethető le, úgy a végrehajtás fázisai is teljes mértékben a pénzügyi ellenőrzés folyamatából eredeztethetők – az alábbi lépésekhez kapcsolódva:

- a vizsgált szervezet megismerése (azaz a külső szabályozás és irányítás, a belső irányítás, tevékenységek, gazdasági jellemzők stb.)
- belső kontroll mechanizmusok megismerése
- ellenőrzési eljárások megtervezése
- belső kontroll mechanizmusok tesztelése.

A módszertan felépítése során igyekeztünk szem előtt tartani a didaktikai igényeket annak érdekében, hogy kiindulópontot nyújtsunk az ellenőrök számára ezen speciális szakterület ismereteinek megértéséhez és elsajátításához. Másrészről hasonlóan fontos szempontnak tartottuk, hogy a mindennapi munkát támogató, az ellenőrzési feladatok végrehajtása során könnyen alkalmazható, gyakorlati segítséget nyújtó anyag készüljön. Mindezek figyelembevételével a módszertan az alábbi négy fejezetre tagolódik.

Az első fejezet az ellenőrzési eljárások tervezésének informatikai vonatkozásaihoz ad iránymutatást, bemutatva a számítógépes környezetben végzett ellenőrzés elméleti-módszertani alapismereteit, a kockázatok értékelésének és az IT kontrollok vizsgálatának lépéseit.

A második fejezet a vizsgált szervezet informatikai környezetének és tevékenységének felmérését, annak tartalmi és módszertani kérdéseit mutatja be. Itt kell megemlítenünk, hogy a módszertan, tekintve az informatika gyors fejlődését, egyes területeken csak késéssel tud lépést tartani az informatikai eszközökre és eljárásokra vonatkozó kérdések aktualitásával. Ezért módszertanunk az ellenőr megítélésére bízza, hogy az adott szervezet esetében milyen további tények feltárását tartja szükségszerűnek.

A módszertan harmadik és negyedik fejezete az IT kontrollok felméréséhez, az általános kontrollok és a pénzügyi alkalmazások részletes feltárásához, kockázatelemzéséhez és értékeléséhez ad iránymutatást és gyakorlati tanácsokat.

I. Az ellenőrzés tervezése

A tervezés az ellenőrzési folyamat kulcsfontosságú eleme, és alapvetően befolyásolja az vizsgálatok minőségét, eredményességét. Hasonlóképpen más ellenőrzési eljárásokhoz, az informatikai rendszerek ellenőrzését is meg kell tervezni annak érdekében, hogy a vizsgálati célok elérése hatékonyan valósuljon meg, és a végrehajtás minél kevesebb fennakadást okozzon az ellenőrzött szervezet működésében.

Eredményes tervezési folyamat az informatikai és a pénzügyi ellenőrök együttműködésén keresztül valósítható meg. A tervezés során határozhatóak meg az ellenőrzési bizonyítékok megszerzésének módszerei, amelyek a vizsgált szervezet informatikai kontrolljai felméréséhez szükségesek. A tervezés természete, terjedelme és ideje függ az ellenőrzött szervezet méretétől, összetettségétől és azon ismeretek mennyiségétől, amelylyel az ellenőrök a szervezet működéséről rendelkeznek.

A tervezés egy olyan iteratív folyamat, mely az ellenőrzési munka elejére koncentrálódik, de a vizsgálat egész ideje alatt folytatódik, hiszen a tételes tesztek mennyiségéről és típusáról szóló döntéseket csak az előzetes megállapítások alapján lehet meghozni. Továbbá abban az esetben, ha az ellenőrök a vizsgálat során olyan bizonyítékokhoz jutnak, amelyek szerint az egyes kontroll-eljárások nem hatékonyak, szükséges lehet a korábbi következtetések, valamint a következtetéseken alapuló tervezési döntések átértékelése.

A tervezés folyamán az ellenőr

1. megérti az ellenőrzött szervezet működését, megismeri a környezet alapvető elemeit és meghatározza azokat a számítástechnikán alapuló folyamatokat, amelyek a vizsgálat szempontjából lényegesek;

2. meghatározza az eredendő kockázatot és a belső kontroll kockázatot;

3. előzetes becslést végez a kontrollok hatékonyságával kapcsolatosan és

4. meghatározza a tesztelendő kontrollokat.

Tekintettel arra, hogy az informatikai rendszerek kontrolljainak ellenőrzése a pénzügyi ellenőrzés részét képezi, figyelembe kell venni, hogy a számítástechnikán alapuló kontrollok értékelését a vizsgálat egyéb szempontjaival összefüggésben kell kialakítani. Ez az értékelés az ÁSZ pénzügyi beszámoló ellenőrzésének tervezésével kapcsolatos részletes útmutatójában került bővebb kifejtésre.

A tervezés során az ellenőr interjúkat szervez a rendszer különböző területeiért felelős vezetőkkel, és beszerzi a releváns rendszerdokumentációkat. Ezek a lépések és információk hozzásegítik az ellenőrt, hogy:

- kifejthesse az ellenőrzöttek számára a vizsgálat célját és hatókörét, és könnyebben kialakíthassa velük az együttműködést;

- megértse:
  - hogyan működik a vizsgált szervezet informatikai rendszere, és hogyan irányítják;
  - a valószínűleg szóba jöhető információ-biztonsági kockázatokat;
- azonosítsa a technológiai kérdéseket és problémákat, amelyekhez házon belüli (ÁSZ) vagy külső IT szakértők segítségét kell igénybe vennie.

1. A szervezet működés és az informatikai környezet megismerése, a számítástechnikával támogatott műveletek azonosítása

A szervezeti működés megismerése az ÁSZ pénzügyi ellenőrzési módszertanának is része, ezért ennek lépéseit jelen keretek között külön nem tárgyaljuk. Ugyanakkor szeretnénk hangsúlyozni a megismerés ezen részének fontosságát, hiszen az informatikai rendszerek funkcióinak megismerése nem képzelhető el anélkül, hogy az ellenőr ne ismerné pontosan a számítástechnikával támogatott folyamatok célját, elveit, kialakítását, működését.

Az IT ellenőr feladata a továbbiakban, hogy megértse és dokumentálja, hogy a vizsgált szervezet működését milyen módon támogatják számítógépes rendszerek. Ez magában foglalja *minden egyes, a pénzügyi beszámoló szempontjából jelentős informatikai alkalmazás áttekintését* is. Az ellenőrzött szervezettel kapcsolatos informatikai ismeretek megszerzése, megértése és dokumentálása két fő területre irányul:

(1) Informatikai környezet megismerése, megértése, dokumentálása (ld. II. fejezet 1.)

(2) Informatikai tevékenység megismerése, megértése, dokumentálása (ld. II. fejezet 2.)

Az informatikai környezet megismerésének szakaszában az ellenőr háttérinformációkat gyűjt össze a szervezet IT infrastruktúrájáról, hardvereiről és szoftvereiről, továbbá a köztük levő összefüggésekről.

Az egyes informatikai eszközök és rendszerek, valamint a közöttük levő kapcsolatok és összefüggések megmutatják, hogy az adott szervezet pénzügyi beszámolója egyrészt milyen számítógépes rendszereken alapul, másrészt közöttük milyen kapcsolat áll fenn. Ezzel behatárolható a vizsgálat kiterjedése, valamint a szükséges szakértelem mértéke is. (A számítógépes rendszerek méreteiről és technikai összetettségükről kapott kép lehetővé teszi az ellenőr számára, hogy megállapítsa, milyen mértékben lesz szüksége IT szakellenőr(ök) segítségére.)

Az informatikai tevékenység megismerése keretében fel kell mérni, hogy a vizsgált intézmény milyen informatikai üzemeltetési tevékenységeket végez, erre milyen szervezeti keretet alakított ki és milyen magas szintű szabályozásokat alkalmaz. A tevékenység vizsgálata szorosan összefügg az informatikai környezet felmérésével, ugyanis az inf-

rastruktúra és a számítógépes alkalmazások megbízható működése az ezeket körülvevő üzemeltetési, szervezeti és szabályozási tényezőktől függ.

Az informatikai tevékenység megismerése tovább bővíti és pontosítja azon kontrollok körét, melyeket az ellenőrzés során részletesen meg kell vizsgálni, azaz amelyek befolyásolják a pénzügyi-számviteli rendszerek megbízható működését.

A szervezeti tevékenységek értékeléséhez nélkülözhetetlen a magas szintű szabályozások és kontrollok megismerése is, mert ezek határozzák meg az informatikai tevékenységek kereteit, az alacsonyabb szintű kontrollok működését és a számonkérhetőség lehetőségeit.

2. Az eredendő kockázat és a belső kontroll kockázat értékelése

Miután az ellenőr megismerte és megértette a szervezet működését, informatikai folyamatait, rendszereit, értékelnie kell az eredendő és a belső kontroll kockázatokat, illetve ezeken keresztül az ellenőrzési kockázatot. Az ellenőrzési kockázat annak kockázatát jelenti, hogy az ellenőr téves véleményt alkot arról, hogy a pénzügyi beszámolót alátámasztó elektronikus adatok és egyéb bizonyítékok teljesek, sértetlenek, megbízhatóak, valamint rendelkezésre állásuk biztosított-e. Az informatikai ellenőrzés kockázatának – ugyanúgy, mint a pénzügyi ellenőrzésének – három összetevője van:

- Az **eredendő kockázat** az informatikai erőforrásoknak (elektronikus adatok, fájlok, szoftverek, számítógépek, hálózati eszközök stb.) *a fenyegetettségek iránti fogékonysága*, azt feltételezve, hogy ezen fenyegetettségek kivédésére irányuló kontrollok nem léteznek. Fenyegetettségnek tekintünk minden olyan nemkívánatos eseményt, amely az adatok teljességét, sértetlenségét, megbízhatóságát vagy rendelkezésre állását hátrányosan befolyásolja. Fenyegetettség lehet külső esemény (tűz, vízkár, vírusok stb.), és lehet belső tényező is (hanyag kezelés, rosszindulatú adatmódosítás, programhiba stb.).

- A **belső kontroll kockázat** annak lehetősége, hogy az ellenőrzött szervezet belső kontroll mechanizmusai nem képesek megelőzni, vagy feltárni és kijavítani a lényeges szabálytalanságot vagy tévedést. A belső kontroll kockázat a belső kontrollok fejlesztésével csökkenthető.

- A **feltárási kockázat** annak veszélye, hogy az ellenőr nem tár fel a szervezet belső kontrollmechanizmusai által nem korrigált lényeges szabálytalanságot vagy tévedést.

Az ellenőrzési kockázat nagysága, valamint az eredendő és kontroll kockázat felmérése alapján az ellenőr meg tudja becsülni az elvárt szintű feltárási kockázat eléréshez szükséges tételes tesztek fajtáit, időigényét és kiterjedését. Például ha az ellenőr mind az eredendő, mind a kontroll kockázatot magasnak ítéli a szervezet informatikai rendszerében, akkor növelnie kell a vizsgálat mélységét, illetve több tételes tesztet kell végrehajtania.

Az ellenőrnek mindenekelőtt azonosítania kell azon körülményeket, amelyek jelentősen növelik az eredendő és kontroll kockázatot, majd ennek alapján el kell döntenie, hogy ezek lehetővé teszik-e egyáltalán hatékony kontrollok alkalmazását a vizsgálat hatókörébe tartozó pénzügyi alkalmazások esetében. Ezen mérlegeléshez szükséges információkat az ellenőrnek a tervezés fázisában kell beszereznie, mégpedig a már említett *megismerés* keretében. A mérlegelés és a szükséges vizsgálati eljárások megtervezése során figyelembe kell venni a már megismert kockázatok és kontroll-gyengeségek teljes hatását a szervezet működésére és beszámolójára nézve, ami komoly szakértelmet és tapasztalatot kíván.

A kockázatbecslés, értékelés módszerét részletesebben lásd: A Központi költségvetési szerv elemi beszámolója pénzügyi ellenőrzésének módszertana c. ÁSZ kiadványának vonatkozó fejezeteiben.

Az eredendő kockázatokat érintő tényezők

A számítástechnikával támogatott műveletek a papír alapú feldolgozási folyamatokhoz képest sajátos eredendő kockázati faktorokkal rendelkeznek, amelyek egyébként a manuálisan működő rendszerekre nem jellemzőek. Ezekre a sajátságos tényezőkre az alábbiakban sorolunk fel néhány példát:

- **Tranzakciók egységes feldolgozása**: Számítógépes programokkal történő adatfeldolgozás esetén az azonos tranzakciók feldolgozása során előforduló programhiba következetesen megjelenik. Így az ebből eredő – a tranzakciókra vonatkozó - megállapítások, következtetések visszavezethetőek egyetlen programhibára.

- **Automatikus feldolgozás**: A számítógépes rendszer automatikusan kezdeményezhet tranzakciókat vagy hajthat végre feldolgozási műveleteket. Ezen feldolgozási lépésekkel kapcsolatos bizonyítékok (és az ide kapcsolódó kontrollok) azonban nem mindig láthatóak.

- **Fel nem tárt hibák növekvő kockázata**: A számítógépek elektronikus formában kezelnek és tárolnak információkat, és a feldolgozás során kevesebb emberi beavatkozást igényelnek, mint a manuális rendszerek. Ez növeli annak a lehetőségét, hogy egyének meghatalmazás nélkül hozzáférjenek az érzékeny információkhoz és látható bizonyítékok nélkül megváltoztassák az adatokat. Az elektronikus forma miatt számítógépes programokban és adatokban végrehajtott változtatások nem könnyen és egyértelműen észlelhetőek. A felhasználók pedig kevésbé kérdőjelezik meg a számítógépes outputok megbízhatóságát, mint a manuális jelentésekét.

- **Létezés, teljesség és kiterjedés az ellenőrzési nyomvonal esetében**: Az ellenőrzési nyomvonal olyan bizonyíték, amely bemutatja, hogy az adott tranzakció hogyan kezdődött, hogyan dolgozták fel és hogyan került összesítésre. Például egy beszerzés esetében az ellenőrzési nyomvonal magába foglalja az árajánlatkérést, vagy valamilyen közbeszerzési eljárás dokumentumait, megrendelőlapot, szállítólevelet, a raktárra-vételről készült bizonylatot, a számlát, a számlaösszesítőbe történt bejegyzést (a

beszerzések nap, hónap és/vagy számla szerinti összesítése), és a számlaösszesítőről a főkönyvbe teljesített feladást. Egyes informatikai rendszereket úgy terveztek meg, hogy az ellenőrzési nyomvonalat csak meghatározott ideig tartsák fenn, csak elektronikus formátumban, esetleg csak összesített formában. Az így létrehozott információ a hatékony elemzés szempontjából túlságosan terjedelmes lehet. Például telephelyek adatainak automatikus összesítése egy tranzakciót eredményezhet. Ellenőrzést támogató, vagy visszakereső szoftver használata nélkül a tranzakciók feldolgozás során történő nyomon követése rendkívül nehézkes lehet.

- **Az alkalmazott hardver és szoftver természete**: Az alkalmazott hardver eszközök és szoftverek jellege érintheti az eredendő kockázatot, amint azt az alábbi példák is mutatják:

  - A számítógépes feldolgozás típusa (on line, batch-en alapuló, vagy osztott) az eredendő kockázat különböző szintjeit képviselik. Feldolgozási típusokról részletesebben lásd II. fejezet 6.3. pontját.

  - Periférikus hozzáférési eszközök vagy interface-ek növelhetik az eredendő kockázatot. Például a rendszerhez való telefonos hozzáférés növeli a rendszer további személyek általi elérhetőségét, és ezért nő az informatikai forrásokhoz való jogosulatlan hozzáférések kockázata.

  - A szervezeten belül kifejlesztett alkalmazási szoftverek magasabb eredendő kockázatot rejthetnek magukban, mint a vásárolt szoftverek, melyeket alaposan teszteltek és általános kereskedelmi forgalomban vannak. Másrészről az újonnan forgalomba került szoftvereket ill. verziókat esetleg nem tesztelték elég alaposan, vagy nem vetették alá olyan mértékű használatnak, melynek során létező hibáira fény derülhetett volna.

- **Szokatlan vagy nem rutin jellegű tranzakciók**: Mint a manuális rendszerek esetében is, szokatlan vagy nem rutin jellegű tranzakciók növelhetik az eredendő kockázatot. Azokban a programokban, melyeket ilyen tranzakciók feldolgozására fejlesztettek ki és nem használják a napi munkában, nagyobb a kockázata annak, hogy a bennük rejlő hibákat később veszik észre.

A belső kontroll kockázatot érintő kontroll elemek

A belső kontroll összetevőinek bemutatásához a Committee of Sponsoring Organizations of the Treadway Comission (COSO) 1992-ben elfogadott, öt alkotóelemből álló meghatározását vettük alapul:

> A **kontroll környezet** meghatározza a szervezet működésének jellegét, befolyásolja az ott dolgozók kontroll-tudatosságát. A belső kontrollok minden egyéb összetevőjének ez az alapja. A kontroll környezeti tényezők magukban foglalják az etikai

értékeket, a szervezet tagjainak szakértelmét, a vezetés filozófiáját, vezetési stílusát és annak módját.

A **kockázatelemzés** a szervezeti célok elérését veszélyeztető kockázatok azonosításának és elemzésének folyamata. Az ellenőr ennek dokumentumai alapján tudja megítélni, hogy az ellenőrzött szervezet hogyan kezeli a kockázatokat.

Kontroll tevékenységek azok a szabályzatok és eljárásrendek, amelyek célja végső soron a szervezeti célok elérése. Kontroll tevékenységek közé soroljuk például a jóváhagyásokat, igazolásokat, visszaigazolásokat, felügyeleti és monitoring tevékenységeket, működési teljesítményről szóló jelentéseket vagy a feladatkörök szétválasztását.

Információ és kommunikáció magában foglalja a helyes információ azonosítását, megszerzését, és a megfelelő személyekhez való továbbítását olyan formában és időben, hogy eleget tudjanak tenni feladataiknak. Ez alatt értendőek például a szervezet tranzakcióinak rögzítésére, feldolgozására, összesítésére és jelentésbe foglalására szolgáló informatikai rendszerek és módszerek.

Monitoringnak nevezzük azokat a folyamatosan működő tevékenységeket, amelyek értékelik a belső kontrollok időbeli működését, és biztosítják, hogy a feltárt hiányosságokról a felső vezetés tudomást szerezzen.

A pénzügyi ellenőrzés során a felsorolt elemek mindegyikét figyelembe kell venni a szervezet belső kontroll mechanizmusának, és ezen belül az informatikai rendszer kontrolljainak értékeléséhez.

A *kontroll környezet* felmérése során az ellenőrnek értékelnie kell az informatikai rendszer alkalmazásával járó egyedi tényezőket is. Így például elemezni kell a felső vezetés hozzáállását az informatikai rendszerek alkalmazásával kapcsolatban, illetve azt, hogy az ezzel együtt járó feladatokat mennyire tudatos és következetes módon kezeli – e nélkül ugyanis a szervezet többi részében sem alakul ki a megfelelő kontroll-tudatosság. A felső vezetés az alábbi módon tudja demonstrálni a megfelelő hozzáállását és tudatosságát:

- felmérte a számítógépes rendszerek alkalmazásának előnyeit és kockázatait;
- szabályozta az informatikai vonatkozású feladat- és hatásköröket;
- folyamatosan felülvizsgálja a számítógépes rendszerek fejlesztésére, módosítására, karbantartására és használatára vonatkozó szabályozórendszert;
- folyamatosan felülvizsgálja a programokhoz és adatokhoz való hozzáférésre kialakított szabályozórendszert;
- felmérte és a szabályozórendszer kialakítása során mérlegelte az informatika alkalmazásával járó eredendő és kontroll kockázatokat;
- figyelembe veszi a korábban felmerült javaslatokat;

- felkészült a számítógépes feldolgozást érintő krízishelyzetek gyors és hatékony kezelésére; és
- vezetői döntéseihez felhasználja az elektronikus adatokat, de ellenőrzi is azok helyességét.

A belső kontrollok további összetevőinek (kockázatelemzés, kontroll tevékenységek, információ és kommunikáció valamint monitoring) bővebb kifejtésére a III. és IV. fejezetekben kerül sor.

3. Az informatikai kontrollok hatékonyságára vonatkozó előzetes értékelés

A belső kontroll kockázat felmérése részeként az ellenőrnek egy előzetes értékelést kell kialakítania az informatikai kontrollok hatékonyságára vonatkozóan. Ez az értékelés elsősorban a szervezet munkatársaival folytatott megbeszéléseken – ideértve a felhasználókat, a rendszeradminisztrátorokat, az információs forrásokért, a rendszerbiztonságért felelős vezetőket stb. – alapul, illetve a számítástechnikával támogatott műveletek megfigyelésén, valamint a politikák és szabályzatok vázlatos áttekintésén.

Ebben a szakaszban az ellenőr legtöbbször még csak az általános, azaz szervezet egészére vonatkozó kontrollokról (ld. III. fejezet) tud valamilyen képet kialakítani magának. Ugyanakkor ehhez már szükség lehet bizonyos részletek megismerésére is, azaz egyes eszközök és helyiségek megtekintésére, valamint a jelentősebb pénzügyi alkalmazásokkal kapcsolatos tájékozódásra.

4. A tesztelendő kontrollok azonosítása

Az eredendő- és belső kontroll kockázat felmérése alapján – beleértve az informatikai kontrollok előzetes értékelését is –, az ellenőrnek azonosítania kell azokat az általános kontrollokat, amelyek véleménye szerint hatékonyan működnek, és ezért az ellenőrzés során ezek tesztelésére sort kell keríteni. Az előzetes értékelés fontossága bemutatható ellentétes szemszögből is: ki kell szűrni azokat a kontrollokat, amelyek nem működnek illetve nem jól működnek, így tesztelésükre nem kell erőforrásokat biztosítani a tervezés során.

II. Az informatikai környezet és tevékenység megismerése

Az ellenőrzés első lépése, és egyben az ellenőrzés tervezésének alapja az informatikai környezet és tevékenység megismerése és átfogó szemléletű felmérése. A megismerésről készült dokumentumokat mindazok rendelkezésére kell bocsátani, akik az ellenőrzés további folyamatában részt vesznek.

Az **informatikai környezet** megismerésének szakaszában az ellenőr háttérinformációkat gyűjt össze a szervezet IT infrastruktúrájáról, hardvereiről és szoftvereiről és a köztük levő összefüggésekről. Az egyes informatikai eszközök és rendszerek, valamint a közöttük levő kapcsolatok és összefüggések megmutatják, hogy az adott szervezet pénzügyi beszámolója egyrészt milyen számítógépes rendszereken alapul, másrészt közöttük milyen kapcsolat áll fenn.

Itt tartjuk célszerűnek a *rendszer* szó meghatározását, azaz, hogy módszertanunkban mit értünk alatta. *A rendszer alatt az intézményi infrastruktúra, erőforrások és kontrollok azon részhalmazát értjük, melyek közvetlenül vagy közvetetten befolyásolják a pénzügyi beszámoló szabályosságát és megbízhatóságát.* Tehát elsődlegesen a szűken vett pénzügyi informatikai rendszert jelenti, de ha a pénzügyi rendszert működtető informatikai eszközök ugyanarra a hálózatra vannak kapcsolva, mint az intézmény többi számítógépe, akkor már minden ilyen számítógép és alkalmazás beletartozhat az ellenőrzésbe bevonandó *rendszer* fogalmába. A határvonal meghúzása az ellenőr feladata és felelőssége.

> Példaként tekintsünk egy intézményt, ahol minden pénzügyi művelet és tranzakció egy-két teljesen elszigetelt számítógépen zajlik, azaz ezen szoftverek és hardverek nem állnak kapcsolatban sem intézményen belüli sem azon kívüli számítógépekkel, hálózattal. Ebben az esetben a vizsgálat csak ezen alkalmazásokra és számítógépekre, illetve a biztonságukat és megbízhatóságukat megalapozó kontrollokra terjed ki. Szakellenőr segítségére pedig akkor lehet szükség, ha ezen rendszer, vagy rendszerek önmagukban nagyon összetettek, vagy speciálisak.

Ez a példa azonban napjainkban egyre ritkábban fordul elő. Sokkal inkább jellemzőek - és ez a fejlődési tendencia - az integrált, egymással és a külvilággal is összekapcsolt informatikai rendszerek. A pénzügyi rendszer már nem egy elkülönült egységet alkot, hanem adatokat kaphat és küldhet is a bérszámfejtési, a logisztikai, a kontrolling stb. rendszereknek. Ugyanakkor maga az alkalmazást futtató számítógép része lehet a szervezeti szintű intranet hálózatnak és kapcsolódhat az internethez is. Ezen esetekben már adott az elvi lehetősége mind az intézményen belüli, mind a kívülről jövő "támadásnak", azaz az olyan hozzáféréseknek, melyek a pénzügyi rendszerekben tárolt információk bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetik. Ezért alapvető feladat, hogy az ellenőr megértse a rendszer működését, és így megállapíthassa, hogy az intézmény pénzügyi rendszere milyen oldalról és milyen módon fenyegetett.

A környezet megismerése folyamán - az alkalmazások felmérésével - az ellenőr már képet kaphat az informatikával lefedett pénzügyi-számviteli és egyéb ügyviteli folyamatokról. Az informatikai tevékenységek azonban ennél tágabb kört alkotnak.

Az **informatikai tevékenység** megismerése keretében fel kell mérni, hogy a vizsgált intézmény milyen informatikai üzemeltetési, fejlesztési tevékenységeket végez, erre milyen szervezeti keretet alakított ki és milyen magas szintű szabályozásokat alkalmaz. A tevékenység vizsgálata szorosan összefügg az informatikai környezet felmérésével, ugyanis az infrastruktúra és a számítógépes alkalmazások megbízható működése az ezeket körülvevő üzemeltetési, szervezeti és szabályozási tényezőktől függ.

Az informatikai tevékenység megismerése tovább bővíti és pontosítja azoknak a kontrolloknak a körét, melyeket az ellenőrzés során részletesen meg kell vizsgálni, azaz amelyek befolyásolják a pénzügyi-számviteli rendszerek megbízható működését. Ha például az intézmény informatikájának üzemeltetéséhez nincsenek meg a megfelelő feltételek, akkor az veszélyeztetheti az alkalmazások biztonságos működtetését, vagy az adatbázis-kezelés hiányosságain keresztül a pénzügyi adatok megbízhatóságát. Így ez utóbbi esetben az adatbázisokra vonatkozó kontrollok részletes ellenőrzésére is szükség lesz.

A szervezeti tevékenységek értékeléséhez nélkülözhetetlen a magas szintű szabályozások és kontrollok megismerése is, mert ezek határozzák meg az informatikai tevékenységek kereteit, az alacsonyabb szintű kontrollok működését és számonkérhetőségét. Példaként említhetjük az informatikai biztonságpolitikát, melynek hiányosságai gyenge vagy "lyukas" biztonságtechnikai kontrollokat eredményezhetnek. Ilyen esetben az ellenőrzés során fokozott hangsúlyt kell fektetni az adatbiztonsággal összefüggő kontrollokra annak érdekében, hogy az ellenőr megbizonyosodhasson a pénzügyi, számviteli alkalmazások megbízható működéséről.

A tevékenységek megismerése és felmérése - az IT környezethez hasonlóan - segíti az ellenőrt annak megállapításában, hogy mely területekhez szükséges informatikai szakellenőr igénybevétele.

Az ellenőrzés fontos része a vizsgálat alá vont **rendszer dokumentálása vagy ábrázolása**. A kapcsolatok és összefüggések megértését segítik a rendszerről készített diagramok és folyamatábrák.

Ennek elkészítését kiemelten fontosnak tartjuk, mivel a vizsgálat során nagyban megkönnyítheti az ellenőrök munkáját, és csökkenti a félreértések előfordulásának valószínűségét. A különböző eljárások grafikus formában való ábrázolása könnyen áttekinthetővé teszi a dokumentációt, és a kommunikációnak is egy magas szintű eszközét nyújtja. A logikus és lényegre törő ábrázolással a felmérés hatékonyabb és egységes lesz, és megkönnyíti a kommunikációt a belső kontroll rendszer vizsgálatában részt vevők és az ellenőrzöttek között. A közös jelölésrendszer alkalmazásával minden érdekelt átlátja és megérti a szervezeti folyamatokat, kontrollokat. A grafikus ábrák továbbá az ellenőrzési dokumentum részét képezhetik.

Az informatikai környezet és tevékenység felmérése során két ábrát célszerű elkészíteni. Az egyik ábra az 1.2 kérdőív része, és elsősorban a szervezet informatikai infrastruktúrájáról, annak topológiájáról ad képet. Az így kirajzolódó fizikai kapcsolatok segítenek a vizsgálandó *rendszer* - már említett - behatárolásában. Ilyen topologikus ábrával a legtöbb szervezet rendelkezik, ilyenkor elegendő erről másolatot készíteni és a kérdőív által kért többlet információkat ezen feltüntetni.

A másik grafikus ábra a szervezet pénzügyi-számviteli folyamatait képezi le, melynek segítségével nyomon követhető minden tranzakció kiindulópontja, feldolgozási és tárolási helye, és eredménye. A későbbiekben a módszertant ilyen példával és jelölésrendszerrel is tervezzük kiegészíteni.

Az informatikai környezet és tevékenység felméréséhez - a kérdőívekre adott válaszokon kívül - általában az **alábbi dokumentumokra van szükség**. A könnyebb tájékozódás kedvéért a dokumentumok mellett megjelöltük, hogy mely kérdőívekhez illetve mely kérdésekhez tartoznak.

- A részletesen is vizsgált alkalmazások felhasználói kézikönyvei (1.2.2.)
- A részletesen is vizsgált alkalmazások működtetési leírása (1.2.2.)
- Az informatikai szolgáltatási szinteket rögzítő szabályozás(ok) (2.1.1.)
- Az informatikai üzemeltetéshez folyamatosan vagy rendszeresen igénybe vett külső szolgáltatókkal/szakértőkkel kötött szerződések (2.1.2.)
- A help-desk által készített összesítések és statisztikák a bejelentett problémákról (2.1.7.)
- Az informatikai rendszerek változási, változtatási eljárásainak írásban rögzített szabályozása (2.1.1.10.)
- Az informatikai biztonsági felügyelő munkaköri leírása (2.2.5.)
- Az informatikai biztonsági felügyelő jelentései két évre visszamenőleg (2.2.5.)
- A szervezet aktuális informatikai stratégiája (2.3.1.)
- A szervezet informatikai biztonsági politikája és biztonsági szabályzata (2.3.3.)
- A szervezet működésfolytonossági és/vagy katasztrófaterve (2.3.7.)
- A dolgozók informatikai erőforrásokhoz való hozzáférését szabályozó dokumentumok (2.3.12.)
- A szervezet dokumentációs politikája (2.3.15.)

- A belső ellenőrzés informatikai vonatkozással is bíró jelentései két évre visszamenőleg (2.3.17.)

1. Az IT környezet felmérése kérdőívek alkalmazásával

Az IT környezet felmérésének célja, hogy az ellenőr megismerje a szervezet által alkalmazott, a vizsgálat tárgyát képező számítógépes rendszer nagyságát és összetettségét. A vizsgálat elsődlegesen közvetlenül a pénzügyi informatikai rendszerre koncentrál, de a közvetett összefüggések miatt szükséges az egész szervezet átfogó IT környezet-felmérése is.

A felméréshez használt kérdőívek kiértékelése alapján megállapítható:

- mennyire összetett a vizsgált szervezet rendszere;
- az egész rendszer mely részeire terjedjen ki a vizsgálat (és a továbbiakban csak ez lesz *a rendszer*);
- mely kontroll területek (pl. biztonságtechnikai kontrollok) ellenőrzéséhez szükséges IT szakellenőr igénybevétele.

A kérdőívek két csoportra oszthatóak: 1. *Infrastruktúra felmérése,* valamint 2. *Alkalmazások felmérése*

A kérdőíveket az ellenőrzött szervezetnek kell kitöltenie, de az ellenőrzési kockázat csökkentése érdekében javasoljuk ebben az ellenőr aktív közreműködését is. A kérdések ugyanis sok helyen – a technikai fejlődés és a közigazgatási intézmények eltérő informatikai környezete miatt szándékosan – általános megfogalmazásúak, ezért az ellenőr orientációs segítsége jelentősen hozzájárulhat ahhoz, hogy a kockázatértékeléshez szükséges minden információt megkapjon. Az orientációhoz támogatást nyújtanak a kérdőívek kitöltési és értékelési útmutatói, de elengedhetetlen, hogy az ellenőr is ismerje a korszerű informatikai megoldásokat és trendeket.

Az 1.1. (Infrastruktúra) kérdőíveit az IT szervezeti egység vezetőjének (vagy ha ilyen nincs, akkor az informatikáért felelős vezetőnek) kell kitöltenie, illetve a topologikus ábrát a kért bejelölésekkel rendelkezésre bocsátania. Az 1.2. (Alkalmazások) első két kérdőívét (1.2.1., 1.2.2.) ugyancsak az informatikai vezetőnek kell kitöltenie, azonban a harmadik (1.2.3.) kérdőív már felhasználói kérdéseket tartalmaz, ezért kitöltésére az adott szoftvert alkalmazó funkcionális terület vezetőjét/vezetőit is fel kell kérni. (A második és harmadik kérdőív egyaránt a pénzügyi alkalmazások részletes felmérésére szolgál, és több kérdés mindkét helyen előfordul. Ennek oka, hogy a pénzügyi alkalmazásokkal kapcsolatos feladatokat a két terület más szemszögből látja, ezért az ugyanarra a kérdésre adott válaszok különböző kockázatokra hívhatja fel a figyelmet – ezzel is teljesebbé téve az ellenőrzés kockázatértékelését.)

1.1. Infrastruktúra: ebben a részben a szervezet lényeges informatikai eszközeit, a hozzájuk tartozó rendszer-szoftvereket és a kapcsolatokat mérjük fel. A "Hardverek és hozzájuk tartozó rendszer szoftverek" űrlapjainak (1.1.1) kitöltésével gyakorlatilag egy egyszerűsített leltárt kapunk a megismeréshez szükséges paraméterekkel. A "Hálózati

hardver és topológia" felmérése keretében (1.1.2) pedig az informatikai hálózat(ok)ról kérünk egy egyszerű ábrázolást, melyen azonosíthatóak a lényeges feldolgozási és felhasználói helyek, valamint a fontosabb hálózati hardver elemek. A grafikus ábrázolás segít megismerni egyrészt a leltárba vett hardver eszközök közötti kapcsolatokat, valamint egy gyors áttekintést nyújt az IT infrastruktúra védelmi rendszeréről.

1.2 Alkalmazások: Ez a felmérés három részből áll, ahol az első rész, az "Alkalmazások felsorolása" (1.2.1) szintén egy rövid leltár. Itt külön választottuk a kifejezett pénzügyi-számviteli, illetve az egyéb szervezeti feladatokat ellátó alkalmazásokat a jobb megkülönböztethetőség érdekében.

A második és harmadik részben "Alkalmazások részletes információi" (1.2.2., 1.2.3.) pedig a már felsorolt pénzügyi alkalmazásokról kérünk részletesebb tájékoztatást. Ez utóbbi adatlapok - ha az ellenőr fontosnak ítéli - kitölthetőek egyes, az előbbi kérdőívben egyéb alkalmazások között felsorolt szoftverekre is.

A megértést segítik az egyes alkalmazások működtetési leírásai - nem keverendőek összsze a "gyári" kézikönyvvel -, melyek az adott szoftver gyakorlati használatát, üzemeltetését írják le az alkalmazottak számára. Ha a vizsgált alkalmazásokhoz az intézmény ilyennel rendelkezik, célszerű elkérni.

1.1.1. Kérdőív: Hardverek és a hozzájuk tartózó rendszer szoftverek

Munkaállomások, terminálok

Típus, gyártó, modell, processzor, memória	db.	helye	operációs rendszer és verzió	hálózati v. egyéb kommunikációs szoftver és verzió	biztonsági szoftver és verzió

Szerverek, mainframe-ek

Gyártó, modell	helye	operációs rendszer és verzió	biztonsági sw. és verzió	adatbázis-kezelő rendszer(ek) és verzió

Kitöltési és értékelési útmutató az 1.1.1. kérdőívhez

Típus, gyártó, modell, processzor, memória: a típust csak az első táblázatban kell kitölteni, vagy "munkaállomás"-t vagy "terminál"-t kell megjelölni.

Gyártóként azt a vállalkozást kell megjelölni (egyértelmű rövidítéssel is elég), amely a számítógépet összeszerelte. (pl. Albacomp, IBM, Compaq, SUN).

A modellt akkor kell megjelölni, ha a számítógép ilyennel rendelkezik, pl. PC 554.; SPARC Classic stb. (a szerverek és mainframe-ek esetében ezt minden esetben fel kell tüntetni!)

A processzor és memória pl.: Pentium IV., 256 MB.

Helye: a számítógépek fizikai elhelyezkedését kell megjelölni: munkaállomások és terminálok esetében az épületnél részletesebben nem szükséges. Pl.: zalaegerszegi raktár, budapesti központi épület stb.; a szerverek és mainframe-ek esetében viszont az épületen belüli helyiséget is fel kell tüntetni.

Egy rubrikába csak egy *Típus* vagy *Hely* írható!

Operációs rendszer és verzió: pl. Windows 98; SunOS 5.3 stb.

Hálózati vagy egyéb kommunikációs szoftver és verzió: bármely olyan, a munkaállomásokra és terminálokra telepített alapszoftver (az operációs rendszeren kívül), mely más informatikai eszközzel kapcsolatot tesz lehetővé. Pl. helyi hálózatok esetében Novell 4.1 vagy külső összeköttetéshez Reachout.

Biztonsági szoftver és verzió: Ide sorolható az adott számítógép(ek)re telepített minden olyan szoftver, amit célzottan biztonsági célból alkalmaznak; azaz az adatok és informatikai eszközök bizalmasságának, sértetlenségének, és rendelkezésre állásának érdekében. Ilyen szoftverek lehetnek: beléptető, azonosító szoftverek; titkosító, kódoló és dekódoló szoftverek; biztonsági mentést (backup) végző alkalmazások; vírusvédelmi rendszerek stb.

Adatbázis-kezelő rendszer(ek) és verzió: az adott szerverre vagy mainframe-re telepített adatbázis-kezelő (DBMS) rendszert kell megjelölni, a kliensként telepített adatbázis hozzáférést nem kell feltüntetni, pl.: Oracle 8, Sybase, SAS 6.12.

1.1.2. Kérdőív: Hálózati hardver és szoftver topológia

- Milyen hálózati protokollokat alkalmaznak a belső és külső kapcsolatokra?

  .....

  .....

  .....

- Rendelkeznek-e az intézmény hálózatát bemutató, naprakész topologikus ábrával (Igen/Nem):

Ha az intézmény nem rendelkezik a fenti ábrával, akkor kérjük elkészíteni!

- A hálózati topológia másolatán kérjük jelölje be az alábbiakat, és az ábrát csatolja a kitöltött kérdőívekhez:

  – a külvilághoz való csatlakozási pontokat és az azon használt protokollokat (pl. internet bérelt vonal, TCP/IP; modem, PPP; X.400)

  – pénzügyi-számviteli alkalmazások feldolgozási és felhasználói helyeinek (pl. bérszámfejtés, beszerzés, utalványozás stb.) munkaállomás- vagy terminál-azonosítóit, és az alkalmazás azonosítóját

  – pénzügyi-számviteli alkalmazások output kibocsátási pontjaihoz (pl. pénzügyi beszámoló, bérlista stb. nyomtatása) tartozó munkaállomás- vagy terminál-azonosítókat, és az alkalmazás azonosítóját

  – főbb hálózati elemeket (pl. gateway-ek, router-ek, switch-ek, hub-ok)

  – védelmi rendszereket (pl. tűzfal, behatolásvédelmi rendszer (IDS) stb.)

Kitöltési és értékelési útmutató az 1.1.2. kérdőívhez

Milyen hálózati protokollokat alkalmaznak: csak felsorolásszerűen kell feltüntetni az intézményben - belső és külső kapcsolatokra - alkalmazott protokollokat. Pl. TCP/IP, IPX 32, X.400, EDI.

Rendelkeznek-e az intézmény hálózatát bemutató, naprakész topologikus ábrával: a topologikus ábra az intézmény informatikai eszközeit, fizikai kapcsolatait és külvilághoz való csatlakozását mutatja be. Azonosíthatónak kell lennie annak, ha az intézmény több épületben helyezkedik el, illetve telephelyekkel rendelkezik. Az ábrának mindig naprakésznek kell lennie, azaz hűen kell tükröznie az aktuális állapotot.

A topologikus ábra hiánya még kisebb informatikai park esetén is megnöveli az ellenőrzés kockázatát. Ennek hiánya - többek között - megnehezíti a rendszer hatékony és biztonságos üzemeltetését és karbantartását; másrészt az ellenőr sem tudja a szervezet informatikai parkját és kapcsolatait átlátni, és így a vizsgálandó rendszert körülhatárolni. Ezért ha a szervezetnek ilyen topologikus ábra nem áll rendelkezésre, el kell készíttetni!

A topologikus ábra kiegészítése:

A kiegészítésre két célból van szükség. Egyrészt egy első értékelési támaszt nyújt az ellenőrnek a biztonságtechnikai kockázatok felméréséhez, illetve annak eldöntéséhez, hogy milyen informatikai szakértelemre lesz szükség a vizsgálat során. Ha az intézmény kiterjedt és "szövevényes" informatikai parkkal rendelkezik, akkor a kritikus pontokon (külvilággal, alhálózatokkal való kapcsolódási pontok, modemes bejelentkezési helyek stb.) részletesebben kell felmérni az informatikai biztonságra vonatkozó kockázatokat. Ugyanakkor egy kisebb rendszer is hordozhat magában nagy kockázatot, ha a pénzügyi rendszer informatikai eszközei védelem nélkül csatlakoznak a külvilághoz. Továbbá a topologikus ábra alapján megítélheti az ellenőr azt is, hogy mely kritikus fontosságú - biztonsági - eszközök részletes vizsgálatára lesz szükség, és ehhez esetleg milyen szakértőt kell igénybe venni.

Másodsorban a topologikus ábra a legalkalmasabb eszköz arra is, hogy az ellenőr behatárolja, a pénzügyi-számviteli rendszer vizsgálatához az informatikai park mely jól körülhatárolható részét kell figyelembe vennie. A rendszer körülhatárolása csak akkor korlátozódhat az intézmény egy részére, ha azt a részterületet jól működő és megbízható kontrollok - fizikai eszközök és védelmi szoftverek - védik az egyéb területektől.

1.2.1. Kérdőív: Alkalmazások felsorolása

Pénzügyi-számviteli alkalmazások

Alkalmazás neve, azonosítója, verziószáma	Hardver platform és operációs rendszer	Az alkalmazást felhasználó szervezeti egységek

Egyéb, az ellenőrzés és a szervezeti működés szempontjából jelentős alkalmazások

Alkalmazás neve, azonosítója, verziószáma	Hardver platform és operációs rendszer	Az alkalmazást felhasználó szervezeti egységek

Kitöltési és értékelési útmutató az 1.2.1. kérdőívhez

Mi számít pénzügyi-számviteli és mi egyéb alkalmazásnak: pénzügyi alkalmazásnak tekintendő minden olyan szoftver, mely konkrét pénzbeli értékkel bíró tranzakciókat kezel, feldolgoz, vagy ilyen információkat tart nyilván. A legjellemzőbb ilyen típusú alkalmazások: pénzügyi beszámoló elkészítését támogató, főkönyvi, előirányzat-, kötelezettségvállalás-, számlanyilvántartó, logisztikai, bérszámfejtési, kontrolling, készletnyilvántartó stb. rendszerek.

Egyéb alkalmazásokhoz azon felhasználói szoftvereket kell felsorolni, melyek a fentebb említett pénzügyi-számviteli rendszerekhez kapcsolódnak, azaz felhasználják azok nyilvántartását, illetve adatokat szolgáltatnak feléjük.

> *Ellenőrzésük azért bír jelentősséggel, mert az egymással összefüggésben levő alkalmazó rendszerek inkonzisztens működése - közvetve vagy közvetlenül - veszélyeztetheti a pénzügyi adatok megbízhatóságát. Ilyen alkalmazások jellemzően: személyi nyilvántartás, munkaügyi nyilvántartás, vezetői információs rendszerek stb.*

Alkalmazás neve, azonosítója, verziószáma: a név általában tömören, természetes nyelven határozza meg az alkalmazást, pl.: Bérszámfejtő Rendszer. Az azonosító rendszerint az előbbi megnevezés rövidítése, és sok esetben így hivatkoznak rá egyéb rendszerek is, pl. BÉRR.

> *Egy alkalmazás az idő folyamán kisebb-nagyobb változásokon megy keresztül (pl. jogszabálykövetés, korszerűsítés miatt), miközben alapvető feladatai és funkciói nem biztos hogy változnak (a nagyobb változások esetén már azok is). Ugyanakkor szükséges pontosan azonosítani, hogy az alkalmazás mikor, melyik állapotát használták, illetve használják. Erre szolgál a verziószám, pl. 5.4. (Az első szám általában nagyobb változtatásokkor "ugrik", pl. ha karakteres verzióról áttérnek grafikusra; a második vagy ha van harmadik pedig kisebb módosításkor, pl. új nyomtatási funkciókat tesznek bele az alkalmazásba.)*
>
> *Az alkalmazás azonosításával az ellenőr kialakíthatja első benyomását a kockázatokról. Ha ismert, és más helyeken ugyanilyen formában használt és már ellenőrzött alkalmazásról van szó, akkor könnyebben behatárolható az eredendő és a kontroll kockázat, és csökkenhet az ellenőrzés kockázata.*

Hardver platform és operációs rendszer: annak a hardvernek és operációs rendszernek a típusát kell megjelölni, amelyen az adott alkalmazás fut. Ha több hardver platformon és/vagy különböző operációs rendszer alatt fut az alkalmazás, mindet meg kell jelölni. Pl. 4 db. Pentium II-es PC, 2 db. Pentium IV-es PC, MS Windows 2000; illetve SUN Sparc Classic, SunOS 5.3.

Ha az alkalmazás kliens-szerver módban működik, akkor a szerverként működő gépet és operációs rendszerét (a fenti módon) alá kell húzni!

Ezek olyan információk, melyek elsősorban az alkalmazás környezetéről alakítanak ki képet az ellenőr számára. A hardver és az operációs rendszer már önmagában meghatároz bizonyos fenyegetettségeket és kockázatokat, melyeket a továbbiakban figyelembe kell venni. (Pl. Egy DOS-os vagy Windows 98-as operációs rendszer önmagában nem rendelkezik olyan biztonsági funkciókkal, amelyek egy komoly pénzügyi rendszer védelméhez szükségesek.)

1.2.2. Kérdőív az IT vezetés számára: Alkalmazások részletes információi

Alkalmazás neve, azonosítója, verziószáma:	
Fejlesztő cég neve / belső fejlesztés / testreszabott szoftver:	
Programozási nyelve, amiben fejlesztették:	
A szoftver adatbázis-kezelő rendszere és verziója:	
Összes felhasználó száma:	
Tranzakció indítási és/vagy adatmódosítási jogokkal rendelkezők száma:	
Milyen egyéb végfelhasználói alkalmazásokkal áll kapcsolatban; kiemelendő, ha a kapcsolat elektronikus:	
Alkalmazás szinten milyen védelmet alkalmaz a hozzáférések korlátozására:	
Telepítés dátuma:	Utolsó módosítás dátuma:
Az utolsó módosítás oka:	
Az alkalmazás esetleges problémái, korlátai:	

1.2.3. Kérdőív a felhasználók szakterületi vezetői számára: Alkalmazások részletes információi

Alkalmazás neve, azonosítója, verziószáma:
Alkalmazás rövid leírása (tüntesse fel, milyen típusú és volumenű tranzakciókat kezel / év):
Összes felhasználó száma:
Tranzakció indítási és/vagy adatmódosítási jogokkal rendelkezők száma:
Milyen egyéb végfelhasználói alkalmazásokkal áll kapcsolatban; kiemelendő, ha a kapcsolat elektronikus:
Alkalmazás szinten milyen védelmet alkalmaz a hozzáférések korlátozására:
Utolsó módosítás dátuma:
Az utolsó módosítás oka:
Az alkalmazás esetleges problémái, korlátai:

Kitöltési és értékelési útmutató az 1.2.2. és 1.2.3. kérdőívhez

Az alábbiakban az 1.2.2. és 1.2.3. kérdőív kérdéseit – a témakör egyezése és a részben átfedések miatt – egyben tárgyaljuk!

Mely alkalmazásokhoz kell kitölteni a kérdőíveket:

- *az 1.2.1-ben felsorolt minden egyes pénzügyi-számviteli alkalmazáshoz,*
- *az ellenőr által kiválasztott egyéb alkalmazásokhoz is, melyeket a felmérés szempontjából szükségesnek ítél.*

Alkalmazás neve, azonosítója, verziószáma: ugyanaz, mint az 1.2.1. kérdőívben. Ez a mező szolgál azon alkalmazások - az 1.2.1. kérdőív alapján - azonosítására, amelyekhez részletesebb adatlapot is kitöltöttek.

Alkalmazás rövid leírása: olyan leírást kell kérni, amely bemutatja, hogy:

- az adott alkalmazás milyen típusú adatokat dolgoz fel (pl.: tárgyi eszközök mozgása, pénzügyi mozgások, utalások);
- honnan származnak a bemenő adatok, (input, pl: bizonylatok, más rendszertől kapott feladás listán, elektronikus úton);
- milyen típusú pénzügyi, számviteli, vagy egyéb feldolgozást végez, (esetleg milyen szabályok, rendelkezések alapján); valamint
- milyen kimenetet, adatokat állít elő és kinek/minek részére (pl.: nyomtatott listák, táblázatok, elektronikus feladások a bérszámfejtés számára).

  A tranzakciók volumenének meghatározása segíti az ellenőrt az adott alkalmazás jelentősségének, kockázatának megítélésében.

Fejlesztő cég neve / testreszabott / belső fejlesztés: Csak a fejlesztő cég(ek) nevét kérjük feltüntetni, ha az alkalmazást a vizsgált szervezet készen vásárolta és változtatás nélkül alkalmazza, vagy saját követelményeik alapján külső vállalkozóval / intézménnyel fejlesztette.

Testreszabott szoftvereknek nevezzük azon alkalmazásokat, melyek olyan paraméterezési lehetőségekkel rendelkeznek, melyeken keresztül az alkalmazás működését a szervezet igényeihez és működéséhez lehet igazítani. A paraméterek értékét a felhasználói igények és a szervezeti szabályok alapján határozzák meg, és beállításukhoz - a legtöbb esetben - nem szükséges programozói szakértelem. Testreszabott rendszer esetében fel kell tüntetni hogy "testreszabott", valamint a fejlesztő és telepítő cégek nevét.

"Belső fejlesztés"-t kell megjelölni abban az esetben, ha az alkalmazás kifejlesztése az intézmény saját erőforrásaival (humán, hardver, szoftver, stb.) történt.

A fejlesztő cég meghatározása egyrészt az alkalmazás pontos azonosítását szolgálja. Ez azért lényeges, mert az ellenőrzés kockázata csökken, ha egy, korábban már több alkalommal is vizsgált és ismert szoftverről van szó. Részletes ellenőrzés esetén az ellenőr esetleg további információkért is fordulhat a fejlesztőkhöz.

A testreszabott rendszerek nagy előnye, hogy a szervezeti igényekhez való alakítása, paraméterezése - azaz testreszabása - kisebb kockázattal jár, mint a számítógépes forráskód átprogramozása. Ezáltal az ilyen rendszerek telepítése és módosítása - általában - biztonságosabb.

Programozási nyelve, amiben fejlesztették: a programozási nyelve megjelölése egyértelmű, pl. C++, Java, Delphi.

Az adatbázis-kezelő rendszer és verziója:. Adatbázis-kezelő rendszernek azt kell megjelölni, amelyben az alkalmazás által kezelt adatbázisokat tárolják. Pl. DBASE 4 ; Oracle 8.

A fenti információk sokat elárulhatnak a kockázatokról, illetve az ellenőrzéshez szükséges speciális szakértelemről. Nagy kockázatot jelenthet pl. ha egy bérszámfejtési alkalmazást DOS-os alapon, DBASE/CLIPPER-ben fejlesztettek, mert ez a környezet eleve nem nyújt hatékony védelmi lehetőséget a programok számára, és így a bér adatok vagy törzsállományok egy egyszerű szövegszerkesztővel is módosíthatóak. Nagyobb biztonságot nyújthat (hangsúlyozva a feltételes módot, mert csak lehetőség!) egy UNIX alapú, ORACLE SQL-ben fejlesztett alkalmazás. Ez utóbbi ellenőrzése viszont komolyabb, speciális szakértelmet igényelhet.

Összes felhasználó száma: a felhasználók a szervezet azon dolgozói, akik valamilyen – bármilyen – hozzáféréssel rendelkeznek az adott alkalmazáshoz.

Általában minél nagyobb a felhasználók száma, és minél jelentősebb pénzügyi szempontból az alkalmazás, annál nagyobb a bizalmasság sérülésének kockázata is.

Tranzakció indítási illetve adatmódosítási jogokkal rendelkezők száma: az összes felhasználóból hányan rendelkeznek olyan hozzáférési jogokkal, amivel tranzakciókat indíthatnak (pl. bevételezések, feladások), illetve pénzügyi (átutalási összegek, főkönyvi adatok) vagy törzsadatokat (adókulcsok, személyi besorolás) rögzíthetnek, módosíthatnak.

A tranzakció indítási és adatmódosítási jogok relatíve nagy száma pedig további kockázatot jelent az adatok sértetlenségére, hitelességére és rendelkezésre állására is.

Milyen egyéb végfelhasználói alkalmazásokkal áll kapcsolatban; kiemelendő, ha a kapcsolat elektronikus: az egyes szervezeti funkciók és feladatok kapcsolatban állnak egymással, tehát adatokat szolgáltatnak egymásnak és kapnak egymástól. Hasonló módon az egyes számítógépes alkalmazások - amelyek gyakorlatilag az említett feladatokat hivatottak ellátni vagy megkönnyíteni -, is kapcsolatban állnak egymással. A kapcsolat lehet papír alapú (pl. az egyik alkalmazás kinyomtatott adatait felhasználják a másik alkalmazás input-jához) vagy elektronikus (amikor az adatok elektronikus úton - hálózat, lemez stb. - kerülnek át egyik alkalmazásból a másikba).

> *Elektronikus kapcsolat esetén - bonyolultságtól függően - növekedhet a kockázat, valamint a kontrollok ellenőrzéséhez speciális szakértelemre is szükség lehet.*

Alkalmazás szinten milyen védelmet alkalmaz a hozzáférés korlátozására (ha van ilyen): az alkalmazási szintű védelem azt jelenti, hogy a hozzáféréshez szükséges ezen védelmi eljárások csak az alkalmazás elindításakor, illetve futása közben lépnek működésbe. Nem tartoznak ide tehát a számítógép elindításához, hálózatba való belépéshez tartozó védelmi eljárások.

A leggyakrabban a következő eljárásokat alkalmazzák: egyéni felhasználói azonosítók és jelszavak a programba való belépéshez vagy egyes adatbázisokhoz való hozzáféréshez; egyéb hitelesítő eszközök, mint pl. "smart card", biometrikus azonosítók; egy bizonyos tétlenségi idő után a program jelszavas lezárása (time out) stb.

> *Ha nincs legalább egy jelszavas védelem a programhoz, az növeli a kockázatot. Ez a kockázat továbbá nagyon magas lehet, ha egy olyan pénzügyi szempontból jelentős alkalmazásról van szó, ami hálózatba kötött gépen fut.*

Telepítés dátuma: az az időpont, amikor az alkalmazást a jelenlegi azonosítója alatt telepítették a számítógépekre.

> *Sokszor előfordul, hogy egy alkalmazás nagyobb változásokon megy keresztül, megváltoznak funkciói és feladatai is. Az ilyen változtatások esetében nem csak az alkalmazás megjelenése, hanem belső működése is jelentős módosításokon esik át. A fejlesztők ilyen esetekben új azonosítóval látják el az alkalmazást, és az ellenőrzés szempontjából ezen verzió telepítése a releváns információ.*
>
> *A friss programok a tapasztalat hiánya és az elkerülhetetlen hibák miatt általában nagyobb kockázattal rendelkeznek, továbbá az új funkciókkal új fenyegetettségek, sebezhetőségek és kockázatok jelennek meg.*

Utolsó módosítás dátuma: az a dátum, amikor az alkalmazás forráskódját vagy jelentős beállításait a telepítés óta megváltoztatták. Mindkét esetben fejlesztők vagy IT szakemberek által végzett változtatásokról van szó, ugyanis optimális esetben a felhasználó nem tud olyan változtatást végrehajtani az alkalmazáson, mely a működést módosíthatja.

Ha az utolsó módosítás régen történt, az jelentheti az alkalmazás megbízható működését és alacsonyabb kockázatát (fordítva nem igaz, azaz az alkalmazás friss módosítása még nem jelenti feltétlenül a szoftver megbízhatatlan működését).

Az utolsó módosítás oka: a módosítást az előző pontban definiáltuk (az alkalmazás forráskódján vagy beállításain fejlesztők vagy IT szakemberek változtatást végeznek).

A módosítást kezdeményezhetik a felhasználók, az IT biztonsági felügyelő és az IT szakemberek is, így célszerű erről a kérdésről minden oldalról tájékozódni, a pontos információ érdekében. Természetesen a pénzügyi ellenőrzés szempontjából a pénzügyi szakmai, illetve a működtetési okokból bekövetkezett változtatások a lényegesebbek. Ugyanakkor fontos lehet az is, ha pl. új - informatikai - biztonsági szolgáltatást építenek be az alkalmazásba.

A kérdésre adott válasz, azaz a módosítás oka sokat elárulhat az alkalmazás megbízhatóságáról és kockázatáról, s ezzel pontosítja az adott alkalmazásról kialakított képet.

Az alkalmazás esetleges problémái, korlátai: szabadon kitölthető, megjelölhető az alkalmazás minden olyan tulajdonsága és paramétere, amit a felhasználók vagy az informatikai személyzet problémának vagy korlátnak tart. Pl.: rendszeres lefagyás, sok visszautasított tranzakció, hosszú válaszidő, bonyolult hozzáférési eljárások, nehéz karbantarthatóság.

Az alkalmazás korlátai olyan funkcióbeli hiányosságok lehetnek, amelyeket az adott szoftver nem tud elvégezni vagy kezelni.

Az összes lehetséges probléma felsorolása, és értékelése természetesen nem lehetséges, példaként említünk néhányat. A problémák között szerepelhet pl. az alkalmazás rendszeres lefagyása, vagy a gyakori visszautasított tranzakciók, melyek egyértelműen az alkalmazás gyengeségét mutatják. Hasonlóan problémaként jelenhet meg pl. a hosszú válaszidő egy tranzakció elindítása után, vagy a túl bonyolult hozzáférési eljárások, amelyek szintén jelenthetnek gyengeséget az alkalmazásban vagy a rendszerben, de jelenthetik a biztonsági eljárások nagyfokú alkalmazását is. A nehéz karbantarthatóság pedig bármely egyéb probléma vagy változáskövetés kezelését nehezíti, növelve a nem megfelelő vagy nem hatékony üzemeltetés kockázatát.

Sokszor előfordul, hogy ha egy szoftver alkalmazása és üzemeltetése korlátokba ütközik, akkor a hiányosságokat ad-hoc vagy szabálytalan megoldásokkal küszöbölik ki. Ezek megnövelhetik a hibázások számát és a pénzügyi rendszerben rejlő kockázatokat.

A problémák és korlátok - a módosítások okaihoz hasonlóan - közvetlenül utalhatnak az alkalmazás gyengeségeire, kockázataira. Ezeken keresztül az ellenőr gyorsabban és hatékonyabban behatárolhatja, hogy a pénzügyi rendszer, és ezen

belül az egyes alkalmazások ellenőrzésekor milyen mélységű vizsgálatra és milyen szakértelemre lesz szüksége.

2. Az informatikai tevékenység felmérése kérdőívek alkalmazásával

Az informatikai tevékenység felmérésének célja, hogy az ellenőr megismerje azon tevékenységeket és szervezeti működést, melyek a pénzügyi-számviteli rendszerek megbízható működését befolyásolhatják. Itt is megemlítjük, hogy a vizsgálat elsődlegesen közvetlenül a pénzügyi informatikai rendszerre koncentrál, de a közvetett összefüggések miatt szükséges az egész szervezet informatikai szemszögű, átfogó felmérése annak érdekében, hogy az ellenőr minden lehetséges befolyásoló tényezőt feltárhasson.

A kérdőívek kiértékelése alapján megállapítható:

- a szervezeti keretek lehetővé teszik-e az informatika - és benne a pénzügyi-számviteli rendszerek - megfelelő működtetését;
- megvan-e a szükséges magas szintű szabályozás a részletesebb kontrollok megfelelő kialakításához;
- milyen kontrollok töltenek be lényeges szerepet a szervezetnél;
- mely kontroll területek ellenőrzéséhez szükséges IT szakellenőr igénybevétele.

A kérdőívek három csoportra oszthatóak: *1. Üzemeltetés, fejlesztés; 2. Szervezeti keretek; 3. Magas szintű szabályozások*

A kérdőíveket az ellenőrzött szervezetnek kell kitöltenie, de az ellenőrzési kockázat csökkentése érdekében itt is javasoljuk az ellenőr aktív közreműködését. Az informatikai tevékenység felmérésére vonatkozó mindhárom kérdőívet az informatikáért legmagasabb szinten felelős szervezeti vezetőnek, illetve vele együtt kell kitölteni!

Üzemeltetés, fejlesztés

A szervezetnek gondoskodnia kell informatikai környezetének megfelelő üzemben tartásáról annak érdekében, hogy az intézmény működését, illetve ezen belül a pénzügyi-számviteli rendszerek működését biztosítsák. Mivel a szervezetek feladatai és igényei folyamatosan változnak, ez a tevékenység nem korlátozódhat kizárólag a fenntartásra, biztosítani kell változtatások és fejlesztések megfelelő végrehajtását is. Ez utóbbi nem csak a zökkenőmentes átállás biztosítását igényli, hanem az információ-biztonság és ellenőrizhetőség megőrzését a változtatások alatt és után is.

Az üzemeltetésre és fejlesztésre vonatkozó kérdések a következő területeket fedik le:

- a számítógépes rendszer működtetése
- problémák kezelése
- konfiguráció-kezelés
- változáskezelés

- új rendszerek fejlesztése

Szervezeti keretek

Az informatikai tevékenységekhez soroljuk az informatika szervezeti helyének, illetve szervezeten belüli kezelésének és vezetésének megismerését is. Az informatika intézményen belül betöltött szerepe, helye és irányításának módja ugyanis befolyásolja, hogy a rendelkezésre álló erőforrásokat megfelelően tudják-e kezelni. Azaz az üzemeltetés, a problémák megoldása és az informatikai fejlesztés ütközhet-e szervezeti akadályokba, megállapíthatóak-e a felelősségi és feladatkörök, adottak-e az információ-biztonság megteremtésének szervezeti feltételei.

A szervezeti keretekre vonatkozó kérdések a következő területeket fedik le:

- az informatika helye a szervezetben
- a felső vezetés elkötelezettsége
- feladatkörök szétválasztása

Magas szintű szabályozások

Az informatikai tevékenység megismerésének keretében tartjuk célszerűnek felmérni a magasabb szintű szabályozásokat, a politikákat is. A politikák két szempontból lényegesek az ellenőrzés számára. Egyrészt megmutatják, hogy megvan-e a szabályozottságnak az a szükséges mértéke, amely számonkérhető módon teszi lehetővé a pénzügyi, ügyviteli folyamatok számítógépesített lekövetését. Másrészről a gyakorlat azt mutatja, hogy a magas szintű IT politikák, eljárások és sztenderdek nagyon fontos szerepet játszanak a szervezet belső kontroll mechanizmusának kialakításában. Azon intézmények, melyek nem rendelkeznek stabil, magas szintű szervezeti és vezetői IT kontrollokkal, valószínűleg a részletes alsóbb szintű kontrollokat sem tudják megfelelően kialakítani.

A magas szintű szabályozások csoportjában a kérdések a következő területeket fedik le:

- informatikai stratégia
- informatikai biztonságpolitika
- működésfolytonossági terv
- hozzáférések szabályozása
- dokumentációs politika
- belső ellenőrzés szerepe

2.1. Kérdőív: Üzemeltetés, fejlesztés

A számítógépes rendszer működtetése

2.1.1. Léteznek-e rögzített szabályozások arról, hogy az IT szervezeti egység milyen szolgáltatási szintet (rendelkezésre állás, normák stb.) biztosít a felhasználói rendszerek számára?

2.1.2. Igénybe vesz-e a szervezet külső szolgáltatókat/szakértőket egyes informatikai üzemeltetési tevékenységek ellátására (rendszer karbantartás, adatbázis adminisztráció stb.)? Ha igen, milyen tevékenységekre?

2.1.3. Ki, milyen módon és milyen gyakorisággal felügyeli a rendszergazdák és az esetleges külső szolgáltatók/szakértők tevékenységét? Milyen eljárásokat alkalmaznak a felügyeletükre?

2.1.4. Milyen képzettsége és gyakorlata van az üzemeltető (rendszergazda, karbantartó, technikus, stb.) alkalmazottaknak?

2.1.5. A hálózat központi egységei, illetve a pénzügyi rendszerek előállítanak-e feldolgozási naplókat (log-okat)? Gyakorlat-e ezek felhasználása a szokatlan vagy szabálytalan tevékenységek detektálására?

Problémák kezelése

2.1.6. Szabályozott-e a felhasználók informatikai problémáinak jelentése és kezelése? Létezik-e ún. help desk funkció a szervezetben?

2.1.7. Készítenek-e a bejelentett problémákról összesítéseket, statisztikát?

Konfiguráció-kezelés

2.1.8. Ki felelős a konfiguráció-kezelésért?

2.1.9. Rendelkeznek-e naprakész konfigurációs nyilvántartással, amely tartalmazza a hardver, a szoftver, a dokumentációs és adatkommunikációs elemeket?

Változáskezelés

2.1.10. Rendelkezik-e a szervezet írásban is meghatározott változáskezelési eljárással?

Új rendszerek fejlesztése

2.1.11. Folyamatban van-e olyan új alkalmazói szoftver fejlesztése vagy beszerzése, amely közvetlenül vagy közvetve kapcsolódik a szervezet pénzügyi-számviteli ügyme-neteihez? (Ha igen, akkor kérjük, csatolja ezen szoftverek jellemzését az 1.2.2. kérdőív "Alkalmazás rövid leírása" kitöltése alapján)

2.1.12. A specifikációk elkészítése folyamán tekintetbe vették-e a szoftverek ellenőrizhetőségének követelményét? (Erre csak akkor válaszoljon, ha az előző kérdésre igennel válaszolt!)

Kitöltési és értékelési útmutató a 2.1. kérdőívhez

Az üzemeltetési kontrollok csökkentik az IT osztályon belüli nem megfelelő munkagyakorlat kockázatát. A nem megfelelő munkagyakorlat befolyásolja az ellenőrzést is, mivel a legtöbb esetben az informatika alkalmazásán alapul a pénzügyi jelentések készítése. Az üzemeltetési környezet gyengeségei kihasználhatóak nem engedélyezett programok futtatására vagy a pénzügyi adatok szabálytalan megváltoztatására; illetve ilyen esetben gyakoribb a nem szándékos hibák előfordulása. Az üzemeltetési környezet megfelelő kialakítása ugyanakkor lehetővé teszi a visszaélések és hibák feltárását, és biztosítja a számonkérhetőséget is.

A számítógépes rendszer működtetése

2.1.1. A szervezeti folyamatokon belül az informatika alapvetően kiszolgáló funkciót tölt be, azaz az egyéb funkcionális feladatokat ellátó területek működési feltételeit - legalábbis egy jelentős részét - biztosítja. A felhasználói és informatikai területek megfelelő működésük biztosítása érdekében szabályozást készíthetnek az informatika által nyújtandó *szolgáltatási szintről*. A szabályozás rögzíti azon feltételeket, amelyeket a felhasználók az informatikától elvárnak, illetve azt, amit az informatikának nyújtania kell. Ez a dokumentum tehát a felügyeletet teszi könnyebbé és átláthatóbbá. A szabályozásban rögzíthető feltételek lehetnek:

- a rendszer rendelkezésre állása, azaz annak meghatározása, hogy hiba/leállás esetén maximum mennyi idő alatt kell helyreállítani annak működését;

- a rendszer válaszideje, azaz egy-egy tranzakció elindítása és megerősítése között legfeljebb mennyi idő telhet el;

- a tárigény meghatározása, azaz az informatikának mekkora adattárolási területet kell biztosítania a rendszer(ek) számára;

- biztonsági követelmények megállapítása, azaz milyen szintű logikai és fizikai védelmet kell biztosítani a rendszerek és adatok számára;

- a mentések meghatározása, azaz milyen rendszerességgel kell az adatbázisokról vagy rendszerekről mentést készíteni; stb.

Az ellenőrzés szempontjából a legfontosabb a pénzügyi-számviteli rendszerek szolgáltatási szintjének szabályozása. Ha nincs ilyen szabályozás, az növeli a pénzügyi-számviteli rendszerek nem megbízható működésének, és ebből kifolyólag az adatok sértetlenségének kockázatát. Ebben az esetben az ellenőrzés folyamán részletesebben kell megvizsgálni a rendszerek megbízható működését biztosító kontrollokat, és nagyobb figyelmet kell szentelni az esetleges üzemzavarok hatásának.

Fontos tényező a szabályozás naprakészsége is, hiszen egy új vagy fejlesztett rendszer más igényeket támaszthat mint elődje.

A szolgáltatási szint szabályozásába foglalandó feltételek egy része általában megtalálható egyéb dokumentumokban is (katasztrófa terv, biztonsági szabályzat stb.), de ezek nem pótolják megfelelően a már említett feltételek egységes rögzítését. Ez a szabályozás a leghatékonyabb módja a számonkérhetőség és az informatikai felügyelet biztosításának.

2.1.2. Tüntessen fel minden olyan tevékenységet, melyet az informatikai infrastruktúra (hardver, szoftver, hálózat) üzemeltetése, karbantartása céljából rendszeresen vagy folyamatosan igénybe vesznek!

Az informatikai tevékenységek "kiadásának" jellemző formája az ún. "outsourcing", de létrejöhet bármely más szerződéses kapcsolat keretében. A szervezetek gazdasági megfontolásokból, vagy a megfelelő saját humán erőforrás hiánya miatt vehetnek igénybe rendszeresen külső szolgáltatót/szakértőt. Ez azonban kockázattal jár, mivel az üzemeltetés minősége befolyásolja az intézmény működését, továbbá az üzemeltetési feladatok ellátása közben hozzáférhetnek bizalmas vagy titkos adatokhoz is. Ezért ha a szervezet üzemeltetési tevékenységeinek egy részét "kiadja", akkor részletesen meg kell vizsgálni a szerződés betartására vonatkozó, az üzemeltetési, az adatok bizalmasságát és sértetlenségét biztosító kontrollokat.

2.1.3. Azt a dolgozót/vezetőt kell megjelölni, akinek munkaköri feladatai közé tartozik a rendszergazdák és szolgáltatók/szakértők tevékenységének felügyelete. A felügyelet többféleképpen érvényesíthető (vegyesen is): beszámolók és jegyzőkönyvek készítésén, napló file-ok (ld. 2.1.5.) rendszeres felülvizsgálatán keresztül, belső ellenőrzés keretében stb. A gyakoriság alatt a felügyeleti tevékenység rendszerességének mértéke értendő, mely nem választható el az előbb említett módozatoktól. Például: eseti jellegű, belső ellenőrzés keretében; vagy havi beszámolók készítése, a napló file-ok heti áttekintése; vagy kizárólag a kivételes eseményekről jegyzőkönyv készítése.

Az üzemeltetési tevékenységek bizalmi munkakörök. Feladatkörükbe tartozhat a számítógépek, a hálózatok, a kommunikációs eszközök, a rendszerprogramok, az alkalmazói rendszerek, az adatbázisok felügyelete, beállítása, a működésük biztosítása. Feladataik ellátása érdekében nagyon magas szintű hozzáférési jogokkal, nagy helyismerettel és szakértelemmel rendelkeznek. Tevékenységük rendszeres eljárásokon alapuló felügyelete ezért kiemelkedő fontosságú. Ha nincs felügyeleti tevékenység, vagy eseti jellegű, az megnöveli a rendszerek nem megfelelő működtetésének, illetve a visszaélések kockázatát.

Hiányosságok esetén a tranzakciók és naplófájlok (log-ok) részletes vizsgálatára lehet szükség:

- *fel kell tárni az esetleges visszaéléseket,*
- *részletesebben meg kell vizsgálni a rendszerek megbízható működését biztosító kontrollokat, és*

- *nagyobb figyelmet kell szentelni az esetleges üzemzavarok hatásának.*

2.1.4. Üzemeltető alkalmazottak alatt értendőek a rendszergazdai, karbantartói, technikusi és egyéb üzemeltetési feladatokat ellátó dolgozók. Végzettségként a dolgozó legmagasabb, a feladatkör szempontjából releváns iskolai végzettségét kell megjelölni, gyakorlatként pedig az elmúlt két évben betöltött főbb feladatköreit (akkor is ha azt más intézménynél töltötte be).

> *A szakértelem egy erős kontroll a hibák felett. A nem megfelelő gyakorlat és képzettség növeli a hibázások, a hosszabb idejű rendszerleállások, az adatok véletlen elvesztésének kockázatát. Ha az ellenőr nem megfelelőnek ítéli az üzemeltető alkalmazottak szakértelmét, akkor részletesebben kell megvizsgálni a rendszerek megbízható működését biztosító kontrollokat, és nagyobb figyelmet kell szentelni az esetleges üzemzavarok hatásának.*

2.1.5. A feldolgozási naplók (log-ok) olyan feljegyzések és fájlok, melyek események vagy tevékenységek sorozatáról készülnek. Az ellenőrzés (és egyben a válasz) szempontjából csak azon naplók relevánsak, melyeket a hálózat központi egységei, illetve a pénzügyi számviteli rendszerek készítenek. Ezeket kérjük egyértelműen feltüntetni.

A második kérdés arra vonatkozik, hogy ezen naplókat *rendszeresen* áttekintik-e abból a célból, hogy ezek alapján a szokatlan vagy szabálytalan tevékenységeket feltárják.

Log fájlok többféle célból és többféle módon készülhetnek, többek között:

- *egy folyamatról, melynek segítségével nyomon követhetőek a tranzakciók lépései;*

- *egyes erőforrások használatáról, melynek alapján megállapítható, hogy pl. ki és mikor használta őket;*

- *felhasználókhoz kötődően, ami pl. azt mutatja, hogy az adott felhasználó mit és mikor használt, milyen tranzakciót futtatott.*

Hogy melyik módszer a hatékonyabb, az mindig az adott cél alapján dönthető el. A naplók alapvetően két célt szolgálnak: az ellenőrizhetőséget (felügyeletet), és üzemzavar esetén a visszaállíthatóságot.

A naplók - az ellenőrizhetőség megteremtésével - csökkentik a szabálytalan tevékenységek kockázatát, illetve - a visszaállíthatóság biztosításával - csökkentik az esetlegesen előforduló hibák végleges hatását. Mindemellett ezek biztosít(hat)ják a leghatékonyabb ellenőrzési nyomvonalat és ellenőrzési bizonyítékokat. Emiatt, ha a rendszerek nem állítanak elő naplót, az jelentősen megnöveli az ellenőrzés kockázatát, ezért az üzemeltetés és az alkalmazások vizsgálatakor részletes tesztekre lesz szükség. Ha van napló, de ezeket nem használják fel a tevékenységek felügyeletére, akkor a tranzakciók és naplófájlok részletesebb vizsgálatára lehet szükség az ellenőrzés során az esetleges visszaélések feltárása érdekében.

Problémák kezelése

2.1.6. Rendelkezik-e a szervezet írásban lefektetett eljárásrenddel, amely:

- meghatározza hogy a felhasználók kihez fordulhatnak az informatikával kapcsolatos problémáikkal és kérdéseikkel, és

- biztosítja hogy a problémák kezelése a lehető legrövidebb időn belül a megfelelő szakemberhez kerül?

  Sok szervezetben ezt egy úgynevezett "help desk" munkakör vagy szervezeti egység kialakításával oldják meg. A felhasználók problémáikkal a "help desk"-hez fordulnak, ahol a bejelentést rögzítik, és ott döntik el, hogy melyik szakembert kell megbízni a megoldással. A "help desk" feladatköréhez tartozik még a végrehajtás ellenőrzése is.

  A problémák jelentését és kezelését meghatározó eljárásrend csökkenti a problémák megoldatlanságának, és a hosszabb üzemzavarok kockázatát. Pénzügyi-számviteli rendszerek esetében pedig kiemelten fontos a problémák gyors és szakszerű megoldása. Ha ilyen eljárásrenddel nem rendelkezik a szervezet, akkor részletesebben kell megvizsgálni a folyamatos üzemeltetést biztosító kontrollokat.

2.1.7. Az összesítések és statisztikák célja a gyakran előforduló hibák és problémák egységes feldolgozása, hogy ennek alapján a vezetés megtehesse a szükséges intézkedéseket.

> *Az összesítések és statisztikák alapján a szervezet hatékonyabban tud védekezni a gyakran előforduló hibák és problémák ellen, és segíthet felderíteni a ritkábban előforduló, de jelentősebb kihatású problémák megoldását. Az összesítések és statisztikák továbbá ellenőrzési nyomvonalat biztosítanak a vizsgálat számára a múltban előforduló problémák azonosítására, a jelentősebb kockázattal rendelkező területek, folyamatok meghatározására. Az összesítések alapján gyorsan kiszűrhetőek a pénzügyi-számviteli rendszereket és folyamatokat érintő problémák és azok kezelése is.*

Konfiguráció-kezelés

2.1.8. Azt a dolgozót/vezetőt kell megjelölni, akinek munkaköri feladatai közé tartozik a konfiguráció-kezelés tevékenysége. A konfiguráció-kezelés célja, hogy kontrolláljon minden, az informatikai rendszert felépítő komponenst (konfigurációs elemet). Ebbe beletartoznak a számítógépes hardverek, adatkommunikációs eszközök és hálózatok, számítógépes szoftverek, az informatikai rendszerek dokumentációi (specifikációk, tervek, kézikönyvek stb). A konfiguráció-kezelés alapvető feladatai: a konfigurációs elemek teljes körű meghatározása; az egyes konfigurációs elemek pillanatnyi státusának nyilvántartása; a konfigurációs elemek állapotának felügyelete, rendszeres ellenőrzése. A

konfigurációs nyilvántartást biztosíthatja egy leltári rendszer is, ha annak alapján egyértelműen azonosítható, hogy milyen hardvereken milyen szoftvereket alkalmaznak.

> *A konfiguráció-kezelés a változáskezeléshez (ld. 2.1.10. kérdés) szorosan kapcsolódó terület, és gyakori, hogy a változáskezelésért felelős személy egyben felelős a konfiguráció-kezelésért is. Ha van olyan dolgozó, akinek feladatkörébe tartozik a konfiguráció-kezelés, akkor kisebb a kockázata annak, hogy a rendszerben engedély nélküli vagy szabálytalan programok működnek, valamint annak, hogy szabálytalan változtatások észrevétlenek maradnak. Mindezek csökkentik az ellenőrzés kockázatát is.*

2.1.9. Ez az előző kérdésben említett felelős személy egy részfeladatára kérdez rá, de az ellenőrzés szempontjából lényegesnek tartjuk kiemelni a nyilvántartás meglétét, teljességét és naprakészségét. Ilyen nyilvántartással akkor is rendelkezhet a szervezet, ha a már előzőekben említett feladatkört nem hozták létre.

> *Annak vizsgálatához, hogy az egyes konfigurációs elemek szabályszerű állapotban működnek-e, alapvető a nyilvántartás megléte. A szabálytalan komponensek veszélyeztethetik a rendszerek megbízható működését, illetve visszaélésekre adhatnak lehetőséget. Emiatt egy naprakész nyilvántartás hiánya esetén az ellenőrnek részletesebb vizsgálatot kell végezni, hogy felmérje, mely komponensek működnek szabálytalanul vagy engedély nélkül a rendszerben.*
>
> *A nyilvántartás további előnye, hogy a működésfolytonossági terv végrehajtásához fontos segítséget nyújt. Ugyanis ha bármely informatikai rendszert egy katasztrófa után újból üzembe kell állítani, szükség lesz annak ismeretére, hogy a rendszer milyen komponensekből állt össze, és ezek hogyan kapcsolódtak egymáshoz. Egy átfogó konfiguráció-kezelési adatbázis meg tudja adni ezen információkat. A nyilvántartás hiánya tehát a működésfolytonossági tervvel összefüggő kontrollok mélyebb vizsgálatát is szükségessé teszi.*

Változáskezelés

2.1.10. A változáskezelési eljárások rendszerint magukban foglalják:

- a változtatás okának meghatározását,
- a változtatás tárgyának meghatározását,
- a kockázatok felmérését,
- engedélyeztetést,
- üzembe helyezés módját,
- a változtatás sikerességének ellenőrzését, valamint
- mindezen tevékenységek dokumentálását és iktatását.

A gyakorlat azt mutatja, hogy napjainkban az IT szolgáltatás minőségi problémáinak jelentős része visszavezethető az IT rendszer valamely részének megváltoztatására. A változáskezelési eljárások hivatottak biztosítani azt, hogy a számítógépes rendszerek változtatásai megfelelően szabályozottak, teszteltek, elfogadottak és dokumentáltak legyenek. A nem megfelelő változás-kontrollok hibákat vagy visszaéléseket eredményezhetnek a rendszerekben, módosíthatják a pénzügyi adatokat, vagy letörölhetnek ellenőrzési nyomvonalakat. Ha a szervezet nem rendelkezik írásban meghatározott változáskezelési eljárással, akkor részletesebben kell megvizsgálni a változáskezelési, üzemeltetési és alkalmazási kontrollokat.

Új rendszerek fejlesztése

2.1.11. Az új alkalmazói szoftverekbe beleértendőek azon alkalmazások is, amelyeket egy vagy több, már működő alkalmazás leváltására fejlesztenek/szereznek be.

A vezetésnek az új alkalmazások fejlesztése és beszerzése folyamán is gondoskodnia kell az új szoftver(ek) biztonsági és ellenőrizhetőségi követelményeiről, továbbá arról, hogy megfeleljen a tervezett céloknak. Ez a pont tájékoztatást nyújt az ellenőrnek, hogy ezen szempontokat mely fejlesztési vagy beszerzési projektek esetében kell megvizsgálnia.

2.1.12. A szoftverek ellenőrizhetőségének követelményei:

- dokumentált kockázat elemzés és ennek alapján a szükséges kontrollok meghatározása az üzembe állítás előtt,
- olyan funkciók létrehozása az alkalmazásokban, amelyek működés közben lehetővé teszik az ellenőrzési nyomvonal készítését;
- a biztonsági jellemzőket el kell fogadtatni a biztonsági felügyelővel, és
- a fentiek rendszeres ellenőrzéséhez szükséges lehetőségek megteremtése.

A még be nem vezetett alkalmazások nem jelentenek kockázatot az aktuális pénzügyi beszámoló, és az ellenőrzés szempontjából. Ellenőrizhetőségük vizsgálatával elsősorban a következő pénzügyi ellenőrzéseket könnyítjük meg. Ezzel egyrészt ismereteket szerezhet az ellenőr a jövőben használt rendszerekről, másrészt az ellenőrizhetőségi kritériumok számonkérésével csökkentheti a következő vizsgálat ellenőrzési kockázatát.

2.2. Kérdőív: Szervezeti keretek

Az informatika helye a szervezetben

2.2.1. Hol helyezkedik/helyezkednek el az informatikai szervezeti egység(ek) a vizsgált intézmény szervezeti felépítésében?

2.2.2. Meghatározottak-e az informatikai szervezeti egység(ek) felelősségi és hatáskörei? Ha igen, milyen dokumentum határozza meg?

A felső vezetés elkötelezettsége

2.2.3. Ki képviseli az informatikát a felső vezetésben?

2.2.4. Létezik-e a szervezetben informatikai munkabizottság? Képviselteti-e benne magát a felső vezetés?

2.2.5. Ki (név, beosztás) felelős a szervezet informatikai biztonságának felügyeletéért? Milyen időközönként készít jelentést a felső vezetés számára?

Feladatkörök szétválasztása

2.2.6. Kérjük karikázza be az alábbi feladatkörök közül azokat, amelyeket a szervezet dolgozói nem megosztottan végeznek! (Azaz az adott feladatkörben foglalkoztatott dolgozó más feladatkört nem lát el.)

a) IT vezetés
b) Rendszertervezés
c) Alkalmazások fejlesztése
d) Rendszerprogramozás
e) Minőségbiztosítás / tesztelés
f) Változáskezelés
g) IT support - üzemeltetés
h) Rutinszerű karbantartás
i) Adatrögzítés
j) Rendszerbiztonság
k) Adatbázis adminisztráció
l) Hálózat-adminisztráció

m) Egyéb, éspedig:

2.2.7. Kérjük csoportosítsa azon feladatköröket, amelyeket az informatikai alkalmazottak megosztottan végeznek! (Elegendő az előbbi kérdésben alkalmazott betűjeleket használni.) Például ha van dolgozó, aki rendszerprogramozással és alkalmazás fejlesztéssel is foglalkozik, másvalaki pedig rendszertervezéssel és adatbázis adminisztrációval, akkor a következőképpen csoportosítsa: (c,d) ; (b,k).

Kitöltési és értékelési útmutató a 2.2. kérdőívhez

Az informatika helye a szervezetben

2.2.1. Az informatikai szervezeti egység(ek) elhelyezkedése legcélszerűbben egy szervezeti felépítési ábrán mutatható meg. Ha ilyet nem tudnak rendelkezésre bocsátani akkor az informatikát magába foglaló nagyobb szervezeti egységet és a felettes vezetői szinteket kell megjelölni.

Az informatikai szervezet helye a szervezeti hierarchiában meg kell hogy feleljen az informatika szerepének a szervezet működésében. Nem célszerű, ha az informatika más funkcionális területeknek van alárendelve, mivel rendszerint a szervezet minden területét ki kell szolgálnia, illetve működésüket biztosítania. Ehhez pedig az egyéb funkcióktól minél függetlenebb informatikai szervezeti egységre van szükség. Ha a szervezeti hierarchiában az informatika elhelyezkedése nem megfelelő, az növeli az üzemeltetési kockázatot.

2.2.2. A szervezeti egységek feladat- és hatásköreit általában a szervezeti és működési szabályzat határozza meg. Ha ezen kívül van olyan szabályzat vagy dokumentum, ami ezt kiegészítheti vagy módosíthatja, kérjük azt is jelölje meg!

Ha az informatika feladat- és hatásköre nem egyértelműen szabályozott, az megnöveli a hatáskör túllépésének vagy egyes feladatok elhanyagolásának kockázatát. Hiányos szabályozás esetén nincs meg a számonkérhetőség megfelelő alapja sem, ami növeli az ellenőrzés kockázatát.

A felső vezetés elkötelezettsége

2.2.3. A felső vezetés azon tagját kell megjelölni, aki az informatikai tárgyú témákat a vezetés számára előterjeszti, illetve az informatikai feladatok végrehajtásért végső soron felelős.

Az informatikai rendszerekbe történő befektetés mértéke és hatása megköveteli, hogy a felső vezetés személyesen is részt vegyen benne és elkötelezett legyen iránta. Emellett szól az is, hogy az informatikai rendszerek tervszerű és koncentrált alkalmazásán keresztül elérhető befektetési megtérülés igen nagy mérvű lehet.

A vezetés érdeklődése és tudatos hozzáállása a számítástechnikai folyamatokhoz és kontrollokhoz továbbá fontos szerepet játszik abban, hogy a kontrollok tudatosodása a szervezet egészében megtörténjék.

Az ellenőrnek meg kell határoznia, hogy az IT megfelelően van-e képviselve a szervezet vezetésében, azaz az informatikai vezető tagja-e az intézmény legfel-

sőbb irányító testületének (igazgatóság, irányító bizottság, stb.), vagy megfordítva: az irányító testületnek van-e olyan tagja, aki felelős az informatikáért.

A vezetői elkötelezettség hiánya növeli annak kockázatát, hogy a felső vezetői döntések figyelmen kívül hagyják az informatika követelményeit, vagy a már rendelkezésre álló lehetőségeit. Ennek eredménye a felesleges költségeken túl az informatikai rendszer integritásának fellazulása is lehet, ami a rendszerek adatainak megbízhatóságát jelentősen befolyásolhatja.

2.2.4. Ideális esetben a szervezetben működik egy munkabizottság is, amely az informatikáért, annak átfogó irányításáért felelős. A bizottság nem közvetlenül a pénzügyi és számviteli rendszerekért, hanem a közvetlen mögöttük álló informatikai kérdésekért felelős. A bizottság tagjait általában a funkcionális területek és az informatikai osztály képviselői alkotják. (A munkabizottság mérete a szervezet méretétől függ: egy nagyobb intézményben célszerű formálisan is létrehozni ezt a testületet, míg egy kisebben ez működhet informális keretek között is.)

Növeli a hatékonyságot, ha a bizottságban a közép és felső vezetés is képviselteti magát, ezzel is növelve a meghozott döntések súlyát.

Csökkenti az informatikai rendszerek ellenőrzésének kockázatát, ha az informatikai beszerzés, fejlesztés koordinációjában részt vesznek a felhasználók és a felső vezetés. Ennek hiánya a rendszerek kontrollálatlan működtetéséhez vezethet, ami lehetővé teheti az adatok szabálytalan kezelését, hozzáférését is.

2.2.5. Az informatikai biztonságért felelős dolgozó feladatkörébe tartozik az informatikai biztonsági szabályzat (ibsz) és a biztonsági politika összhangjának karbantartása, az ibsz folyamatos aktualizálása a - jogszabályi, innovációs vagy infrastrukturális - változásoknak megfelelően, az ibsz betartatásának folyamatos és rendszeres ellenőrzése, valamint javaslatok tétele a biztonsági követelmények fejlesztésére. A legtöbb szervezetben erre a feladatra hozzák létre a biztonsági felügyelői munkakört.

A biztonság kiemelt fontosságú tényező az intézmények működésében, ezért ennek felügyeletére létre kell hozni a fentiekben már meghatározott munkakört. A felügyeleti tevékenységet végző dolgozónak függetlennek kell lennie, jelentési kötelezettséggel a felső vezetés felé kell rendelkeznie, és tevékenységéről rendszeresen be is kell számolnia. Ezek hiányában a vizsgálat folyamán részletesen kell ellenőrizni az informatikai biztonsággal összefüggő kontrollokat, mind általános tekintetben - a szervezet egészére nézve -, mind az alkalmazások szintjén.

Feladatkörök szétválasztása

2.2.6. és 2.2.7. Ezekben a kérdésekben az informatikai feladatkörök szétválasztásának mértékét és formáját szeretnénk felmérni. Ha van olyan tevékenység amely egyértelmű-

en egyik megnevezett kategóriába sem sorolható be, akkor kérjük, írja be az m) ponthoz!

A feladatkörök szétválasztása az IT osztályon belül csökkenti a hibák és visszaélések kockázatát. Ha a feladatkörök nincsenek eléggé elkülönítve, akkor az egyes számítógépes funkciókat kezelő személyek hibáit vagy visszaéléseit kisebb valószínűséggel lehet észrevenni. A feladatkörök szétválasztása eredményeként a fellépő hibákat hamarabb lehet detektálni. A feladatkörök szétválasztásáról képet kaphat az ellenőr a munkaköri leírások alapján is. Ahol a szükséges feladatköri szétválasztás nem lehetséges - pl. ha az IT osztály kicsi - akkor az ellenőrnek részletesen meg kell néznie az ezt kompenzáló kontrollokat.

A felsorolt feladatkörök részletes leírását ld. a III. fejezet 1.1. pontjában!

2.3. Kérdőív: Magas szintű szabályozások

Informatikai stratégia

2.3.1. Van-e a szervezetnek a felső vezetés által jóváhagyott IT stratégiája? Mióta készítenek rendszeresen IT stratégiát?

2.3.2. A stratégia kiterjed a pénzügyi rendszerekre is?

Informatikai biztonságpolitika

2.3.3. Rendelkezik-e a szervezet informatikai biztonságpolitikával?

2.3.4. Rendelkezik a szervezet informatikai biztonsági szabályzattal?

2.3.5. A fenti dokumentumok (ha vannak) készítése során figyelembe vették-e az ITB 8. és 12. számú ajánlásaiban megfogalmazott tartalmi követelményeket?

2.3.6. Hogyan gondoskodnak arról, hogy az IT biztonságpolitikát és szabályzatot minden dolgozó megismerje (pl. tanfolyamok, közzététel a belső hálózaton, köröztetés)?

Működésfolytonossági terv

2.3.7. Rendelkezik-e a szervezet a felső vezetés által elfogadott működésfolytonossági tervvel?

2.3.8. Lefedi-e a terv pénzügyi-számviteli rendszereket is?

2.3.9. Ki a felelős a terv folyamatos aktualizálásáért, naprakészen tartásáért?

2.3.10. Mikor tesztelték a tervet utoljára? Készült-e a tesztelésről jegyzőkönyv?

2.3.11. Készítenek-e és milyen rendszerességgel mentéseket (backup) a pénzügyi-számviteli adatokról és alkalmazásokról? Az erre használt adattároló eszközöket megfelelően védett helyen tartják?

Hozzáférések szabályozása

2.3.12. Rendelkezik-e a szervezet külön hozzáférés-politikával? Ha nem, akkor milyen egyéb politika keretében került meghatározásra?

2.3.13. Milyen dokumentum szabályozza a hozzáférési jogosultságok megállapítását, engedélyezését, módosítását, karbantartását és visszavonását?

2.3.14. Van-e naprakész nyilvántartása a szervezetnek arról, hogy mely dolgozó milyen hozzáférésekkel rendelkezik a szervezet informatikai rendszereihez? Ki a felelős a nyilvántartás vezetéséért?

Dokumentációs politika

2.3.15. Rendelkezik-e a szervezet IT dokumentációs politikával?

2.3.16. A dokumentációs politika kiterjed-e:

a) a rendszer-specifikációkra,

b) a program dokumentációkra,

c) az operátori/kezelési utasításokra,

d) a felhasználói kézikönyvekre?

Belső ellenőrzés szerepe

2.3.17. A belső ellenőrzések céljába és tárgyába beletartozik-e az informatikai kontrollok (biztonsági, üzemeltetési, hozzáférési, változáskezelési, IT szervezeti stb.) vizsgálata?

2.3.18. Léteznek-e korlátozó rendelkezések, amelyek az informatikai területen befolyásolják a belső ellenőrzés munkáját? Melyek azok?

2.3.19. Rendelkeznek-e a belső ellenőrök informatikai képzettséggel / gyakorlattal?

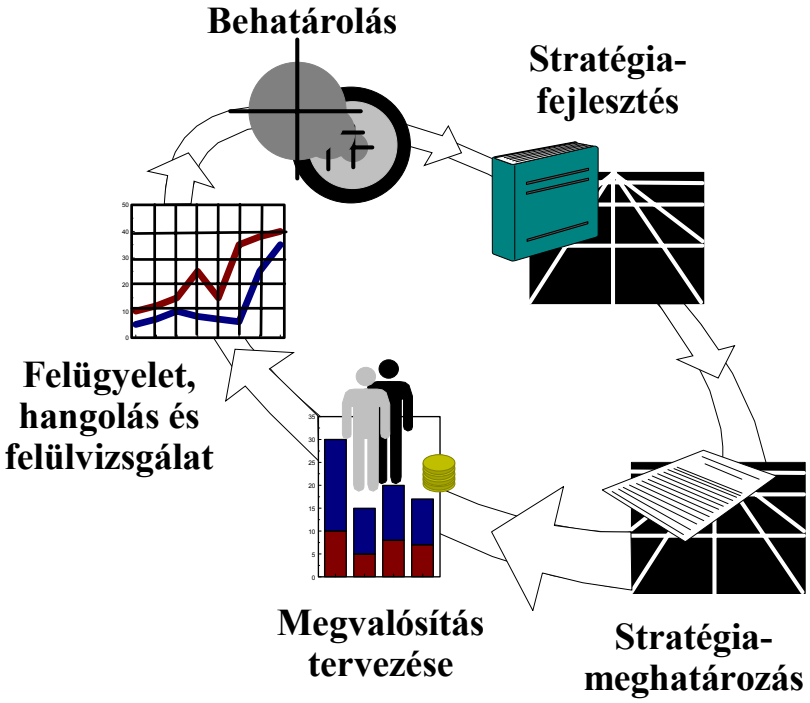
Kitöltési és értékelési útmutató a 2.3. kérdőívhez

A 2.3 kérdőív esetében nem adtunk minden kérdéshez részletes kitöltési és értékelési útmutatót. Csoportonként ismertetjük, hogy az adott témakör az ellenőrzés szempontjából miért fontos, illetve az ott talált hiányosságok milyen kockázatokhoz vezetnek.

Informatikai stratégia

Az informatikai rendszerek magukban hordozzák annak a lehetőségét, hogy megváltoztassák egy szervezet működését. Új lehetőségeket nyitnak, leegyszerűsíthetik az eljárásokat, növelhetik a vezetés hatékonyságát. Hatással vannak a munka- és vezetési gyakorlatra, munkakörökre, beosztásokra, szervezetre, szakértelemre és létszámra. Az informatikai rendszereknek lényegileg kell támogatniuk a szervezet törekvéseit és céljait.

Az informatikai stratégiai tervezés ciklikus és evolúciós jellegű. (Általában 2-3 évre szól.) Rendszeres felügyeletre és hangolásra van szükség, kiegészítve éves és általános felülvizsgálatokkal. A stratégiának, ahogy fejlődik, vissza kell tükröznie a szervezetben és súlypontjaiban bekövetkezett változásokat. Az informatikai stratégia általános felülvizsgálatára 3-5 évenként kell sort keríteni.



Nagyobb szervezetekben több informatikai stratégiára lehet szükség a fő szervezeti-politikai csoportosulásoknak megfelelően.

> *Ha nincs IT stratégia, vagy gyenge minőségű, az olyan rendszerek fejlesztéséhez (beszerzéséhez) vezethet, amelyek nem felelnek meg a szervezet szükségleteinek. A jelenleg működő rendszerek tekintetében növeli az ellenőrzési kockázatot, ha*

IT stratégia már az előző években sem állt rendelkezésre, vagy az gyenge minőségű. Ilyen esetben ugyanis előfordulhat, hogy a már végrehajtott változások, beszerzések nincsenek összhangban a szervezeti célokkal.

IT biztonságpolitika

A felső vezetésnek világos irányvonalat kell kialakítania és demonstrálnia kell támogatását és elkötelezettségét az információ-biztonság felé azáltal, hogy meghatározza a szervezeti informatikai biztonsági politikát.

Az Informatikai Biztonságpolitika (vagy IT Biztonságpolitika) a hatékony információbiztonság menedzsment alapja. A politikát írásban kell rögzíteni és elérhető kell hogy legyen mindazok számára, akik valamilyen felelősséggel rendelkeznek az információbiztonsággal kapcsolatban (általában minden dolgozó).

Az informatikai rendszernek és szolgáltatásainak úgy kell működnie, hogy a felhasználókat megbízható információval lássa el és megvédje az informatikai rendszer adatait a véletlenszerű vagy szándékos sérüléstől. A biztonságpolitika a szervezet és tagjainak az informatikai biztonsághoz kívánatos viszonyulása, az érvényesítés alapelveit fogalmazza meg egységes szemlélettel és az intézmény egészére. Ezek a dokumentumok képezik minden gyakorlati intézkedés és szabályozás alapját.

Az informatikai biztonságpolitika dokumentumainak formája változó, de általában meg kell találni benne az információ-biztonság meghatározását, annak magyarázatát, hogy miért fontos ez a szervezetnek, valamint annak megállapítását, hogy mi szükséges ezek eléréséhez.

Az intézmény területén és kezelésében működő kommunikációs és informatikai rendszerek tervezésére, bevezetésére, üzemeltetésére és ellenőrzésére vonatkozó feladatokat úgy kell elvégezni, hogy a rendszerek védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos. (A közigazgatási intézmények területére az általános biztonságpolitika megfogalmazását lásd az ITB 12.sz ajánlása A Biztonságpolitika megfogalmazása c. fejezetben.)

Ha a szervezetnek nincs informatikai biztonságpolitikája, vagy az nem megfelelő, akkor magas a kockázata annak, hogy a dolgozók nem ismerik pontosan a biztonsági kockázatokat és saját felelősségeiket sem. Biztonsági politika és szabályozás hiányában a következő biztonsági vonatkozású kontrollok részletes vizsgálata szükséges: (logikai és fizikai) hozzáférések, működésfolytonosság, üzemeltetés.

Működésfolytonossági terv

Az informatikai rendszerek folyamatos működtetéséhez meg kell határozni azon stratégiát és terveket, amelyek biztosítják, hogy a kulcsfontosságú működési folyamatok visszaállíthatóak legyenek egy olyan időtartam alatt, amely egy rendszer hiba vagy katasztrófa esetén minimalizálja a működési tevékenység zavarából fakadó veszteséget. Ez utóbbi lehet a működési tevékenységek feletti pénzügyi kontroll elvesztése, vagy a megfelelő számviteli nyilvántartás vezetésének elégtelensége.

A működésfolytonossági terv részletezettsége függ az informatikai osztály méretétől és a számítógépes feldolgozásra való ráutaltságtól.

Az informatikai rendszer kockázat elemzésének egyik szempontja, hogy azonosítsák azon informatikai rendszereket, melyektől a szervezet működése függ, ezek relatív prioritását és azon időtartamot, melyen belül működésüket vissza kell állítani (akár csökkentett hatásfokkal is) annak érdekében, hogy a szervezeti működés ne szenvedjen jelentős kárt. A visszaállítási időtartam több hét és néhány óra között változhat, a szervezeti igényektől függően, illetve nagyon kritikus rendszerek esetében szükséges lehet a folyamatos működés biztosítása egy "tükrözött", vagyis alternatív rendszer segítségével.

A kockázat értékelésen túl, a szervezeti igényekkel összhangban, a folyamatos működtetéshez nagyon fontosak a megfelelő rendszer mentések (backup), egy formális működésfolytonossági terv, egy vezetői keretterv az előbbiek működtetésére, karbantartására és rendszeres időközönként tesztelésére. Egy nem tesztelt működésfolytonossági terv nagy valószínűséggel nem lesz hatékony, továbbá nincs az a működésfolytonossági terv, amely használható lenne, ha a rendszerről nincs biztonsági mentés (backup), illetve egyes katasztrófa típusok előfordulása esetén, ha a mentések nem elérhetőek.

> *A nem megfelelő működésfolytonossági terv növeli a visszaállításhoz szükséges időt a rendszer leállása esetén. Ez befejezetlen, vagy hibás nyilvántartásokhoz vezethet, valamint befolyásolhatja az intézmény működési képességét.*
>
> *A nem megfelelő mentési politikák és eljárások növelik annak kockázatát, hogy a szervezet nem képes megfelelő ellenőrzési nyomvonalat (audit trail) fenntartani.*
>
> *A mentések nem biztonságos tárolása adatvesztéshez, vagy szabálytalan változtatásokhoz vezethet. Megfelelő biztonsági szabályozást kell alkalmazni.*

Hozzáférések szabályozása

Informatikai rendszerek esetében kétféle hozzáférésről beszélhetünk: fizikai és logikai hozzáférésről.

A fizikai hozzáférés kontrollok alatt olyan környezeti kontrollokat értünk, amelyek átfogják az egész IT környezetet, és hatással vannak minden számítógépes alkalmazásra.

Ezeket a kontrollokat arra tervezik, hogy megvédjék a számítógépes hardvert és szoftvert a sérülésektől, lopástól és illetéktelen hozzáféréstől. A hozzáférés kontrollok különböző szinten helyezkedhetnek el, attól kezdve hogy megakadályozhatják a belépést a helyiségekbe, az egyéni kulcsok alkalmazásáig az egyes PC-ken. Az IT rendszerekhez való korlátozott fizikai hozzáférés csökkenti a kockázatát annak, hogy illetéktelen személyek pénzügyi információkat változtatnak meg.

A logikai hozzáférés kontrollok működhetnek mind rendszer, mind alkalmazás szinten. A rendszer szintű kontrollok bizonyos alkalmazásokhoz vagy adatokhoz való hozzáférést hivatottak korlátozni. A logikai és fizikai hozzáférés kontrollokat gyakran együtt is alkalmazzák, ezzel is csökkentve a programok vagy adatok szabálytalan, illetéktelen megváltoztatásának lehetőségét.

> *Hozzáférési politika nélkül nehéz felmérni, hogy a hozzáférés kontroll szabályok megfelelőek-e, mert a politikának kell irányítania a megfelelő kontrollok adaptációját.*
>
> *A hozzáférések szabályozása, a hozzáférési jogosultságok megállapítása, nyilvántartása és karbantartása nélkül nem alakítható ki olyan rendszer, mely megbízható védelmet nyújt az általa kezelt tranzakcióknak és információknak. Ennek hiányában az informatikai rendszer biztonsági kockázata nagyon magas.*

Dokumentációs politika

A dokumentációs politikának kell biztosítania, hogy az informatikai vonatkozású dokumentációk naprakészek és átfogóak legyenek, valamint rendelkezésre álljanak az illetékes alkalmazottak és vezetők részére. Továbbá meg kell határoznia, hogy csak a legfrissebb verziókat használják.

> *A nem megfelelő dokumentációs politika növeli annak kockázatát, hogy nem elfogadott munkamódszerek, eljárási gyakorlatok honosodnak meg az intézmény IT szervezetében, növekednek az IT alkalmazottak által elkövetett hibák, valamint nehézzé válik a rendszerek karbantartása, a változások kezelése. (Pl. a lokális hálózat dokumentációjának hiánya, illetve karbantartásának elmaradása a hiba feltárásának és elhárításának akadálya lehet, a hiba elhárításának időigénye jelentősen megnövekedhet.)*

Belső ellenőrzés szerepe

A belső ellenőrzés tartalmazza többek között a számviteli és a belső irányítási és szabályozási rendszerek minőségének és eredményességének vizsgálatát, értékelését és nyomon követését.

> *Ennek részeként meg kell vizsgálni, hogy át szokta-e tekinteni a szervezet belső ellenőrzése a szervezet számítógépes rendszerét és/vagy a pénzügyi rendszerek működtetését, használatát, biztonságát; azaz az informatikai kontrollokat.*
>
> *Amennyiben meggyőződünk arról, hogy a belső ellenőrzés megállapításaihoz és következtetéseihez kellő bizonyíték áll rendelkezésre, lehetőségünk van a belső ellenőrzés munkájának felhasználására. Lehetséges, hogy ily módon sajátos eredendő és belső kontroll kockázatokat tudunk azonosítani. Az ellenőrzési munka során esetleg arra is szükség lehet, hogy a belső ellenőr jelentésére hivatkozzunk.*

III. Általános informatikai kontrollok felmérése

1. Feladatkörök szétválasztása

Az informatikai rendszerek működtetése során a feladatkörök szétválasztása csökkenti a hibák és visszaélések kockázatát, elősegítik a hibakereséseket és a minőségellenőrzést. Ha a feladatkörök nincsenek eléggé elkülönítve, akkor az egyes számítógépes funkciókat kezelő személyek hibáit vagy visszaéléseit kisebb valószínűséggel lehet észrevenni. A feladatkörök nem megfelelő szétválasztása továbbá megnöveli annak kockázatát, hogy a jelentősebb tudással rendelkező alkalmazottak szabálytalan műveleteket hajtanak végre, majd ennek el is tüntetik a nyomait.

Az egyes feladatköröket úgy kell elkülöníteni, hogy a kritikus folyamatok minden szakaszát más személy hajtsa végre, illetve felügyelje. Például az egyes számítógépes programok változásainak elfogadása csak az alkalmazást használó szervezeti egységek feladata lehet, a programozóké nem. Ennek oka egyrészt az, hogy *nem a programozók a "tulajdonosai" a rendszereknek*, hanem a felhasználó szervezeti egység. Másrészt *nem a programozók felelősek annak eldöntéséért, hogy a programok megfelelnek-e a felhasználói igényeknek*. Hasonló megfontolásból, egyazon programozó szintén nem végezheti el egy program megírását, tesztelését és elfogadását is.

A legtöbb esetben az intézmények a feladatkörök szétválasztását az egyes szervezeti egységek közötti felelősség-megosztással érik el. Ez a fajta megosztás az egyes alkalmazottak vagy csoportok között jelentősen csökkenti annak valószínűségét, hogy hibák, vagy szabálytalan műveletek kerülnek a rendszerbe; ugyanis ily módon az egyik csoport vagy személy gyakorlatilag a másik munkáját ellenőrzi.

A feladatkörök szétválasztásának mértékét két tényező befolyásolja:

- a szervezet mérete, valamint
- a szolgáltatásokkal és tevékenységekkel összefüggő kockázatok.

Egy nagyobb szervezet rugalmasabban szét tudja osztani kulcsfontosságú feladatait az alkalmazottai között mint egy kisebb, melynél néhány alkalmazott látja el az informatikai tevékenységeket. Ezért a folyamatok megfelelő kontrollja érdekében ezek a kisebb szervezetek sokkal inkább rá vannak utalva a felügyeleti, felülvizsgálati tevékenységekre, mintegy kompenzálandó a feladatköri szétválasztás lehetőségének hiányát.

Célszerű viszont a szétválasztás mértékét növelni olyan tevékenységek esetén, amelyek nagy kockázattal bírnak (pl. amelyek keretében nagy összegű tranzakciókat hajtanak végre). Ekkor a tevékenység egyes részfeladatait meg kell osztani, és szigorú felügyelet alatt kell tartani.

A számítógépes működés jellegéből adódóan a feladatkörök szétválasztása egymagában még nem biztosítja azt, hogy az alkalmazottak csak jóváhagyott, szabályos műveleteket végezzenek. Annak érdekében, hogy megelőzhessék és felfedhessék a szabálytalan vagy hibás tevékenységeket, hatékony vezetői felügyeletre és formális működési eljárásokra is szükség van.

A feladatkörök szétválasztása vizsgálatának legfontosabb területei a működtetési (operátori), üzemeltetési és programozási tevékenységek - beleértve ebbe a felhasználói, alkalmazásfejlesztői és adatközponti feladatokat. Meg kell vizsgálni, hogy a vezetés megalkotta-e azon politikákat, melyek behatárolják ezen csoportok vagy alkalmazottak felelősségi köreit, ez a politika mennyire dokumentált, mennyire ismert és mennyire érvényesítik a szervezetben.

Annak érdekében, hogy az ellenőr megállapíthassa, a feladatköröket megfelelően szétválasztották-e, valamint az alkalmazottak tevékenysége megfelelő kontroll alatt áll-e, az alábbi területeket kell megvizsgálni:

1. Az egymással össze nem egyeztethető feladatok szétválasztása, és az erre vonatkozó politikák megalkotása.

2. Megfelelő hozzáférés kontrollok kialakítása a feladatkörök szétválasztásának biztosításához.

3. Az alkalmazottak tevékenységének felügyelete megfelelő formális eljárásokon keresztül.

Bizonyítékokat a feladatkörök szétválasztásáról a következő módokon szerezhetünk:

- interjú a vezetéssel és az IT személyzettel
- szervezeti ábrából, melyből nyomon követhető, hogy ki, kinek tartozik jelentési kötelezettséggel
- munkaköri leírásokból.

1.1. Politikák meghatározása, feladatok szétválasztása

A feladatkörök szétválasztásának vizsgálatához első lépésként át kell tekintenünk a szervezet működését, azonosítani kell az összeférhetetlen tevékenységeket, és ezeket hozzá kell rendelni az egyes szervezeti egységekhez vagy személyekhez. A munkafolyamatokat általánosan tekintve alapvetően a következő feladatokat kell elkülöníteni: engedélyezés, végrehajtás, rögzítés és a tranzakciók felügyelete.

A feladatkörök hatékony és megfelelő szétválasztása érdekében a vezetésnek célszerű megalkotni az erre vonatkozó szervezeti politikát. A politika célja, hogy egységes

iránymutatást adjon az alsóbb szintű kontrollok, a szervezeti felépítés és az egyes munkakörök kialakításához. A szervezeti politika másrészt segít megbizonyosodni arról, hogy a vezetés tisztában van a feladatkörök szétválasztásának szükségességével, és így csökkentheti a kontroll kockázatot. Az alábbiakban megemlítünk néhány követelményt, amelyet a politikában célszerű megfogalmazni:

- A felhasználók ne férhessenek hozzá az operációs rendszerekhez és az alkalmazások kódjaihoz.

- A programozók nem lehetnek felelősek a programok élő környezetbe ültetéséért, és nem is férhetnek hozzá az élő programokhoz és adatbázisokhoz.

- Az operációs rendszer dokumentációihoz csak a jogosult rendszer-programozók, rendszergazdák férhetnek hozzá.

- Az alkalmazói szoftverek rendszer-dokumentációihoz csak a jogosult fejlesztők férhetnek hozzá.

- Csakis a felhasználók, és nem az IT személyzet felelősek a tranzakciók indításáért és javításáért, valamint csak ők kezdeményezhetnek változtatásokat az alkalmazásokban.

A feladatkörök szétválasztásának gyakorlati megvalósításáról - első megközelítésben - a szervezeti felépítés alapján kaphat információt az ellenőr. Ha rendelkezésre áll formális szervezeti ábra, amelyen az is be van jelölve, hogy ki kinek tartozik jelentési kötelezettséggel, az biztosíthatja, hogy a személyzet tisztában legyen saját és mások korlátaival, felelősségével. Ez csökkenti annak kockázatát, hogy egyes dolgozók - szándékosan vagy véletlenül - észrevétlenül (nyom nélkül) hajtsanak végre szabálytalan műveleteket.

A szervezeti felépítés alapján megállapítható, hogy az IT szervezeti egység mennyire különül el a felhasználói csoportoktól. Ez az elkülönülés a pénzügyi funkcióktól a legfontosabb mind szervezeti egység mind vezetési tekintetben. Az IT funkciók és a felhasználók elkülönítése csökkenti a visszaélések és hibák kockázatát, azaz csökkenti annak lehetőségét, hogy a felhasználók szabálytalan módon változtatják meg az adatokat vagy szoftvereket. Az olyan alkalmazottaknak, melyek mind IT, mind pénzügyi feladatokkal foglalkoznak, nagyobb lehetőségük van olyan visszaéléseket elkövetni, amelyeket nehéz feltárni.

Az egymással össze nem egyeztethető feladatkörök szervezetenként változóak lehetnek, de az alábbi tevékenységeket - lehetőség szerint - általában külön személyeknek célszerű ellátnia:

> **IT vezetés:** azon személyek, akik az informatikai szervezeti egység tevékenységét és dolgozóit irányítják, meghatározzák.

Rendszertervezés: feladata hogy megértse és meghatározza a felhasználói információs igényeket, ezeket "lefordítsa" és dokumentálja a követelmény specifikációban, amely a rendszerek kialakításának alapja lesz.

Alkalmazások fejlesztése: feladatai közé tartozik bizonyos alkalmazói programok fejlesztése és karbantartása, mint pl. bérszámfejtés, leltár, főkönyvi rendszer.

Rendszerprogramozás: feladatai közé tartozik a rendszer-szoftvert alkotó programok fejlesztése és karbantartása, mint pl. operációs rendszer, rendszerszolgáltatások, fordító programok, biztonsági szoftverek, stb.

Minőségbiztosítás / tesztelés: feladatai közé tartozik hogy áttekintse és tesztelje az újonnan fejlesztett rendszereket és módosításokat, megállapítsa hogy ezek a felhasználói igényeknek megfelelően működnek-e, illetve hogy a funkcionális specifikációval összhangban teljesítenek-e. A tesztelés során meg kell állapítania, hogy kifejlesztették-e a megfelelő eljárásokat, kontrollokat és dokumentációt, és csak ezek után engedélyezhető a rendszer vagy változtatás működő környezetbe helyezése.

Változáskezelés: feladata a változáskezelési eljárások felügyelete, karbantartása, közreműködik a változtatás okának és tárgyának meghatározásában, a kockázatok felmérésében, az engedélyeztetésében, üzembe helyezésében, a változtatás sikerességének ellenőrzésében, valamint mindezen tevékenységek dokumentálásában és iktatásában.

IT support - üzemeltetés: feladatai közé tartozik az intézmény informatikai rendszereinek vagy egyes alrendszerek működésének folyamatos biztosítása, ezek felügyelete, a hardver és szoftver változások üzembe állítása, a felhasználói problémák megoldása.

Rutinszerű karbantartás: az informatikai környezet működtetésével kapcsolatos, magas szakképzettséget nem igénylő feladatokat látja el, mint pl. kisebb hardverhibák elhárítása, patroncsere nyomtatókba stb.

Adatrögzítés: feladata a nyomtatványokon beérkező különböző adatok számítógépes rendszerbe való rögzítése.

Rendszerbiztonság: a funkciót betöltő dolgozó felelős a szervezet informatikai biztonsági programjának fejlesztéséért és adminisztrációjáért. Ez magában foglalja a biztonsági politikák, eljárások és útmutatók fejlesztését, valamint a biztonsági előírások tudatosítását és oktatását a dolgozók részére. Foglalkozik még a hozzáférési kontrollokkal és a működésfolytonossági eljárásokkal kapcsolatos feladatokkal.

Adatbázis adminisztráció: feladatai közé tartozik a szervezeten belül használt adatok tervezése és adminisztrációja. Meghatározza, katalogizálja, kontrollálja és koordinálja a szervezet információs szükségleteit. Az adatbázis-adminisztrátor

ennek a feladatnak egy szűkebb értelmezése, aki a szervezet adatbázisainak üzembe állításának és karbantartásának technikai vonatkozásaival foglalkozik.

Hálózat-adminisztráció: felelős a biztonságos és megbízható on-line kommunikációs hálózatok és szolgáltatások karbantartásáért, foglalkozik a felhasználói osztályok hálózattal kapcsolatos igényeivel és problémáival.

Függetlenül attól, hogy milyen feladatköröket és milyen mértékű szétválasztást alakítottak ki a szervezetben, minden alkalmazottnak rendelkeznie kell dokumentált munkaköri leírással. A munkaköri leírás csökkenti annak kockázatát, hogy a dolgozó túllépi saját hatáskörét, és lehetőséget biztosít az ellenőrnek, hogy megvizsgálja, hogy az aktuális tevékenységek megfelelnek-e a leírásnak.

A munkaköri leírásnak meg kell határoznia az adott munkakör feladat és hatásköreit, az ellátásához szükséges képzettsége(ke)t és képessége(ke)t. A szervezet dolgozói számára kötelező informatikai biztonsági követelményeket az informatikai biztonsági szabályzatnak (IBSZ) tartalmaznia kell, de az egyes feladat- és hatáskörök szempontjából kihangsúlyozandó informatikai biztonsági szabályokat a munkaköri leírásban is célszerű rögzíteni. A vezetésnek továbbá gondoskodnia kell arról, hogy az alkalmazottak megismerjék saját munkaköri feladataikat, és ezt számon is lehessen kérni rajtuk.

A feladatkörök szétválasztásának vizsgálatán belül ki kell emelni a pénzügyi, számviteli tevékenységekkel kapcsolatos tranzakció-feldolgozási feladatokat. A tranzakció-feldolgozáshoz kapcsolódó tevékenységek szétválasztása csökkenti annak kockázatát, hogy a pénzügyi, számviteli rendszerekben az alkalmazottak hibás vagy szabálytalan műveleteket, átutalásokat hajtsanak végre anélkül, hogy azt a vezetés felismerné, illetve feltárná. A vizsgálathoz át kell tekinteni a szervezeti ábrát, a felelősségi és hatásköröket, továbbá interjút kell készíteni a személyzettel. A tevékenységek helyszíni megfigyelése szintén segítheti az egymással össze nem egyeztethető munkakörök felfedését.

Kérdések az 1.1. ponthoz:

1.1.1. Van-e az ellenőrzött szervezetnek politikája a feladatkörök szétválasztására?

1.1.2. Van-e az ellenőrzött intézménynek naprakész szervezeti felépítési ábrája?

1.1.3. Elkülönül-e az IT szervezeti egység mind fizikai mind vezetés tekintetében a felhasználóktól, különös tekintettel a pénzügyi funkciókra?

1.1.4. Az alábbi alapvető IT tevékenységeket különböző személyek végzik-e?

a) IT vezetés

b) Rendszertervezés

c) Alkalmazások fejlesztése

d) Rendszerprogramozás

e) Minőségbiztosítás / tesztelés

f) Változáskezelés

g) IT support - üzemeltetés

h) Rutinszerű karbantartás

i) Adatrögzítés

j) Rendszerbiztonság

k) Adatbázis adminisztráció

l) Hálózat-adminisztráció

1.1.5. Rendelkeznek-e az IT alkalmazottak megfelelő munkaköri leírással?

a) Pontosan meghatározza a felelősségi köröket?

b) Mindenki megkapta-e a sajátját?

c) Benne vannak-e az IT biztonsági követelmények?

d) Meghatározzák-e a munkakör betöltéséhez szükséges technikai képzettséget, és képességet?

1.1.6. Vannak-e olyan alkalmazottak, akik olyan tranzakció-feldolgozási feladatokat hajtanak végre, amelyek egymással össze nem egyeztethetőek? Például:

a) Adatbevitel és az adatok helyességének ellenőrzése

b) Adatbevitel és az eredményeknek a bevitellel való összevetése

c) Adatbevitel és felügyeleti, engedélyezési tevékenységek (pl. egyes összeghatárokon felül a visszautasított tranzakciók független áttekintése szükséges a feldolgozási folyamat folytatásához)

1.2. Hozzáférés kontrollok és a kontrollok felügyelete

A feladatkörök szétválasztását támogató politikák és a munkaköri leírások kialakítása után létre kell hozni ezen politikák betartását biztosító kontrollokat is. Ezeket két nagyobb csoportba sorolhatjuk: a hozzáférési kontrollok, valamint a vezetés felügyelete a kontroll technikák hatékonysága felett.

Mind a fizikai, mind a logikai hozzáférés kontrollok egyik fő célja, hogy a feladatkörök szétválasztására vonatkozó szervezeti szabályozásokat biztosítsa. Ezen kontrollok az egyes szervezeti egységek és az egyes személyek munkájához kapcsolódó felelősségi körökhöz kapcsolódnak. Például a logikai hozzáférés kontrollok megakadályozhatják, hogy egy programozó élő alkalmazásokhoz, vagy azok adataihoz férjen hozzá. Hasonló módon a fizikai hozzáférés kontrollok (pl. azonosító-kártya) megakadályozhatják, hogy a felhasználók belépjenek a számítógépközpontba.

A hozzáférés kontrollokról részletesen ld. a fejezet 2. pontját.

A vezetésnek rendszeresen meg kell vizsgálnia, hogy a dolgozók a meghatározott politikák szerint végzik-e munkájukat. Ezen felülvizsgálatok segíthetnek abban, hogy ha a szervezet működése megváltozik, a politikát is aktualizálják ennek megfelelően.

A rendszeres felmérések ki kell hogy terjedjenek a dolgozók teljesítményére is annak érdekében, hogy a vezetés megvizsgálja: a munkaköri leírásban meghatározott célok teljesülnek-e. Rendszeres áttekintés és vizsgálat hiányában a munkaköri leírások irreális vagy nem megfelelő feladatokat és feltételeket támaszthatnak, ami kockázatot jelent a rendszerek megbízható, szabályos működésére nézve. Ilyen esetekben a munkaköri feladat- és hatáskörök egyenkénti, részletes vizsgálatára van szükség.

Gyakorlatilag a vezetésnek azon tevékenységeket kell rendszeresen áttekintenie, melyeket a fizikai és logikai hozzáférés kontrollok nem képesek megfelelően szabályozni. A dokumentált áttekintések segítik a vizsgálat lefolytatatását, tartalmuk alapján az ellenőr csökkentheti az ellenőrzés kockázatát.

Kérdések az 1.2. ponthoz:

1.2.1. Rendszeresen megvizsgálja-e a vezetés a dolgozók munkáját, teljesítményét, hogy megbizonyosodjanak arról, a munkaköri leírásokban megfogalmazott célok teljesülnek-e?

1.2.2. A vezetés áttekinti-e rendszeresen, hogy a feladatkörök szétválasztását célzó kontrollok megfelelően működnek-e?

1.3. Az alkalmazottak tevékenységének felügyelete

Az alkalmazottak tevékenységét a vezetésnek felügyelet alatt kell tartania, ehhez pedig megfelelő formális eljárásokat kell alkalmaznia. Ez különösen fontos a számítógépes üzemeltetésre vonatkozóan. Ha ezen a területen gyenge a felügyelet, a hibák gyakoribb előfordulását idézheti elő, valamint a számítógépek nem rendeltetésszerű használatát vonhatja maga után.

A vezetésnek olyan formális - írásban is lefektetett - utasításokat kell kidolgozni, ami segíti (vezérli) az alkalmazottakat munkájuk szabályszerű végzésében. Az ilyen instrukciók különösen fontosak a számítógépes üzemeltetésre vonatkozóan. Például egy üzemeltetési kézikönyv megmutathatja, hogyan kell elindítani és leállítani a rendszereket, mi a teendő vészhelyzet esetén, valamint felsorolja a tiltott tevékenységeket. Az alkalmazás-specifikus kézikönyvek további instrukciókat adhatnak az üzemeltetőknek az egyes alkalmazásokra vonatkozóan, mint pl. a folyamat alapállapotba hozása, hibaüzenetek kezelése, vagy egy esetleges rendszer leállást követő újraindítási és visszaállítási lépések leírása.

Az alkalmazottak munkájának rendszeres áttekintése és felügyelete biztosíthatja azt, hogy a tevékenységeket az előre meghatározott eljárásoknak megfelelően végezzék, a hibákat megfelelően korrigálják, valamint a számítógépeket csak rendeltetésszerűen használják. A felügyelet egyik fontos eszköze, hogy minden üzemeltetői, rendszergazdai tevékenységet naplózni (log-olni) kell, ami egyben az ellenőrzés nyomvonalaként is szolgál. A felügyeleti tevékenység során a vezetésnek rendszeresen át kell nézni ezeket a log-fájlokat, és meg kell vizsgálni a rendellenességeket.

Különösen figyelni kell az üzemeltető személyzet tevékenységére a rendszerek indításakor, ugyanis egyes kezdeti környezeti paraméterek ilyenkor könnyen átállíthatóak, ami befolyásolhatja a számítógépes biztonságot és rendelkezésre állást is.

Kérdések az 1.3. ponthoz:

1.3.1. Van-e a szervezetnek informatikai üzemeltetési kézikönyve?

1.3.2. Van-e működtetési útmutató az egyes - fontosabb - alkalmazásokra vonatkozóan?

1.3.3. A vezetés felügyeli-e az alkalmazottak tevékenységét, beleértve az IT üzemeltetést is?

1.3.4. Az üzemeltetési, rendszergazdai tevékenységeket naplózzák-e?

1.3.5. A felügyeleti tevékenység során áttekintik-e a log-fájlokat?

1.3.6. A rendszerek indítását felügyelik-e? Ezt csak az arra jogosultak tudják elvégezni?

2. Hozzáférés kontrollok

A hozzáférés kontrollok feladata, hogy megfelelően biztosítsák a számítógépes erőforrások (adat fájlok, alkalmazói programok, és egyéb számítógépes felületek és eszközök) védelmét az illetéktelen módosítások, betekintések, lopás, adatvesztések vagy sérülés ellen. Ezen kontrollok egy része fizikai kontroll, ami pl. azt szabályozza, hogy a számítógépeket egy zárt szobában tartsák, korlátozandó a fizikai hozzáférést. Másik része pedig logikai kontroll, mint pl. azok a biztonsági szoftverek, melyek az érzékeny fájlokhoz való illetéktelen hozzáférést észlelik vagy megakadályozzák. (A fizikai és logikai kontrollok részletes meghatározását ld. később.)

A nem megfelelő hozzáférési kontrollok növelik az informatikai rendszerek sebezhetőségét, azaz növelik az adatokba való illetéktelen betekintések vagy módosítások kockázatát és csökkentik a számítógépen tárolt adatok megbízhatóságát. Az alábbi példák a sebezhetőség lehetséges következményeit mutatják be:

◊ Ha valaki közvetlen hozzáféréssel rendelkezik valamely adatbázishoz, vagy rendszerhez, az szabálytalan változtatásokat is végrehajthat, vagy saját céljai érdekében érzékeny információkhoz juthat hozzá. Például:

- ♦ megváltoztathatja egy utalványozott bizonylaton szereplő címet/számlaszámot és átirányíthatja a kifizetéseket saját magának, vagy
- ♦ megváltoztathatja a leltári adatokat, ezzel tüntetve el egy lopás nyomait, vagy
- ♦ hozzájuthat bizalmas üzleti tranzakciók adataihoz vagy személyes információkhoz.

◊ Ha valaki hozzáféréssel rendelkezik a tranzakciók végrehajtására szolgáló alkalmazói programokhoz, az:

- ♦ szabálytalan módosításokat hajthat végre a programokban, vagy
- ♦ rosszindulatú programokat telepíthet, melyeket felhasználhat az adatfájlokhoz való közvetlen hozzáféréshez, ami a már előbb részletezett következményekkel járhat, vagy
- ♦ lefuttathat szabálytalan/illegális tranzakciókat is, így megváltoztathatja a bérszámfejtési programot úgy, hogy egyes személyeknek a jogosultnál többet utaljon ki.

◊ Ha valaki hozzáféréssel rendelkezik a számítógépes felületekhez és eszközökhöz, az:

- ♦ hozzáférhet azokhoz a terminálokhoz és telekommunikációs eszközökhöz melyeken számítógépes adatokat rögzítenek, vagy

- ♦ hozzáférhet a mágneses adattárolókon vagy a kinyomtatott papíron rögzített bizalmas és érzékeny információkhoz, vagy

- ♦ eltulajdoníthat vagy tönkretehet számítógépes eszközöket, adathordozókat és szoftvereket.

A hozzáférések korlátozásának célja tehát, hogy:

- a felhasználók csak a feladataik ellátásához szükséges hozzáféréssel rendelkezzenek,

- a nagyon érzékeny erőforrásokhoz, mint pl. a biztonsági szoftverek, a lehető legkevesebb ember férhessen hozzá, valamint

- az alkalmazottak ne férhessenek hozzá olyan funkciókhoz, ami már nem tartozik a feladataik közé, vagy túllép felelősségi körükön. (Ez összefügg a feladatkörök szétválasztásának kontrolljával is! ld. előző fejezet)

Ha ezek a célok teljesülnek, akkor az adatok, programok szabálytalan módosításának, és a bizalmas információk nyilvánosságra kerülésének a kockázata anélkül csökkenthető, hogy a felhasználók munkavégzését korlátozná. Ugyanakkor tudni kell, hogy ha egyensúlyt akarunk teremteni a felhasználói igények és biztonsági követelmények között, akkor körültekintően elemezni kell a rendelkezésre álló információs erőforrások kritikusságát és érzékenységét, valamint a felhasználók által végrehajtandó feladatokat.

A megfelelő hozzáférés kontrollok megvalósításához először azonosítani kell, hogy az egyes erőforrásoknak milyen szintű és típusú védelemre van szüksége, és kinek szükséges hozzáférni ezen erőforrásokhoz. Ennek alapján el kell végezni az alkalmazói szoftverek biztonsági osztályba sorolását. (*Az ITB 12. sz. ajánlása alapján a következő biztonsági osztályok célszerű meghatározni: alap, fokozott, kiemelt.)* Ezt a feladatot az erőforrások tulajdonosainak[*] kell elvégezni. Például egy pénzügyi rendszert alkalmazó osztály vezetőjének meg kell határoznia, hogy a pénzügyi tranzakciókat feldolgozó és tároló alkalmazások milyen biztonsági osztályba tartoznak, és milyen fajta hozzáférést szükséges biztosítani azon a dolgozóknak, akik végrehajtják, értékelik és dokumentálják a program műveleteit. Hasonlóképpen, a szoftverfejlesztésekért és változtatásokért felelős vezetőnek is meg kell határoznia az irányítása alá tartozó hardver és szoftver erőforrások érzékenységét; a rendszerszervezők és programozók hozzáférési jogosultságát.

[*] Az erőforrás tulajdonosának nevezzük azt a vezetőt, aki felelős az erőforrás által kezelt/tárolt adatokért.

A hozzáférés kontrollok kiértékelése egyben annak értékelése, hogy a vizsgált szervezet milyen minőségben hajtotta végre az alábbi kulcsfontosságú feladatokat:

2.1. Az információs erőforrások osztályozása kritikusságuk és érzékenységük alapján

2.2. Nyilvántartás vezetése az engedélyezett felhasználókról és engedélyezett hozzáféréseikről

2.3. Fizikai és logikai kontrollok létrehozása az illetéktelen hozzáférések megakadályozására vagy észlelésére

2.4. A hozzáférések felügyelete, a biztonsági szabályok megszegésének vizsgálata, és a szükséges korrigáló lépések megtétele

2.1. Az információs erőforrások osztályozása kritikusságuk és érzékenységük alapján

Az erőforrások megfelelő és költség-hatékony védelméhez a tulajdonosoknak először meg kell határozniuk, hogy milyen szintű védelemre van szükség. Tulajdonképpen minden információs erőforrásnak szüksége van valamilyen fokú védelemre, a legkritikusabb erőforrásokhoz pedig a legerősebb védelmi kontrollokat kell hozzárendelni. Azonban a védelmi kontrolloknak vannak beszerzési, üzembe állítási és fenntartási költségei is. Ráadásul ezek a kontrollok még a hatékonyságot is csökkentik, mivel pótlólagos tevékenységeket követelnek meg a dolgozóktól az adat és egyéb erőforrás hozzáféréshez. Ezért a szervezetnek általában törekednie kell arra, hogy a sajátos kockázatok mellett megfelelő szintű védelmet alakítson ki, figyelembe véve ennek költségeit és a védelemből származó előnyöket. (A védelem költségei ugyanis – célszerűen – nem haladhatják meg az elért előnyöket.)

Erőforrások osztályozása és a vonatkozó kritériumok megállapítása

Egy olyan politika, amely osztályozási kategóriákat és az ezekre vonatkozó kritériumokat határoz meg, nagy segítséget nyújthat az erőforrások tulajdonosainak a védelmi szükségletük szerinti osztályozásban. Az osztályozás első lépése az "érzékeny" adatokat feldolgozó vagy kezelő rendszerek, illetve ezek *tulajdonosainak* meghatározása. Érzékeny adatnak tekintendő minden olyan információ, melynek elvesztése, szabálytalan használata, illetéktelen hozzáférése vagy módosítása hátrányosan befolyásolja a nemzeti érdekeket, a közigazgatási feladatok végrehajtását, sérti a személyes, hivatali és üzleti adatok bizalmasságát.

Feltételezhetően minden nagyobb rendszer tartalmaz érzékeny információkat, amelyeket védeni kell, de a különleges biztonsági kontrolloknak csak néhány, valóban nagy kockázatú vagy fontosabb alkalmazásra kell koncentrálnia.

A legmegfelelőbb kontroll kiválasztásához a szervezetnek ki kell dolgoznia az osztályozási kategóriáikat, amelyek megfelelnek a saját működési és szabályozási környezetüknek mind a bizalmasság, sértetlenség és rendelkezésre állás szempontjából.* Például néhány alkalmazói rendszer/adatbázis esetében kiemelten fontos megvédeni azok bizalmasságát és sértetlenségét is, míg más rendszerek esetében elég lehet csak a sértetlenségre figyelni. Az osztályozásban felhasználhatóak a hierarchikus biztonsági szintek is, mint pl. minimálisan érzékeny, közepesen érzékeny és nagyon érzékeny. Az osztályozás legfontosabb tényezője, hogy az osztályokat pontosan meg kell határozni az eredendő kockázatok alapján.

Az erőforrások osztályozási rendszerének karbantartása

Az erőforrás *tulajdonosoknak* meg kell állapítaniuk, hogy a felelősségük alá tartozó erőforrások mely osztályokba tartoznak. Ez a meghatározás egyenesen következik a kockázatok értékeléséből, amelyen keresztül azonosították a fenyegetettségeket, a sebezhető pontokat és azon lehetséges negatív következményeket, amelyeket a bizalmas adatokba való betekintések vagy kritikus tranzakciókat támogató adatok integritásának sérülése okozhat. Minden erőforrás osztályozást felül kell vizsgálnia és el kell fogadnia az illetékes felsőbb vezetésnek, ezt rögzíteni kell, és rendszeres időközönként meg kell vizsgálni, hogy a jelenlegi helyzetet tükrözi-e.

Kérdések a 2.1. ponthoz:

Erőforrások osztályozása és a vonatkozó kritériumok megállapítása

2.1.1. Létrehozták-e az osztályozási szisztémát és az hozzá tartozó kritérium rendszert, és ezt az erőforrás tulajdonosok tudomására hozták-e?

2.1.2. Az erőforrásokat azok *tulajdonosai* kockázat értékelés alapján osztályozták-e?

2.1.3. Dokumentált-e az osztályozás, és elfogadta-e a felsőbb vezetés?

Az erőforrások osztályozási rendszerének karbantartása

2.1.4. Felülvizsgálják-e rendszeres időközönként az osztályozást?

* Az információ-biztonság három fő alapösszetevője: a **bizalmasság** (csak az ismerhesse, akinek joga van hozzá), a **sértetlenség** (az információ hiteles forrásból származik és eredeti formájában), valamint a **rendelkezésre állás** (az informatikai erőforrások működőképesek, és ott működőképesek, ahol szükség van rájuk).

2.2. Nyilvántartás vezetése az engedélyezett felhasználókról és engedélyezett hozzáféréseikről

A vizsgált szervezetnek politikákat és eljárásokat kell kidolgoznia az információs erőforrásokhoz való hozzáférések engedélyeztetésére, valamint ezen engedélyeztetések dokumentálására. Ezen politikák és eljárások le kell hogy fedjék a mindennapos, rutinszerű műveleteket, a sürgős esetekben történő hozzáféréseket, valamint szervezeten kívüli személyekkel/csoportokkal történő adatmegosztás és elhelyezés kérdéseit.

Az engedélyezett felhasználók meghatározása és hozzáférésük engedélyeztetése

A számítógépes erőforrás *tulajdonosának* meg kell határoznia azon felhasználókat vagy felhasználói osztályokat, amelyek számára közvetlen hozzáférést biztosít a felügyelete alá tartozó erőforrásokhoz.

A tulajdonosnak meg kell határoznia továbbá minden felhasználó és minden erőforrás esetében a hozzáférés természetét és mértékét. Ezt nevezzük felhasználói (user) "profile"-nak. A folyamatot leegyszerűsítheti az ún. "standard profile"-ok alkalmazása, melyek az azonos munkakörben dolgozók (pl. bérszámfejtők) számára határozzák meg a hozzáférési szükségleteket. A felhasználók általában az alábbi hozzáférési jogokkal rendelkezhetnek (egyszerre többel is) az egyes számítógépes erőforrásokhoz:

- Hozzáférés olvasásra, ami azt jelenti, hogy az adatokat vagy szoftvereket megtekintheti és másolhatja.
- Hozzáférés felülírásra, ami azt jelenti, hogy az adatokat vagy szoftvereket megváltoztathatja.
- Hozzáférés törlésre, ami azt jelenti, hogy az adatokat vagy programokat törölheti, ill. eltávolíthatja.
- Hozzáférés összefésülésre, ami azt jelenti, hogy két különböző forrásból származó adatokat kombinálhat.
- Hozzáférés indításra, ami azt jelenti, hogy programokat elindíthat.

A hozzáférés értelmezhető fájl, rekord vagy mező szinten. A fájlok rekordokból épülnek fel, jellemzően egy tétel vagy tranzakció egy rekord. Az egyes rekordok pedig mezőkből állnak, melyek a rekord adatelemeit tartalmazzák.

A hozzáférési jogosultságokat szabványos formában kell dokumentálni, a felsőbb vezetéssel el kell fogadtatni, és el kell juttatni a biztonsági felügyelőhöz.[*] A *tulajdonosoknak* rendszeres időközönként át kell tekinteniük az engedélyezési nyilvántartást, és meg kell vizsgálniuk, hogy az megfelelő helyzetet tükrözi-e.

[*] Biztonsági felügyelőnek azt az alkalmazottat nevezzük, aki - egyebek mellett - a hozzáférési jogosultságok végső engedélyezését és felügyeletét az egész szervezetre átfogóan kezeli. Egy ilyen feladatkör nélkülözhetetlen az intézmény biztonsági rendszerének egységes és konzisztens kialakításához és fenntartásához.

A széleskörű vagy speciális hozzáférési jogosultságokat csak az az illetékes és lehetőleg kis számú alkalmazott kapja meg, akik az informatikai rendszer fenntartását, vagy a sürgős esetek kezelését végzik. Ilyen jogosultságok szükségesek például az operációs rendszer kezeléséhez, illetve ezek birtokában akár a szabályos kontrollok felülírására is lehetőség nyílhat.

Az ilyen speciális jogosultságok állandó vagy ideiglenes jelleggel is kiadhatóak. Azonban minden ilyen hozzáférést el kell fogadtatni a biztonsági felügyelővel, az írásos igazolásokat iktatni kell, továbbá a kiemelten érzékeny fájlok és hozzáférési jogosultságok használatát a vezetésnek gondosan felügyelnie kell.

Az olyan rendszerek esetében, amelyek nyilvános telekommunikációs vonalon keresztül is elérhetőek, egyes felhasználók számára létre lehet hozni ún. "dial-up" hozzáférést is. Ez azt jelenti, hogy ezen felhasználók modem vagy bérelt vonal segítségével egy távoli helyről (pl. otthonról, vagy vidéki irodából) el tudják érni a rendszert. Mivel ez a fajta hozzáférés jelentősen megnöveli az illetéktelen hozzáférés kockázatát, ezért ezt megfelelően korlátozni kell, és mérlegelni kell a kapott előnyöket a kockázatokkal szemben. Ezen "dial-up" hozzáférések kockázatának menedzselését segíti, ha a hozzáférési engedélyeket írásban is rögzítik, és azt a tulajdonosok elfogadják. (A 2.3. alfejezet további kontrollokat mutat be a kockázatok kezelésére, mint pl. a visszahívási eljárásmód, ami biztosítja hogy csak az előre engedélyezett számokról lehessen a rendszert elérni; vagy biztonsági modemek, vagy kártyák használata a jogosult személy hitelességének igazolására.)

Az engedélyezett felhasználók listáját, azok sajátos hozzáférési igényeit és bármilyen változtatást el kell fogadtatni az illetékes vezetéssel, és ezekről az erőforrás tulajdonosnak írásban is tájékoztatnia kell a biztonsági felügyelőt. Az ilyen engedélyezésekre célszerű létrehozni egy formális (írásba foglalt) eljárásmódot, melynek része egy egységes hozzáférés-igénylő űrlap. Ezzel jelentősen csökkenthető a félreértések, változtatások és félrekezelések kockázata. A biztonsági felügyelőnek át kell tekintenie minden új és minden módosítandó hozzáférés-engedélyezést, az esetleges vitatott kérdéseket pedig az engedélyeztetővel kell megbeszélnie. A már elfogadott engedélyeket iktatni kell.

Ugyanilyen fontos a biztonsági felügyelő értesítése abban az esetben, ha egy alkalmazott munkaviszonya megszűnik, vagy valamilyen okból kifolyólag már nem engedélyezett számára az információs erőforrásokhoz való hozzáférés. Célszerű ilyen esetekben, hogy a humánpolitikai osztály küldje ezt az értesítést, de küldheti más osztály is, a lényeg: *a politikában kell pontosan meghatározni ki a felelős az értesítésért*. Ha az elbocsátott alkalmazottaknak megmarad a hozzáférésük a kritikus vagy érzékeny informatikai erőforrásokhoz, igen nagy kárt okozhatnak; különösen azok, akik "zűrös" körülmények között hagyták el a munkahelyet.

A hozzáférési engedélyeket a biztonsági felügyelőnek rendszeresen át kell tekintenie, illetve össze kell hasonlítani a dolgozó aktuális, alkalmazott hozzáféréseivel. A legtöbb hozzáférést kontrolláló szoftver képes az ilyen összehasonlításra: mihez férhet hozzá a

felhasználó és a gyakorlatban milyen hozzáféréseket vesz igénybe. Részletes ellenőrzés esetén szükség lehet a statisztika átvizsgálására is.

A sürgősségi és ideiglenes hozzáférés-engedélyezés kontrollja

Időnként előfordulhatnak olyan esetek, amikor olyan személyeknek kell hozzáférést biztosítani, akik rendszerint nem, vagy csak korlátozottan rendelkeznek hozzáférési jogokkal. Ilyen esetek lehetnek sürgősségi vagy vészhelyzetek, amikor az ideiglenes feladatok ellátásához szükség lehet az érzékeny vagy kritikus erőforrásokhoz való hozzáférésre. Ilyen eset lehet még karbantartási munka vagy sürgős javítás is. Előfordulhat továbbá hogy egy, az intézménnyel szerződésben levő cég számára szükséges - ideiglenesen - többlet hozzáférést biztosítani, pl. rendszerfejlesztéshez, vagy egyéb munkálatokhoz.

Éppen úgy, mint normális esetben, az ideiglenes hozzáférést is el kell fogadtatni, és a vonatkozó engedélyt dokumentálni kell. Az ideiglenes felhasználói azonosítókat és hitelesítő eszközöket is úgy kell megtervezni, hogy azok érvényessége egy meghatározott idő után lejárjon.

Az adatok elhelyezésének és megosztásának meghatározása

A rendszerek – mint erőforrások – *tulajdonosainak* írásban kell szabályozni, hogy a programokat/adatbázisokat mikor, kinek szükséges karbantartani, archiválni vagy törölni.

Az erőforrás tulajdonosainak meg kell határozniuk továbbá, hogy ezen erőforrásokat megosztják-e mással/másokkal, és ha igen, milyen módon. Amikor fájlokat osztanak meg más szervezetekkel, nagyon fontos, hogy:

- az adatok tulajdonosa tisztában legyen az ezzel járó kockázatokkal, és elfogadja ezt a megosztást, továbbá
- az átvevő intézmény tisztában legyen az adatok érzékenységével, és ennek megfelelően védje is azokat.

Ezen feltételek megkövetelik, hogy az érzékeny információk megosztása előtt a felek az így megosztott erőforrások közös használatát *írásban is szabályozzák*.

Kérdések a 2.2. ponthoz:

Az engedélyezett felhasználók meghatározása és hozzáférésük engedélyeztetése

2.2.1. Van-e a szervezetnek eljárásrendje a hozzáférések meghatározására, engedélyezésére, megadására és visszavonására?

2.2.2. A hozzáférés engedélyezések:

a) egységes formában dokumentáltak és karbantartottak?

b) elfogadta a vezetés?

c) továbbítják-e a biztonsági felügyelőnek?

2.2.3. Áttekintik-e rendszeres időközönként a tulajdonosok a hozzáférési engedélyek nyilvántartását, és megvizsgálják-e hogy megfelelő-e még?

2.2.4. Korlátozott-e azon felhasználók száma, akik modemen keresztül elérhetik a rendszert, dokumentáltak-e a hozzáféréshez szükséges igazolások, és elfogadta-e a tulajdonos?

2.2.5. Áttekinti-e a hozzáférés engedélyezéseket a biztonsági felügyelő, és megtárgyalja-e a vitás kérdéseket az erőforrás tulajdonosával?

2.2.6. Automatikusan naplózza-e (log-olja) a rendszer a biztonsági "profile"-ok változtatásait, és áttekinti-e rendszeres időközönként ezt a naplót egy - a biztonsági felügyelőtől független - vezető?

2.2.7. Azonnal értesítik-e a biztonsági felügyelőt dolgozó távozása vagy áthelyezése esetén?

A sürgősségi és ideiglenes hozzáférés-engedélyezés kontrollja

2.2.8. A sürgősségi és ideiglenes hozzáférés engedélyezések:

a) egységes formában dokumentáltak és karbantartottak?

b) elfogadta-e az illetékes vezetés?

c) továbbítják-e a biztonsági felügyelőnek?

d) érvényét veszíti-e automatikusan egy előre meghatározott idő után?

Az adatok elhelyezésének és megosztásának meghatározása

2.2.9. Léteznek-e egységes űrlapok, hogy dokumentálni lehessen az adatfájlok archiválásának, törlésének vagy megosztásának engedélyezését?

2.2.10. Készítettek-e írásos szabályozást az adatok védelme érdekében, mielőtt a szervezet megosztotta adatait vagy programjait más szervezetekkel?

2.3. Fizikai és logikai kontrollok létrehozása az illetéktelen hozzáférések megakadályozására vagy észlelésére

A vizsgált szervezetnek működtetnie kell egy – célszerűen – költség-hatékony módszert az adatfájlok, alkalmazói programok és a hardver-eszközök védelmére: ezt a fizikai és logikai kontrollok kombinációjával érheti el. A fizikai kontroll a számítógépes erőforrásokhoz való fizikai hozzáférés korlátozását jelenti. Ennek leggyakoribb esetei amikor a számítógépek elhelyezésére szolgáló épületbe való bejutást korlátozzák, vagy zárakat szerelnek a terminálokra. Azonban a fizikai kontrollok egymagukban nem biztosíthatják az adatok és programok védelmét. Ezért a fizikai és logikai kontrollok együttes alkalmazása nagyon fontos ahhoz, hogy megőrizhető legyen az érzékeny adatok sértetlensége és bizalmassága. A fizikai és logikai kontrollok kialakításáért és karbantartásáért - az erőforrás tulajdonos által nyújtott engedélyek alapján - végső soron a biztonsági felügyelő a felelős.

A hozzáférés kontrollokat kriptográfiai (titkosítási) eszközökkel is lehet támogatni, amelyek segítségével a tranzakciós vagy tárolt adatok illetéktelen személyek számára érthetetlenek lesznek, és/vagy fenntartható ezek sértetlensége. Manapság a kriptográfiai eszközöket még ritkán használják a közigazgatási intézményekben. Azonban ezek különösen fontosak lehetnek hálózati környezetben, továbbá az elektronikus aláírás igényének megjelenésével párhuzamosan számítani lehet növekvő felhasználásukra. (Az elektronikus aláírás egyrészt hitelesíti az üzeneteket, a feladó személyazonosságát, másrészt biztosítja az adott fájl sértetlenségének megőrzését is.)

A fizikai és logikai kontrollok hatékonyságának kiértékeléséhez szükség lehet mélyebb technikai ismeretekre, különösen nagy, integrált rendszerek esetében, vagy olyan rendszereknél, amelyek telekommunikációs eszközöket is magukban foglalnak. Ezért még a gyakorlottabb IT ellenőröknek is szüksége lehet szakértőre egyes technikai jellegű kérdések esetében.

A. Megfelelő fizikai biztonsági kontrollok kialakítása

A fizikai biztonsági kontrollok a fizikai hozzáférést korlátozzák a számítógépes erőforrásokhoz, és védik a véletlen vagy szándékos rongálástól, eltulajdonítástól. A védendő számítógépes erőforrások közé tartoznak:

- a központi számítógépes egységek
- a rendszereket hűtő berendezések, szünetmentes tápegységek és egyéb működést biztosító hardver eszközök
- a számítógépes terminálok
- személyi számítógépek
- számítógépes adattároló eszközök
- telekommunikációs és hálózati eszközök, felszerelések és vonalak, beleértve az elektromos kapcsolószekrényeket is.

Olyan fizikai védelmet kell kialakítani, amely arányban áll a fizikai sérülések és hozzáférések kockázatával

A fizikai biztonsági kontrollok kiértékeléséhez az ellenőrnek meg kell vizsgálnia, hogy a szervezet:

- azonosította-e minden területét – mint pl. épületek, egyedi szobák vagy felszerelések, fizikai tároló eszközök vagy telekommunikációs vonalak – amelyek érzékenyek a fizikai hozzáférésre, a rongálásra, eltulajdonításra;
- azonosította-e az érzékeny területek minden hozzáférési pontját és lehetséges fenyegetettségeit;
- kialakított-e költség-hatékony biztonsági kontrollt minden fizikai hozzáérési pontra - figyelembe véve minden lényeges fenyegetettséget - az érzékeny területeken.

A hozzáférést azokra az alkalmazottakra kell korlátozni, akiknek ez a munkájuk ellátásához igazoltan szükséges. A vezetésnek rendszeres időközönként át kell tekintenie az érzékeny felületekhez fizikai hozzáférési engedéllyel rendelkező alkalmazottak listáját.

A fizikai biztonsági kontrollok különbözőek lehetnek, de leggyakrabban az alábbiak valamelyikét vagy kombinációját alkalmazzák:

- hagyományos záras, vagy rejtjel-záras ajtók,
- mágneses ajtózárak, melyek elektronikus kártyával nyithatók,
- biometrikus hitelesítés (a biometrikus azonosítást ld. később),
- biztonsági őrök,
- fényképes azonosító,
- a belépő személyek nyilvántartása,
- a mágnesszalagok és egyéb adattároló eszközök tárolóból/raktárból való ki- és bevitelének nyilvántartása és engedélyeztetése,
- elektronikus és vizuális őrző rendszerek,
- az érzékeny épületek körbekerítése,
- betörésvédelmi rendszerek,
- a számítógépes terminálok fizikai lezárása.

Az ellenőrnek fel kell mérnie, hogy az érzékeny felületek védelmi rendszerét ki lehet-e játszani, azaz be tud-e jutni illetéktelen személy azáltal, hogy például:

- megfigyeli mások - engedélyezett felhasználók - belépési kódját,
- megszerezhet védetlenül hagyott kulcsokat (kártyákat),
- átmászik olyan térelválasztón, amely álmennyezet alatt van,
- gipszkarton fal esetén lyukat fúr a falba olyan helyen, amit bútor takar.

A fizikai kontrollokhoz soroljuk még a környezeti kontrollokat is, mint pl. füst érzékelők, tűzjelzők, tűzoltó készülékek és a szünetmentes áramellátást biztosító eszközök. Mivel ezek a kontrollok inkább a váratlan eseményekre vonatkoznak, ezek tárgyalására a működésfolytonossági terv kontrolljai keretében kerül sor.

A fizikai biztonsági kontrollok kiértékeléséhez az ellenőrnek meg kell vizsgálnia a szervezet politikáját és gyakorlatát:

- a hozzáférési jogok (engedélyek) kiadását és visszavonását,
- az ajtókulcsok kiadását,
- a munkaidő alatti és utáni beléptetések kezelését,
- mágnesszalagok és egyéb adattároló eszközök tárolóból/raktárból való ki és bevitelét,
- vészhelyzetek kezelését,
- vészhelyzetek utáni újbóli belépéseket,
- kompenzáló kontrollok kialakítását, ahol a fizikai kontroll alkalmazása nem keresztülvihető (gyakori eset a telekommunikációs vonalak esetében).

A látogatók kontrollja

Egyes esetekben - a szokásosan engedélyezett alkalmazottakon kívül - egyéb személyek számára is hozzáférést kell biztosítani az érzékeny területekhez. Lehetnek ők szervezeten belüli, de más osztályhoz tartozó dolgozók, karbantartó személyzet, a szervezettel szerződésben levő vállalkozó, ritka vagy váratlan vendég. Mindezen "látogatók" hozzáférését kontrollálni kell, és soha nem kaphatnak korlátlan hozzáférést mindenhez. A kontroll eszközei lehetnek:

- előre megbeszélt időpont a találkozásra vagy hozzáférésre (azaz csak egy egyeztetett időpontban férhetnek hozzá az információkhoz),
- személyi azonosítás,
- a recepciós terület ellenőrzése,
- a látogatók nyilvántartása,
- a látogatók kísérete, míg az érzékeny területen tartózkodnak,
- a belépési kódok rendszeres cseréje annak megelőzésére, hogy a már megismert kóddal egy látogató újra bejuthasson.

Megjegyzés: jelen pont ellenőrzési folyamatát célszerű összehangolni a már említett működésfolytonossági terv környezeti kontrolljainak vizsgálatával (ld. III. fejezet 4.2.), mivel számos ellenőrzési cél és technika azonos.

Kérdések a 2.3. pont A. részéhez:

A. Megfelelő fizikai biztonsági kontrollok kialakítása

Olyan fizikai védelmet kell kialakítani, mely arányban áll a fizikai sérülések és hozzáférések kockázatával

2.3.1. Meghatározták-e az érzékeny és kritikus erőforrások tárolására szolgáló épületeket, helységeket, tárolókat?

2.3.2. Meghatározták-e az érzékeny és kritikus erőforrások minden lényeges fenyegetettségét és a hozzájuk tartozó kockázatokat?

2.3.3. Korlátozzák-e a hozzáférés lehetőségét azokra az alkalmazottakra, akiknek ez a munkájuk ellátásához szükséges?

2.3.4. Alkalmaznak-e biztonsági őröket, jelvényes azonosítót, vagy beléptető eszközöket, mint pl. chip-kártya?

2.3.5. Áttekinti-e rendszeres időközönként a vezetés az érzékeny felületekhez fizikai hozzáféréssel rendelkező alkalmazottak listáját?

2.3.6. Szükséges-e kulcs vagy egyéb eszköz a számítógépes termekbe való belépéshez?

2.3.7. Biztonságosan tárolják-e a kiosztásra nem került kulcsokat és egyéb beléptető eszközöket?

2.3.8. Léteznek-e ún. újbóli belépési eljárások, melyek vészhelyzetek után biztosítják, hogy csak az engedélyezett személyek jussanak be az érzékeny területekre? (pl. tűzriadó után)

A látogatók kontrollja

2.3.9. Léteznek-e előírások és biztosítanak-e kíséretet azon esetekre, amikor látogatók érzékeny helyekre – mint pl. a központi számítógép terem – lépnek be.

2.3.10. Megváltoztatják-e rendszeres időközönként a belépési kódokat?

2.3.11. Megtörténik-e a látogatók, szerződéses vállalkozók vagy karbantartók hitelesítése azáltal, hogy csak előre megbeszélt időpontokban engedélyezik a belépésüket/hozzáférésüket, és személyi azonosítást is alkalmaznak?

B. Megfelelő logikai hozzáférés kontrollok kialakítása

A számítógépes szoftverek és adatok a logikai hozzáférés kontrollok alkalmazásával védhetőek meg az illetéktelen hozzáféréstől. A logikai kontrollok a felhasználói azonosító (ID), a jelszó vagy más egyéb azonosító alkalmazásával határozzák meg a felhasználó számára előre megállapított hozzáférési lehetőségeket. A logikai kontrollokat úgy kell megtervezni, hogy a jogosult felhasználók a szükséges időben és mértékben hozzáférhessenek a megfelelő rendszerekhez, programokhoz és adatbázisokhoz, míg más "felhasználóktól" - mint pl. hackerek - teljesen megvédje azt.

A logikai biztonsági kontrollok alkalmazásával a szervezet:

- elkülönülten azonosíthatja a felhasználókat vagy számítógépeket, amelyek engedélyezett hozzáféréssel rendelkeznek a számítógépes hálózatokhoz, adatokhoz és egyéb erőforrásokhoz;
- a hozzáférést korlátozhatja az adatok vagy egyéb erőforrások egy bizonyos részére;

– ellenőrzési nyomvonalat és elemzési lehetőséget biztosít a rendszer és a felhasználók tevékenységére vonatkozóan;
– védekező lépéseket tehet a külső behatolások kivédésére.

A logikai biztonsági kontrollok kiértékeléséhez az ellenőrnek meg kell vizsgálnia, hogy a szervezet:

– tudja-e hatékonyan azonosítani és hitelesíteni a felhasználókat,
– megállapította-e a rendszerek, az érzékeny programok és adatok összes elérési útvonalát, és
– kialakított-e hatékony technikákat a tervezett mértékű hozzáférés-korlátozásra, kézbentartására.

Jelszavak, és egyéb eszközök a felhasználók azonosítására és hitelesítésére

Az azonosítás célja, hogy az egyes felhasználókat meg lehessen különböztetni egymástól. Ezt általában a felhasználói azonosítóval (ID) érik el. (pl. Kovács István azonosítója lehet egy rendszerben : "kovacsi") A felhasználói azonosító azért fontos, mert ehhez rendelik hozzá a felhasználó jogosultságait, és ennek alapján azonosít mindenkit a rendszer. Azonban az azonosító használata egymagában nem biztosít elég védelmet, ezért hitelesítő eljárásokat kell kialakítani - annak biztosítására, hogy a felhasználó valóban az legyen, akinek jelzi magát.

A legszélesebb körben használt hitelesítési eljárás a jelszavak használata. Azonban a jelszó egymagában még szintén nem bír bizonyító erővel, hiszen lehet tippelni, le lehet másolni, kihallgatni, vagy felvenni és visszajátszani. A jelszavak védelme érdekében az alábbi kontrollokat szokás alkalmazni:

– A jelszó kiválasztása kizárólag az adott felhasználó hatásköre.
– A jelszavakat rendszeres időközönként – 30-90 naponként – cserélni kell. Minél érzékenyebb adatokhoz lehet hozzáférni általa, vagy minél érzékenyebb maga a munkakör, annál sűrűbben kell cserélni.
– A jelszót nem írhatja ki a számítógép a bevitel közben. (pl. * jelenik meg minden karakter helyett)
– Egy jelszónak minimum 6 karakternek kell lennie, hogy ne lehessen könnyen kitalálni.
– Nevek, szavak vagy régebbi jelszavak - hat generációig visszamenőleg - használata nem engedhető meg, míg az alfanumerikus* jelszavak használata ajánlott, mert nehezebb kitalálni.
– A rendszer fejlesztője által megadott jelszavakat mint pl. SYSTEM, DEFAULT, USER, DEMO és TEST az új rendszer üzembe állításakor azonnal meg kell változtatni.

* Alfanumerikus karaktersorozat: amikor a karaktersorozat egyaránt tartalmaz betűket és számokat is, pl: ka2vo81

– Célszerű megkülönböztetni az egyéni felhasználókat, és lehetőség szerint el kell kerülni a csoportos azonosítókat és jelszavakat.

A jelszavak kitalálása ellen úgy is lehet védeni a rendszert, hogy csak korlátozott számú érvénytelen próbálkozás lehetséges - általában 3-4 érvénytelen kísérletet szoktak megengedni. Ha ezt kombinálják az alfanumerikus jelszavak használatával, az jelentősen lecsökkenti annak kockázatát, hogy egy illetéktelen felhasználó úgy jut be a rendszerbe, hogy szavak vagy nevek százait próbálgatja, míg hozzáférést nem kap.

Egy másik technika a jelszavak elrejtésére a jelszó-fájl titkosítása. Habár ehhez a jelszó fájlhoz elvileg csak nagyon kevés embernek szabad hozzáférnie, a titkosítás tovább csökkenti annak kockázatát, hogy illetéktelenek elolvashatnák a jelszavakat. (Általában erről a titkosításról – különböző mértékben – a legtöbb rendszer maga is automatikusan gondoskodik.)

A jelszavakon kívül egyéb azonosító eszközök is használatosak, mint pl. azonosító kártyák, belépő kártyák, zsetonok, és kulcsok. Ezen eszközök hatékonysága azon múlik, hogy :

– milyen gyakran ellenőrzik, hogy a felhasználónak megvan-e az azonosítója,
– a felhasználók megértsék, hogy ne engedjék másoknak használni a saját azonosítójukat és jelszavukat, és azonnal jelentsék, ha elveszítenék azt.

Egy ma még kevésbé elterjedt hitelesítési módszer a biometrikán alapul. Ez egy automatikus felismerési és ellenőrzési módszer, amely a személyeket fiziológiai vagy viselkedési jegyek alapján azonosítja. A biometrikus eszközök vizsgálhatják az ujjlenyomatot, retina mintát, a kéz alakját, beszédmintát, vagy akár a kártya-lehúzás dinamikáját. Ha a vizsgálat során ilyen technikákkal találkozik az ellenőr, tekintse át az eszközöket, figyelje meg működésüket, és belátása szerint tegye meg a lépéseket a kiértékeléshez (ebbe beletartozik, hogy akár specialista segítségét is igénybe vegye).

Az elérési (hozzáférési) útvonalak azonosítása

A felhasználók az adatokhoz és szoftverekhez egy vagy több elérési útvonalon keresztül - számítógépes hálózaton, hardveren és szoftveren keresztül - juthatnak. Ezért annak érdekében, hogy megfelelő védelmi rendszert építsen ki a szervezet, azonosítani és kontrollálni kell minden lehetséges elérési útvonalat.

Az ún. "stand-alone", azaz egymagában, más számítógéppel kapcsolatban nem álló számítógépek esete viszonylag egyszerű. Azonban egy hálózatos környezetben körültekintő értékelés szükséges a rendszer érzékeny adataihoz vezető összes belépési pont és elérési útvonal meghatározásához. Egy hálózatos rendszer általában több személyi számítógépből áll, amelyek egymással is és egy nagyobb géppel - ami lehet egy fájl szerver, vagy egy mainframe - vannak összekapcsolva. Ezek között lehetnek olyan gépek is, amelyek telefonvonalon keresztül kapcsolódnak a hálózatba. Ez mind azt eredményezi, hogy a rendszerbe számos ponton be lehet lépni. És ha már valaki bent van a rendszer-

ben, a szoftver programokon keresztül már nagyon sok úton el lehet jutni az érzékeny adat- és program fájlokhoz.

Az internethez kapcsolódás további újabb sebezhető felületeket nyit a szervezet rendszerén, potenciális lehetőséget nyújtva több millió embernek a hozzáféréshez. Már számos eset bizonyította, hogy sok internet használót motivál, hogy megpróbáljanak behatolni rendszerekbe, legtöbbször olyan szoftver segítségével, amely a jelszavak szisztematikus próbálgatásával próbálja a hozzáférést létrehozni.

Az elérési útvonalak azonosítását a szervezetnek a kockázat elemzés részeként célszerű elvégezni, és dokumentálnia kell egy ún. elérési útvonal diagramon. Egy ilyen diagram meghatározza a rendszer felhasználóit; a hozzáféréshez használt eszközök típusait; a hozzáféréshez használt szoftvert; az elérhető erőforrásokat; az alkalmazói rendszereket; valamint a működési módot és a telekommunikációs útvonalakat. Az elérési útvonal diagram célja, hogy segítsen azonosítani azon pontokat, amelyeken keresztül a rendszer adatai elérhetőek, és ahol ezért kontrollokat kell kialakítani. *Külön figyelmet kell szentelni az üzemeltető és programozó alkalmazottak esetleges "kerülőutas" megoldásainak az adatok eléréséhez.* A kockázat elemzés többi területéhez hasonlóan az elérési útvonal diagramot rendszeres időközönként át kell tekinteni, valamint ha a rendszerben vagy a programok működésében vagy az adatfájlok elhelyezkedésében változás következik be, aktualizálni kell.

Ha a lehetséges belépési pontokat és az elérési útvonalakat nem azonosítják, akkor ezeket nem is lehet megfelelően kontrollálni, és így illetéktelen felhasználók a kialakított kontrollok mellett, kiskapukon át elérhetik az érzékeny adatokat, programokat vagy a jelszavakat. Továbbá a vezetésnek sem lesz megfelelő képe a rendszerükben rejlő kockázatokról, és így rossz kockázat kezelési döntéseket hozhatnak. Ha a rendszer komplexitása vagy más rendszerekhez való kapcsolódása miatt minden elérési útvonalat nem lehet azonosítani, akkor a vezetésnek ezt a nem mérhető kockázatot bele kell kalkulálnia a kockázat kezelési döntéseibe.

<u>Az adatfájlokra és a szoftver programokra kialakított logikai kontrollok</u>

Az adatfájlokhoz és szoftver programokhoz való hozzáférés korlátozásának legelterjedtebb módja a hozzáférést kontrolláló szoftverek, vagy más néven a biztonsági szoftverek használata. A hozzáférést kontrolláló szoftverekkel meghatározható, hogy ki férhet hozzá a rendszerhez, kinek van hozzáférési joga bizonyos erőforrásokhoz, és az engedélyezett felhasználók milyen tevékenységeket végezhetnek. Ezeken túl automatikusan biztosítja a biztonságos beléptetést és a hozzáférési tevékenységek nyilvántartását.

Ugyan a legtöbb alkalmazói rendszer tartalmaz beépített biztonsági funkciókat, amelyek megvédik az alkalmazásokat és az adatbázisok egy bizonyos csoportját, mégis ajánlatos a hozzáférést kontrolláló szoftver használata. Egy ilyen biztonsági szoftver képes megvédeni az egész informatikai környezetet azáltal, hogy minden alkalmazást felügyel egy központi operációs rendszer alatt. Ezt a szoftvert úgy célszerű beállítani, hogy kiegészítse a szűkebb területre összpontosító alkalmazói rendszerek biztonsági kontrolljait,

ezáltal a hozzáférést kontrolláló szoftver egy átfogó és összehangolt védelmet képes biztosítani.

Általában a hozzáférést kontrolláló szoftverek több olyan funkcióval rendelkeznek, amelyeket a szervezet igényei szerint - a maximális hatékonyság érdekében - aktiválni vagy inaktiválni szükséges. Ilyen választható funkciók lehetnek:

- mely meghatározott erőforrásokat (adatbázisokat és szoftvereket) érhetnek el az egyes felhasználók;
- milyen hozzáférési jogosultságai lehetnek a felhasználóknak (pl. olvasás, módosítás, törlés, összefűzés, program indítás);
- milyen napokon vagy a napok milyen időszakában hajthatnak végre bizonyos feladatokat a felhasználók;
- jelszó hosszúság (karakterek száma) és szintaxis (pl. csak betűk, számok vagy alfanumerikus is), valamint a jelszó maximális élettartama;
- a megengedett maximális belépési próbálkozások száma;
- a passzív felhasználók hozzáférését egy idő után kell-e korlátozni, vagy a terminált ki kell-e kapcsolni (és ha igen, mennyi idő után);
- ki kell-e védeni az illetéktelen hozzáférést, vagy ha illetéktelen hozzáférést észlel, akkor küldjön egy figyelmeztető üzenetet a felhasználónak és/vagy az erőforrás tulajdonosnak.

Az ellenőr elsődleges feladata, hogy megállapítsa, milyen funkciókat aktiváltak, és ez megfelel-e az erőforrás tulajdonosok által megállapított hozzáférés engedélyezésnek.

Annak érdekében, hogy ezen beállításokat ne lehessen elrontani (akár véletlenül, akár szándékosan):

- a biztonsági beállításokat, táblázatokat meg kell védeni az illetéktelen hozzáféréstől és módosítástól: vagy az elérési útvonal korlátozásával vagy titkosítással;
- magához a hozzáférést kontrolláló szoftverhez való hozzáférést korlátozni kell;
- csak a szükséges, de a lehető legkevesebb ember számára szabad megadni a biztonsági beállítások módosításának jogát;
- a hozzáférési-biztonsági ellenőrzési nyomvonalakat (log-okat), melyek a hozzáférést kontrolláló szoftver használatát dokumentálják, védeni kell az illetéktelen változtatásoktól.

Az ellenőr kezében az ún. „áthatolás tesztelés” , vagy más szóval „legális hack-elés” is egy hatásos eszköz a rendszer biztonságának felmérésére. Egy ilyen teszt során az ellenőr saját eszközeivel (pl. hacker programokkal) próbál behatolni a szervezet rendszerébe. Nyomatékosan felhívjuk azonban a figyelmet, hogy ez a módszer igen nagyfokú informatikai szakértelmet és körültekintést kíván, mivel az eljárás során hálózati ellenőrző rendszerek, adatbázisok, beállítások stb. megsérülhetnek. Az áthatolás tesztelést ezért a végrehajtás előtt lépésről lépésre meg kell tervezni és minden lépés lehetséges hatását elemezni kell. Az áthatolás tesztelés tervét minden esetben egyeztetni kell a vizsgált szervezet informatikai vezetésével; és csak az ő jóváhagyásuk mellett, szigorúan dokumentáltan, ellenőrzési nyomvonal kialakításával lehet végrehajtani!

Az adatbázisokra kialakított logikai kontrollok

Logikai kontroll kialakítható átfogóan egy önálló adatbázisra is, az adatbázis menedzsment rendszeren (DBMS) keresztül. Ez a DBMS szoftver kontrollálja, szervezi és kezeli az adatokat, elérési útvonalakat biztosít az adatbázis adataihoz, valamint menedzseli az integrált adatállományt, amely átfogja a szervezet működési, üzemeltetési és szervezeti kereteit. Például azon alkalmazottak esetében, akik hozzáférhetnek a személyi adatállomány jelentős részéhez, letiltható, hogy betekintsenek a jövedelmi információkba. Az adatszótár szoftver (DD), mely a DBMS-sel együttműködve az adatállomány elemeinek típusát tartja nyilván, szintén lehetőséget adhat az adatok védelmének biztosítására.

Hasonlóan, mint az adatfájlokhoz és szoftverekhez kialakított logikai kontrollok esetében, az ellenőr elsődleges feladata, hogy meghatározza, beállították-e a hozzáférési jogosultságokat, és ez megfelel-e az erőforrás tulajdonosok által megállapított hozzáférés engedélyezésnek. Továbbá a DBMS-t, az adatszótárt és az ezekhez tartozó táblákat is védeni kell az illetéktelen beavatkozástól (változtatástól), ami jelen esetben is a logikai hozzáférés kontrollokkal, titkosítással és az ellenőrzési nyomvonal biztosításával érhető el.

A telekommunikációs hozzáférésre kialakított logikai kontrollok

Számos speciális szoftver és hardver létezik, amellyel külső rendszerek vagy személyek hozzáférése korlátozható a telekommunikációs csatornákon keresztül. Egyik ilyen hálózati eszköz az ún. *tűzfal*, mely a hálózatok közötti hozzáférést kontrollálja, és egyben nagyon fontos eszköz, hogy az internet kapcsolattal összefüggő kockázatokat csökkentse. Másik eszköz lehet az ún. "behatolás-védelmi rendszer" (IDS), amely egy olyan program, ami az operációs rendszerrel működik együtt, és szintén a hozzáféréseket tudja korlátozni. Az ún. biztonsági modem pedig jelszó bekérése után létesít csak kapcsolatot a hálózattal. Használatosak még a hitelkártya méretű chipkártyák is a távoli hozzáférések hitelesítésére: ekkor a kártyában levő mikroprocesszor generálja automatikusan az azonosításhoz szükséges kódsorozatot az elérendő gép számára.

Függően attól, hogy pontosan milyen technikát vagy eszközt alkalmaznak, ezek arra használatosak, hogy:

- ellenőrizzék a terminál azonosítóját, hogy korlátozható legyen a belépés bizonyos terminálokról;
- ellenőrizzék az azonosítót és a jelszót bizonyos alkalmazások eléréséhez;
- kontrollálják a hozzáférést a telekommunikációs rendszerek és a terminálok között;
- az alkalmazások csak megfelelő korlátokkal vehessék igénybe a hálózati szolgáltatásokat/lehetőségeket;
- a feladat végrehajtása után automatikusan megszakítsák a kapcsolatot;
- naplózza (log-olja) a hálózati tevékenységet, amellyel egyben felügyelhető (monitorozható) a hálózat használata és konfigurációja;
- az arra felhatalmazott személyeknek lehetővé tegyék a hálózati komponensek kikapcsolását;

- a telefonos kapcsolaton keresztül történő rendszer-hozzáféréseket monitorozzák: a hívó szám monitorozása vagy a vonal azonnali megszakítása után visszatárcsázás egy addig már engedélyezett számra;
- korlátozzák a házon belüli hozzáférést a kommunikációs szoftverekhez;
- kontrollálják a kommunikációs szoftvereken végrehajtott változtatásokat;
- korlátozzák és monitorozzák a telekommunikációs hardverekhez és felületekhez való hozzáférést.

Hasonlóan a többi hozzáférés kontrollhoz, a hatékonyság érdekében a telekommunikációs kontrollokat is az engedélyezések alapján kell kialakítani. Védeni kell továbbá az illetéktelen változtatások ellen a biztonsági korlátozásokat definiáló listákat és táblázatokat, valamint meg kell védeni a kommunikációs biztonsági szoftvereket a házon belüli hozzáféréstől és módosítástól.

Azon esetekre, amikor valaki telekommunikációs vonalon keresztül kíván a rendszerhez hozzáférni, a technikai kontrollokon túl olyan bejelentkező képernyőt kell kialakítani, ami elriasztja az illetéktelen felhasználókat a bejutási próbálkozásoktól, és világossá teszi számára, hogy az illetéktelen böngészést nem tolerálják. Például a bejelentkező képernyőn jelenjen meg egy figyelmeztető üzenet, hogy a rendszert csak az engedélyezett személyek használhatják, és tevékenységüket figyelik (monitorozzák). Azon telefonszámokat pedig, amelyeken a rendszer elérhető, nem szabad nyilvánosságra hozni, és lehetőség szerint a számokat rendszeres időközönként cserélni kell.

Ahhoz, hogy a telekommunikációs hálózaton keresztüli hozzáférések kockázatát és az erre kiépített kontrollok hatékonyságát ki lehessen értékelni, az ellenőrnek meg kell értenie az intézmény informatikai rendszerét, a hálózati konfigurációt és a kiépített kontroll technikákat. Ez sok esetben speciális szakértő segítségét igényeli.

Kérdések a 2.3. pont B. részéhez:

B. Megfelelő logikai hozzáférés kontrollok kialakítása

Jelszavak és egyéb eszközök a felhasználók azonosítására és hitelesítésére

2.3.12. A felhasználói azonosítók:

a) Egyediek-e minden felhasználó számára?

b) Alkalmaznak-e csoportos azonosítókat?

2.3.13. A jelszavak:

a) A felhasználó választja-e ki és kezeli-e a saját jelszavát?

b) Van-e valamilyen (pl. papír alapú) nyilvántartás a felhasználók jelszavairól?

c) Kikényszeríti-e a rendszer automatikusan a jelszavak rendszeres - 30-90 naponkénti - cseréjét?

d) Kiírja a rendszer a jelszót olvasható formában begépelés közben?

e) Meghatározza-e a rendszer a jelszavak minimális – pl. 6 karakter – hosszát?

f) Tiltott-e a régi jelszó használata legalább 6 generáción keresztül?

2.3.14. Tiltják-e nevek vagy szavak jelszóként való használatát? Ezek ellenőrzését a rendszer automatikusan elvégzi-e?

2.3.15. Lecserélik-e azonnal a szolgáltató által megadott jelszavakat?

2.3.16. Korlátozza-e a rendszer 3-4 sikertelen próbálkozásra a hozzáférési kísérleteket?

2.3.17. Titkosítottak-e a jelszó-fájlok?

2.3.18. Az azonosító eszközök esetében, mint pl. mágnes kártya vagy chip-kártya, kulcsok szabályozott-e, hogy ezeket az eszközöket a dolgozók:

a) nem adhatják kölcsön,

b) nem oszthatják meg másokkal, és

c) elvesztésüket azonnal jelenteniük kell?

Az elérési (hozzáférési) útvonalak azonosítása

2.3.19. Meghatározták és dokumentálták-e az érzékeny adatokhoz és erőforrásokhoz "vezető" lehetséges elérési útvonalakat?

2.3.20. Kiértékelik-e újra a logikai elérési útvonalakat a rendszerváltoztatások után?

Az adatfájlokra és a szoftver programokra kialakított logikai kontrollok

2.3.21. Alkalmaznak-e a hozzáférések korlátozására speciális biztonsági szoftvert?

2.3.22. Kik férhetnek hozzá a biztonsági szoftverhez?

2.3.23. Kijelentkeznek-e a rendszerből automatikusan a terminálok vagy munkaállomások bizonyos tétlenségi idő után? Mennyi idő után?

2.3.24. Kiszűrik-e azon felhasználókat, akiknek jogosultságuk és kvótájuk* van a rendszerhez, de ezt nem használják? Eltávolítják-e ezeket a kvótákat ha már nincs szükség rájuk?

2.3.25. A jogosultságokat annak megfelelően állították-e be a biztonsági szoftverben (ha van ilyen), hogy az minden engedélyezett hozzáférést biztosítson, a nem engedélyezetteket pedig megakadályozza?

Az adatbázisra kialakított logikai kontrollok

2.3.26. Úgy alakították-e ki az adatbázis-kezelő rendszer (DBMS) és az adatszótár (DD) kontrolljait, hogy:

a) korlátozza az adatfájlokhoz való hozzáférést nézet, rekord vagy mező szinten?

b) korlátozza az adatszótárhoz való hozzáférést is?

c) folyamatosan biztosítson ellenőrzési nyomvonalat (log-ot) az adatszótár változásainak nyomon követéséhez?

d) csakis a DBMS és az adatszótár felületein keresztül biztosítson lekérdezési és módosítási lehetőséget az alkalmazói programok számára?

2.3.27. Megfelelően korlátozott-e a DBMS utility-jeinek (rendszer-programjainak) használata?

2.3.28. Kontrollálják-e a DBMS szoftvereihez való hozzáférést és a változtatási jogot?

2.3.29. Megfelelően korlátozott-e az adatszótár biztonsági profile-jaihoz** és a DBMS biztonsági tábláihoz való hozzáférés?

A telekommunikációs hozzáférésre kialakított logikai kontrollok

2.3.30. Aszerint állították-e üzembe a kommunikációs szoftvert hogy:

a) ellenőrizze a terminál azonosítóját, hogy a belépés bizonyos terminálokra korlátozható legyen?

b) bizonyos alkalmazások eléréséhez ellenőrizzék az azonosítót és a jelszót?

---

* Ha egy felhasználó kvótával rendelkezik egy rendszerben az azt jelenti, hogy azonosítás után a rendszer előre meghatározott erőforrásokat (kvótát) biztosít számára.

** A biztonsági profile azon paramétereket tartalmazza, melyek az egyes felhasználók hozzáférési jogosultságait meghatározzák a rendszerben.

c) az alkalmazások csak korlátozottan vehessék igénybe a hálózati rendszerszolgáltatásokat?

d) megvédje az érzékeny információkat az adatátvitelek alatt?

e) automatikusan megszakítsa a kapcsolatot a feladat végrehajtása után?

f) folyamatosan naplózza (log-olja) a hálózati tevékenységet?

g) korlátozza a hozzáférést azokhoz a táblákhoz, melyek a hálózati opciókat, erőforrásokat és az operátor profile-okat definiálják?

h) csak az arra felhatalmazott felhasználók (pl. rendszergazda, hálózati adminisztrátor) kapcsolhatják ki a hálózati komponenseket?

i) monitorozza a telefonos kapcsolaton keresztül történő rendszerhozzáféréseket: a hívó szám azonosítása vagy a vonal azonnali megszakítása után visszatárcsáz egy meghatározott engedélyezett számra?

j) korlátozza és monitorozza a telekommunikációs hardverekhez és szoftverekhez való hozzáférést és módosítást?

2.3.31. Védik-e megfelelően azon telefonszámokat, melyen a rendszer elérhető, és megváltoztatják-e rendszeres időközönként ezeket a számokat?

C. Kriptográfiai eszközök

Számos esetben – különösen a telekommunikációval kapcsolatban – nem lehetséges vagy nem hatékony a hozzáférések korlátozása a már említett fizikai és a logikai kontrollok segítségével. Ezekben az esetekben a kriptográfiával (titkosítással) oldható meg a felhasználók azonosítása és hitelesítése, továbbá segíthet az adatok és programok sértetlenségének és bizalmasságának megőrzésében is. Ez a módszer működik akkor is, amikor ezen adatok vagy programok "benne" vannak a rendszerben, vagy éppen továbbítás alatt állnak egy másik rendszerbe, vagy lemezen, mágnesszalagon, egyéb médián vagy egy külső helyszínen találhatóak.

A kriptografikus eszközök egyik eleme egy algoritmus (egy matematikai formula), a másik pedig a "kulcsok" (speciális bit sorozat) kombinációja, amelyekkel megoldhatók például az alábbiak:

- ◊ Egy üzenet vagy fájl titkosítása oly módon, hogy az, aki nem rendelkezik a visszafejtéshez szükséges titkos kulccsal, nem tudja elolvasni; ezzel biztosítható az üzenet tartalmának bizalmassága.
- ◊ Biztosítja az elektronikus aláírás lehetőségét, amellyel:
  - ♦ megállapítható, történt-e változtatás a fájlban, azaz biztosítja a fájl sértetlenségét;

- ♦ a dokumentumhoz hozzárendelhető egy személy vagy egy csoport kulcsa, amivel biztosítható a dokumentum "aláírójának" (azaz feladójának) hitelessége.

A kriptografikus eszközök igen értékesek az olyan folyamatok esetében, amelyekben "papírmentes" tranzakciók is bonyolódnak, illetve azoknak a felhasználóknak, akik el akarják kerülni a papír alapú dokumentumokat, de biztosítani akarják a sértetlenséget és a hitelességet. Például:

◊ elektronikus kereskedelemben, ahol a megrendeléseket, visszaigazolásokat és számlákat kell kiállítani, elfogadni és továbbítani elektronikus úton,
◊ utazási adminisztráció esetében, ahol az utazási megrendeléseket, voucher-eket kell kiállítani, elfogadni és továbbítani elektronikus úton, vagy
◊ amikor dokumentumokat vagy digitális képeket kell megvédeni, mint pl. elektronikus médián tárolt szerződések, személyi akták.

Kriptográfiai eszköz kialakítható egy bizonyos alkalmazáshoz is, de akár több alkalmazás is használhatja ugyanazt az eszközt az adatai titkosítására vagy aláírásra.

A kriptográfiával kapcsolatban van néhány technikai kérdés, amit nem szabad figyelmen kívül hagyni:

- A kriptográfiai eszközök csak szoftveres eljárások, vagy alkalmaznak hardver alapú elemeket is? (Az összetett eljárások általában nagyobb biztonságot nyújtanak.)
- Milyen erős vagy komplex a titkosításhoz használt titkosítási és aláírási algoritmus?
- Hogyan kezelik és osztják ki a kulcsokat?
- Olyan kriptrográfiai technikát választott-e a szervezet, mely költség-hatékony és megfelel a kitűzött céloknak?

A kriptográfiai eszközök igénybevétele az érzékeny adatok védelme érdekében párhuzamosan nő a számítógépes hálózatok növekvő használatával. Azonban használatuk még nem széleskörűen elterjedt a közigazgatási intézményekben, ezért a témát csak tömören tárgyaltuk.

Kérdések a 2.3. pont C. részéhez:

C. Kriptográfiai eszközök

2.3.32. Alkalmaznak-e kriptográfiai eszközöket az érzékeny és kritikus adatok, programok integritásának és bizalmasságának megőrzésére?

D. Az eszközök és adathordozók törlése (sterilizálása) értékesítés és újrahasznosítás előtt

A szervezetnek rendelkeznie kell olyan eljárásmenettel, amely a számítógépekről vagy bármilyen egyéb adathordozó eszközről letöröl minden *érzékeny* információt és szoftvert, mielőtt azt javításra küldenék külső szervizbe, selejteznék, értékesítenék, vagy más területre adnák át hasznosításra. Ha az érzékeny információt nem teljes körűen törlik le,

akkor esetleg az információk visszaállíthatóak és hozzáférhetőek illetéktelen személyek számára, akik az eladás vagy újrahasznosítás után jutnak hozzá az eszközökhöz.

Az információk letörléséért a szervezetnek egyértelműen ki kell jelölnie a felelőst. Továbbá egységes űrlapot és nyilvántartást célszerű alkalmazni annak dokumentálására, hogy minden leselejtezett tételt - érzékeny információ szempontjából - átvizsgáltak, és ezen információkat kibocsátás előtt teljesen letörölték.

A külső szervizből visszahozott adathordozó eszközt meg kell vizsgálni, abból a szempontból, hogy nem tartalmaz idegen szoftvert vagy egyéb fájlt (pl. vírust).

Kérdések a 2.3. pont D. részéhez:

D. Az eszközök és adathordozók törlése (sterilizálása) értékesítés és újrahasznosítás előtt

2.3.33. Alkalmaznak-e megfelelő eljárásmódot az érzékeny adatok és szoftverek letörlésére a leselejtezett, eladott vagy áthelyezett gépek, adathordozó médiák esetében?

2.4. A hozzáférések felügyelete, a biztonsági szabályok megszegésének vizsgálata, és a szükséges korrigáló lépések megtétele

Ahogyan már a 2.3. pontban említettük, a biztonsági szoftverek a legtöbb esetben képesek meghatározni a feldolgozási műveletek - vagy megkísérelt műveletek - kiindulópontját, és felügyelik (monitorozzák) a felhasználók tevékenységét: azaz egy megfelelő ellenőrzési nyomvonalat képesek biztosítani. Azonban a megfelelő hatékonyság eléréséhez:

- ezt a funkciót mindenképpen aktiválni kell, hogy biztosítsa a kritikus ellenőrzési nyomvonalat, és jelezze az illetéktelen vagy szokatlan tevékenységeket, valamint
- a vezetésnek ezeket a jelentéseket meg kell vizsgálnia, és a szükséges lépéseket meg kell tennie.

Az ellenőrzési nyomvonal folyamatos biztosítása

A biztonságos hozzáféréssel kapcsolatos ellenőrzési nyomvonal folyamatos biztosításához célszerű hozzáférést kontrolláló szoftvereket használni, amelyekkel megállapítható, hogy ki, mikor és hogyan hajtott végre bizonyos műveleteket. Ez az információ kiemelten fontos olyan esetekben amikor a kontrollok megfelelőségét kell vizsgálni a biztonsági politika alapján, illetve amikor biztonsági szabályok megszegésének vizsgálata folyik.

A hozzáférést kontrolláló szoftver beállítása egyben meghatározza az ellenőrzési nyomvonal (log file) által nyújtott információ jellegét és terjedelmét is. Az ellenőrzési nyomvonalak általában a felhasználói azonosítót, az elért erőforrást, dátumot, időt, a terminál

azonosítóját, és az egyes módosított adatokat tartalmazzák. A biztosított ellenőrzési nyomvonal annyira lehet teljes és értékes, amilyen mértékben a szervezet képes a napló (log file) alapján azonosítani a kritikus folyamatait és az ezekhez tartozó szükséges információkat.

Az ellenőrzés nyomvonal kialakítását és fenntartását a következő szempontok figyelembevételével kell végezni:

- az adatok és egyéb erőforrások értéke és érzékenysége;
- a működési környezet, pl. rendszerfejlesztés, tesztelés vagy gyártás;
- technikai megvalósíthatóság;
- jogi és szabályozási követelmények.

Az aktuális vagy megkísérelt illetéktelen, szokatlan vagy érzékeny hozzáférések felügyelete (monitorozása)

Mivel a részletes, minden műveletet rögzítő ellenőrzési nyomvonal által nyújtott információ általában nagyon terjedelmes ahhoz, hogy azt rendszeres időközönként részletesen át lehessen vizsgálni, ezért célszerű olyan biztonsági szoftvert üzembe helyezni, mely szelektíven képes azonosítani az illetéktelen, a szokatlan és az érzékeny hozzáférési tevékenységeket. A hatékony felügyelethez az alábbiak felismerése szükséges:

- illetéktelen hozzáférési kísérlet;
- hozzáférési trendek megállapítása, és jelzés, ha eltérés mutatkozik a trendtől;
- hozzáférés az érzékeny adatokhoz és erőforrásokhoz;
- kiemelten érzékeny, privilegizált hozzáférés, mint pl. a biztonsági kontrollok megváltoztatása;
- a hozzáférési jogosultságok megváltoztatása;
- a rendszerhez való sikertelen hozzáférési kísérletek száma.

A biztonsági szoftvert úgy célszerű beállítani, hogy jelezze ezeket a műveleteket, és egyes esetekben tegyen is ellenük lépéseket, amelyek az alábbiak lehetnek:

- jelszó letiltása;
- többszöri sikertelen hozzáférési kísérlet után megtiltja az érzékeny erőforrások elérését;
- műveletek, feldolgozások félbeszakítása;
- terminál kikapcsolása;
- figyelmeztető- vagy hibaüzenet megjelenítése;
- olyan feljegyzést ír az ellenőrzési nyomvonalba, amit normális esetben nem tesz.

A gyanús hozzáférések vizsgálata és megfelelő lépések megtétele

Ha a biztonsági felügyelő vagy más felügyeleti tevékenységet végző dolgozó (pl. informatikai vezető, rendszergazda) illetéktelen vagy szokatlan hozzáférési tevékenységet észlel, akkor azt azonnal át kell tekinteni, és a feltárt vagy feltételezett szabálysértést ki kell vizsgálni. Ha bebizonyosodott, hogy a biztonsági szabályokat megsértették, akkor:

- meg kell tenni a megfelelő lépéseket a gyenge kontrollok – amelyek ezt megengedték – azonosítására és kijavítására,
- ki kell javítani továbbá az okozott károkat, és
- ha szükséges, az azonosított elkövetővel szemben meg kell indítani a fegyelmi eljárást.

Nagyon fontos, hogy a szervezetnél alakítsanak ki egy eljárásrendet a biztonsági szabályok megsértésének eseteire (vagy a gyanús esetekre), amelynek információs központja a biztonsági felügyelő legyen. Ezáltal a több helyen előforduló, egymáshoz hasonló eseteket jól meg lehet határozni, továbbá az összesítések felhívhatják a figyelmet a potenciális fenyegetettségekre. Ilyen esetek lehetnek pl. egyazon hacker-től induló, de több helyen végrehajtott "támadás" (behatolási kísérlet), vagy egyazon vírus ismételt "fertőzése".

Gyors és megfelelő válaszlépések nélkül a biztonsági incidensek, illetéktelen behatolások akár felmérhetetlen károkat is okozhatnak a szervezet erőforrásaiban. A gyors reagálás hiánya sokszor bátorítja is a "támadókat".

A szervezetnek rendelkeznie kell dokumentált eljárásrenddel a biztonsági szabályok megsértésére. Ennek az alábbi eljárásokat, illetve ezek kritériumait kell tartalmaznia:

- szabálysértések dokumentálása, mibenlétének meghatározása,
- a szabálysértés komolyságának/súlyosságának meghatározása,
- a szabálysértés jelentése az illetékes felsőbb vezetésnek,
- a szabálysértés kivizsgálása,
- bizonyos szabálysértések esetén fegyelmi intézkedések tétele,
- az erőforrás tulajdonosának értesítése a szabálysértésről,
- jogsértés esetén feljelentés.

Ezen túl a biztonsági szabályok megszegéséről, rendszerességéről, nagyságrendjéről, a megtett orvosló intézkedésekről rendszeres időközönként, összegző formában tájékoztatni kell a felső vezetést. Az ilyen jelentések segítik a vezetést a kockázatok átfogó menedzselésében azáltal, hogy azonosítják a kiemelt szabálysértési célokat, trendeket, bemutatják a szervezet működtetésének biztonsági költségvonzatát és a szükséges pótlólagos kontrollokat.

Kérdések a 2.4. ponthoz:

Az ellenőrzési nyomvonal folyamatos biztosítása

2.4.1. Naplóznak-e (log-olnak-e) minden olyan tevékenységet, amely az érzékeny vagy kritikus rendszerekhez való hozzáféréssel, vagy módosítással jár?

Az aktuális vagy megkísérelt illetéktelen, szokatlan vagy érzékeny hozzáférések felügyelete (monitorozása)

2.4.2. Jelentik-e a biztonsági felügyelőnek, és kivizsgálják-e a biztonsági szabályok megszegését, a sikertelen bejelentkezési kísérleteket, egyéb sikertelen hozzáférési kísérleteket, és az érzékeny tevékenységeket?

A gyanús hozzáférések vizsgálata és megfelelő lépések megtétele

2.4.3. Létezik-e dokumentált eljárásrend a biztonsági szabályok megsértésének eseteire?

2.4.4. Vizsgálja-e rendszeresen a biztonsági felügyelő a biztonsági szabályok megszegését, és jelenti-e a vizsgálat eredményét az illetékes vezetésnek?

2.4.5. Tájékoztatják-e rendszeresen a felső vezetést egy megfelelő összefoglalóban a biztonsági szabályszegésekről?

2.4.6. Módosítják-e a hozzáférési kontrollokat és technikákat, ha a szabálysértések és a vonatkozó kockázat értékelés eredményeképpen ez célszerű?

3. Konfiguráció- és változáskezelés

3.1. Konfiguráció-kezelés

A konfiguráció-kezelés a változáskezeléshez szorosan kapcsolódó terület, és gyakori, hogy a változáskezelésért felelős személy egyben felelős a konfiguráció-kezelésért is. Célja, hogy kontrolláljon minden, az informatikai rendszert felépítő komponenst (vagy másképpen "konfigurációs elemet"). Ebbe beletartoznak a számítógépes hardverek, az adatkommunikációs eszközök és hálózatok, a számítógépes szoftver és az informatikai rendszer dokumentációi (specifikációk, tervek, kézikönyvek, stb.).

A konfiguráció-kezelés négy feladatot fog át:

- **Azonosítás:** a konfigurációs elemek teljes körű meghatározása, azonosítása és nyilvántartása.

- **Beszámolás az állapotokról:** az egyes konfigurációs elemek aktuális státusának nyilvántartása (fejlesztés alatt, tesztelés alatt, archiválva, élő használatban stb.), valamint a minden előző állapotot tartalmazó nyilvántartás karbantartása - azaz ellenőrzési nyomvonal biztosítása.

- **Kontrollálás:** megfelelő kontroll rendszer működtetése annak érdekében, hogy a konfigurációs elemek megtartsák állapotukat, és változtatásokat kizárólag az illetékes hozzájárulásával hajthassanak végre.

- **Ellenőrzés** ("konfigurációs audit"-nak is nevezik): a konfiguráció-kezelésért felelős személy nyilvántartásának - arról hogy minek kell használatban lennie –, és az aktuálisan használatban levő elemek *rendszeres* összevetése. Ennek egy példája, amikor összehasonlítják az élő használatban levő szoftvereket a konfiguráció-kezelés szoftver modulokról szóló nyilvántartásával, megvizsgálva a verzió- és gyártási számokat, valamint a fájl méreteket. Az ilyen ellenőrzés célja, hogy felfedjék a szabálytalan szoftvereket, vagy azokat a szoftvereket, melyeket szabálytalanul, illetéktelenül változtattak meg. Hasonló teszteket kell rendszeresen végrehajtani a konfigurációs elemek további csoportjaira is.

A konfiguráció-kezelési nyilvántartást átfogóan kell vezetni a szervezet egészére vonatkozóan. A megfelelő nyilvántartás érdekében célszerű rögzíteni a konfigurációs elemek alább felsorolt alapvető információit, és az elemek között fennálló kapcsolatokat és függőségeket:
- tétel hivatkozási száma;
- meghatározása, leírása;
- a modell vagy verzió száma;
- üzembehelyezés ideje;
- elhelyezkedése;

- tulajdonosa;
- változási története.

A konfigurációs nyilvántartást kielégítően biztosíthatja egy leltári rendszer is, ha annak alapján egyértelműen azonosítható, hogy milyen hardvereken milyen szoftvereket alkalmaznak. Azonban a nyilvántartás hatékonyabb, ha erre a célra egy speciális adatbázist, illetve szoftvert alkalmaznak a fentebb bemutatott tartalommal.

A megfelelő konfiguráció-kezelés további alapfeltétele, hogy a konfigurációs elemekben, rendszerekben létrehozott változtatásokat *azonnal* bevezessék a nyilvántartásba, és ha lehet, a változási történet alatt megjelöljék az alábbiakat:
- a változás meghatározása, leírása;
- a változás kérelmezője;
- a változás engedélyezője;
- a változás megvalósítója;
- az üzembe helyezés ideje.

Ha a szervezet a változáskezelési folyamatai során ún. "változtatási kérelmet" is alkalmaz (ld. 3.2. pont), akkor a fenti felsorolás első három pontja a kérelem dokumentációjának azonosítójával is helyettesíthető.

A konfiguráció-kezelés előnye, hogy segíti a működésfolytonossági terv (részletesen ld. III fejezet 4.) gyakorlati megvalósítását is. Abban az esetben ugyanis, ha bármely informatikai rendszert egy katasztrófa után újból üzembe kell állítani, szükség lesz annak ismeretére, hogy az milyen komponensekből állt össze és ezek hogyan kapcsolódtak egymáshoz. Egy átfogó konfiguráció-kezelési adatbázis meg tudja adni ezen információkat. Ezért a különböző adat- és szoftver biztonsági mentések, címlisták stb. mellett (ld. 4. fejezet) erről is kell egy naprakész másolatot tartani egy külső helyszínen[*].

A konfiguráció-kezelés nem igényel teljes munkaidős állást, illetve ez csak ritkán fordul elő. Ez inkább vezetői feladatkör, a gyakorlatban egyéb felelősségi körökkel együtt létezik. Az ellenőrnek ebből a szempontból meg kell vizsgálnia a feladatkörök megfelelő szétválasztását is (ld. az 1. fejezet). Ennek oka, hogy a konfiguráció-kezelésért felelős dolgozó hozzáféréssel rendelkezik a szoftverekhez, ezek dokumentációihoz, valamint megvannak az eszközei a megváltoztatott szoftverek élő környezetbe ültetésének előterjesztéséhez. Ez a feladatkör ezért nem delegálható alkalmazások fejlesztésével vagy a karbantartással (is) foglalkozó alkalmazottakhoz, akiknek megvannak a szükséges eszközeik és képességeik a változtatások végrehajtásához is.

[*] Külső helyszín: olyan épület, mely különállóan helyezkedik el a nyilvántartásban szereplő rendszerek épületeitől. Ez azért fontos, hogy egy tűzvész, vagy egyéb komolyabb katasztrófa hatása ne befolyásolhassa a nyilvántartás hozzáférhetőségét, és így a gyors és pontos helyreállítást.

Kérdések a 3.1. ponthoz:

3.1.1. Van-e a szervezetben konfiguráció-kezelésért felelős személy?

3.1.2. Rendelkezik-e a szervezet olyan egységes nyilvántartással, melynek alapján pontosan meghatározhatóak a használatban levő konfigurációs elemek (hardver, szoftver, dokumentáció, adatkommunikációs eszközök és hálózatok) az egész szervezetre vonatkozóan?

3.1.3. Milyen típusú információkat tartanak nyilván az egyes konfigurációs elemekről? (Pl. tétel hivatkozási száma, leírása, verzió/modell, üzembe helyezés ideje, elhelyezkedése, tulajdonosa, változási története)

3.1.4. Pontosan meghatározható-e a nyilvántartás alapján a konfigurációs elemek közötti kapcsolat és függőség?

3.1.5. Hogyan biztosítják, hogy a konfigurációs elemeken végrehajtott frissítések és változtatások azonnal megjelenjenek a konfiguráció-kezelési nyilvántartásban?

3.1.6. Védett-e a konfigurációs nyilvántartás illetéktelen hozzáférésektől és változtatástól?

3.1.7. Megtörténik-e rendszeresen a konfigurációs nyilvántartás helyességének ellenőrzése, azaz összevetik-e rendszeresen a nyilvántartás adatait a ténylegesen alkalmazott elemekkel?

3.1.8. Készítenek-e biztonsági mentéseket a konfigurációs nyilvántartásról, és hol tartják ezeket a mentéseket?

3.2. Változáskezelés

Minden informatikai rendszer életének bizonyos szakaszaiban változásokon megy át. Ennek okai lehetnek például:

◊ Egy alkalmazás új verziójának bevezetése a korábbi verzió hibáinak kijavítása, jogszabályváltozás, vagy új szolgáltatások kialakítása miatt.

◊ A hálózatba új munkaállomásokat kapcsolnak be, és növelni kell a kapacitásokat az igényekhez.

◊ Az egyik szoftver hibája miatt jelentős mértékben megrongálódik az adatbázis, és közvetlen adatszerkesztéssel kell megoldani a problémát.

◊ A számítógépes terem légkondicionáló berendezését egy korszerűbbel helyettesítik.

Nagyon fontos, hogy a változtatások kezelése körültekintő és szabályozott legyen, mert a *gyakorlat azt mutatja, hogy napjainkban az informatikai szolgáltatások minőségi problémáinak jelentős része visszavezethető az IT rendszer valamely részének megváltoztatására.* A változások, változtatások során a szervezeteknek legtöbbször olyan adottságokkal kell szembenézniük, amelyek esetén csak a megfelelő eljárások biztosíthatják a rendszerek folyamatos, megbízható működését. Például:

◊ A szoftverváltoztatásokat legtöbbször olyan személyek végzik, akik nem tagjai az eredeti rendszert fejlesztő csoportnak, és így valószínűleg nem eléggé tájékozottak ennek tervezésében.

◊ A modern, egymással összekapcsolt rendszerek komplexitása már olyan méreteket ölt, hogy egy komponens megváltoztatása egyéb rendszerekben is nem várt változásokat eredményezhet.

A rosszul kezelt, vagy nem kezelt változtatások az alábbi kockázatokat növelik:

- **Üzemzavar a rendszerben:** annak következménye, ha rendszerváltoztatás esetén nem szentelnek figyelmet a hatáselemzésre, a specifikációra, tervezésre és tesztelésre. Lehetséges következményként hibás pénzügyi adatok fordulhatnak elő.

- **Rendszerhiba:** ugyanaz mint az előbbi esetben, kiegészítve azzal a következménynyel, hogy a megfelelő könyvelési adatok karbantartása is meghiúsulhat.

- **Megbízhatóság csökkenése:** fokozatosan alakul ki. Alapvető oka a gyenge rendszer menedzsment és a minőségi követelmények figyelmen kívül hagyása (pl. a rendszerváltoztatásokat nem dokumentálják és nem tesztelik megfelelően). A rendszer "törékennyé" válik, nehezebb karbantartani és pénzügyi outputjaiban nagyobb valószínűséggel fordulnak elő hibák.

- **Csalás és a rendszer használatával való szándékos visszaélés:** a nem megfelelő kontrollok növelik a szabálytalan változtatások kockázatát, és így a csalás és a rendszer használatával való egyéb szándékos visszaélések kockázatát is, ami hatással lehet a könyvelésre (pl. a pénzügyi adatok megváltoztatása vagy kitörlése, vagy indukált rendszerhiba). A konfigurációs elemeket megfelelően védeni kell a szabálytalan vagy illetéktelen változtatásokkal szemben mind fizikai, mind logikai kontrollokkal, valamint a változáskezelési folyamatban a feladatköröket megfelelően el kell határolni.

- **A működésfolytonossági terv sérül:** egy vészhelyzetben/szükséghelyzetben bármilyen értékről is legyen szó, a működésfolytonossági terveknek reálisnak és megvalósíthatónak kell lenniük. Ha a rendszerváltoztatások után nem frissítik/módosítják az működésfolytonossági terveket, akkor azok értéke gyorsan erodálódik, és könnyen megvalósíthatatlanná válnak.

Változáskezelés kontrollok

A változáskezelés kontrollok hivatottak biztosítani, hogy a számítógépes rendszerek változtatásai megfelelően szabályozottak, teszteltek, elfogadottak és dokumentáltak legyenek. A gyenge változás-kontrollok véletlenszerű (nem szándékos) vagy rosszindulatú változtatásokat eredményezhetnek a szoftverekben és az adatokban. A rosszul megtervezett változások módosíthatják a pénzügyi adatokat, vagy eltörölhetnek ellenőrzési nyomvonalakat.

A változások kezelésének leghatékonyabb kontrollját egy, a felső vezetés által is elfogadott, betartatott és felügyelt eljárásrend biztosíthatja. Ha a vizsgált intézmény nem is rendelkezik ilyen speciális dokumentummal, az eljárás alább részletezett főbb feladatait következetesen alkalmazni kell a változtatások megbízható kivitelezése érdekében.

A változtatás igénye kiindulhat az informatikai vezetéstől (pl. korszerűsítés, kapacitásnövelés), vagy a megváltoztatandó alkalmazói rendszer felhasználóitól, vezetésétől (jogszabályokhoz igazodás, új funkciók, sebességnövelés stb.). Kezdeményezőtől függetlenül meg kell magyarázni és dokumentálni kell a szándékolt változtatások okát, részletesen meg kell határozni a megváltoztatandó eszközöket vagy alkalmazói programokat, adatbázisokat. A változtatási kérelmeket engedélyeztetni kell mind az informatikai vezetéssel, mind a megváltoztatandó rendszer tulajdonosával (felhasználójával). Az ellenőrzési nyomvonal biztosítása érdekében mindezen tevékenységeket dokumentálni kell, aminek szervezeti szintű egységesítésére célszerű bevezetni egy "változási kérelem" űrlapot.

A rendszerek helyes működése érdekében a változtatási kérelmeket felül kell vizsgálni, azaz azonosítani és értékelni kell a vele járó kockázatokat. A kockázatok azonosításába és értékelésébe be kell vonni minden potenciális kockázatviselőt, akik a változás mértékétől függően lehetnek: felhasználói csoportok vezetői, üzemeltetés vezető, adatbázis adminisztrátor, hálózat menedzser, informatikai biztonsági felügyelő, rendszertervezési csoportvezetők stb. A kockázatértékelés eredményeként megtörténhet a tervezet elvetése vagy jelentős módosítása is. Ez utóbbi esetben is dokumentálni kell a módosítás okait és tartalmát.

A változtatások végrehajtása előtt konzultációt kell biztosítani a végfelhasználókkal is az őket érintő IT infrastruktúra-változtatásokról. Példaképpen említhetőek a LAN-ok, WAN-ok, szerverek és operációs rendszerek, amelyek rendszerint nem a felhasználók felügyelete alatt vannak, de működésük megváltozása, vagy maga a változás folyamata kihatással lehet munkavégzésükre. Ezért például az infrastruktúra-változtatásokat olyan időszakokban kell végrehajtani, amikor a felhasználók a legkisebb valószínűséggel találkoznak az ebből fakadó problémákkal és hibákkal (pl. el kell kerülni az év végi könyvelési és a havi bérszámfejtési időszakot).

A változtatások végrehajtása előtt továbbá visszaállítási (regressziós) tervet kell készíteni olyan esetekre, amikor olyan komolyabb probléma merül fel, amit a kockázat elemzés vagy a későbbi tesztelés nem fedett le. Egy sikertelen változtatás működtetési zava-

rokhoz vezethet, ami a biztonsági kontrollok működését is korlátozhatja , valamint a feladatokat tovább nehezíti a feldolgozatlan tranzakciók újbóli "felépítése" is. Ez egy sajátos kockázat, amely új rendszerek bevezetésénél vagy nagyobb rendszerváltoztatások végrehajtásánál jelentkezik. Habár a rigorózus tesztelés csökkenti a hibák kockázatát, gazdaságtalan a rendszer minden lehetséges folyamatát letesztelni az adatok minden lehetséges kombinációjával. Ezért sokkal célszerűbb előre egy olyan megvalósítható tervet készíteni, amellyel vissza lehet állni a régi rendszerre, ha az új valamilyen előre nem látható okból nem működne.

A változtatások végrehajtása során minden esetben biztosítani kell egy teljes ellenőrzési nyomvonalat, még a szükséghelyzeti változtatások során is (ld. később). Az ellenőrzési nyomvonalban a változáskezelési folyamat minden lépését rögzíteni kell, ami alapvetően a folyamat felügyeletét és ellenőrizhetőségét - mind a belső mind a külső ellenőrzés számára - szolgálja.

A változtatások megfelelő végrehajtásának egyik kulcskérdése, hogy mindig legyen a változásnak egy "tulajdonosa", aki az alapvető fontosságú kérdésekben döntést hoz, mint például a rendszer szolgáltatások megtervezése, vagy a költségek és a határidők kérdése. Ha az ilyen döntések nem egy kézben összpontosulnak, az a változtatási folyamat megakadásához, vagy nem megfelelő végrehajtásához vezethet, ami befolyásolhatja az egyéb kapcsolódó - de nem megváltoztatott - rendszerek megbízható működését is.
A változtatások végrehajtása után a szervezet informatikai és felhasználói vezetőinek meg kell bizonyosodniuk arról, hogy a változások megfelelően megtörténtek-e. A legtöbb esetben ez körültekintő teszteléssel még az üzembe helyezés előtt megoldható, ezáltal is csökkentve annak kockázatát, hogy az élő környezetben működési rendellenességek lépjenek fel. Sok esetben azonban olyan a változtatás jellege, hogy az eredmény nem ellenőrizhető azonnal. Ilyen lehet például egy átdolgozott oktatási anyag; vagy a hálózati kapacitás növelése annak érdekében, hogy a csúcsidőszakokban csökkenhessen a válaszidő. Ezen esetekben figyelmet kell fordítani a változások eredményének folyamatos mérésére, tesztelésére.

Ideális esetben a szervezetben van egy kinevezett személy a változtatások kezelésére, de a terület nem igényel teljes munkaidős állást, illetve ez ritkán fordul csak elő. A változáskezelések irányítása és felügyelete inkább vezetői feladatkör, és a gyakorlatban egyéb felelősségi körökkel együtt létezik. Fel kell azonban hívnunk a figyelmet a feladatkörök megfelelő szétválasztására, azaz hogy egy személyben senki ne engedélyezhessen, alakíthasson ki és helyezhessen üzembe változtatásokat. Optimálisan az alábbi feladatokat kell szétválasztani:

- változások engedélyezése és nyilvántartása;
- a megváltoztatandó komponensek felügyelete és kontrollja;
- a változtatás kialakítása (szerelés, programozás, módosítás, stb.);
- a változtatás áttekintése és tesztelése (minőségi kontroll);
- a megváltoztatott komponens élő környezetbe helyezése.

Változtatások szükséghelyzetben

A rendszerváltoztatások nem mindig betervezett események. Üzemszünetek, meghibásodások és egyéb előre nem látható problémák gyakran felmerülnek, amelyek működési okokból sürgős javítást igényelnek. Néha annyira sürgős esetről van szó, hogy a szokásos változáskezelési eljárások alkalmazása, vagy a megfelelő illetékesek elérése - pl. munkaidőn kívül - még tovább növelné a probléma nagyságát. Ilyen körülmények között szükséghelyzeti eljárásokat kell végrehajtani.

A szükséghelyzeti változáskezelési eljárások alapvető minimumként kell hogy tartalmazzanak egy *biztonsági ellenőrzési nyomvonalat* minden eseményről, amely a szükséghelyzeti változtatás alatt történik. Azonban amint a körülmények megengedik, a problémát a szokásos változáskezelési eljárásmenetbe kell terelni. *Ez nem pusztán egy bürokratikus követelmény;* ezáltal biztosítható hogy a rendszerre vonatkozó változási kockázatokat azonosítják és kezelik, a változásokat megtervezik és a szervezet fejlesztési sztenderdjei alapján valósítják meg (különösen fontos a rendszer-dokumentáció megfelelő módosítása), és hogy a megfelelő teszteket végrehajtják.

Kérdések a 3.2. ponthoz:

Változáskezelés kontrollok

3.2.1. Rendelkezik-e a szervezet a felső vezetés által is elfogadott eljárásrenddel a változások, változtatások kezelésére?

3.2.2. Hogyan biztosítják, hogy a dolgozók következetesen alkalmazzák a változáskezelési eljárásrendet?

3.2.3. Megfelelően dokumentáltak-e a változtatási kérelmek:

a) Magyarázatot adnak-e a változtatás okáról;

b) Meghatározzák-e a megváltoztatandó komponenseket

c) Szükséges-e mind az informatikai, mind a felhasználói szervezeti egység vezetőjének engedélye?

3.2.4. Meghatározzák és értékelik-e a kockázatokat a változtatási kérelem alapján?

3.2.5. Rendszeresen bevonnak-e minden érintettet a változtatás kockázatainak vizsgálatába?

3.2.6. Készítenek-e visszaállítási tervet a változtatások megkezdése előtt?

3.2.7. Biztosítják-e az ellenőrzési nyomvonalat a változtatási folyamatok során, azaz nyilvántartják-e (naplózzák-e) a folyamat minden lépését?

3.2.8. Kineveznek-e minden változtatás esetében egy olyan felelős személyt (a változtatás "tulajdonosát"), aki a folyamat meghatározásával és végrehajtásával kapcsolatos kérdésekben egy személyben dönt?

3.2.9. Biztosított-e a változtatások eredményének megfelelő ellenőrzése, tesztelése?

3.2.10. Megfelelő-e a feladatköri szétválasztás a változáskezelési folyamatokban?

Változtatások szükséghelyzetben

3.2.11. Van-e a szervezetnek meghatározott eljárásrendje a szükséghelyzeti változtatások eseteire?

3.2.12. Rögzítenek-e ellenőrzési nyomvonalat a szükséghelyzeti változtatások folyamán?

3.2.13. Hogyan biztosítja a vezetés, hogy a szükséghelyzeti változtatások ne eredményezhessék a változáskezelési rendszerrel való visszaélést azáltal, hogy megkerülik a szokásos (pl. engedélyezési, kockázat értékelési, tesztelési, dokumentálási) eljárásokat?

3.2.14. Végre kell-e hajtani utólag a szokásos változáskezelési eljárásokat a szükséghelyzeti változtatások után? Ha igen, mely lépéseket?

4. Működésfolytonossági terv

Ha egy intézmény hosszabb vagy rövidebb ideig nem tudja feldolgozni, előhívni vagy megvédeni elektronikusan kezelt információit, miközben működési folyamataiban jelentős mértékben alkalmaz elektronikus rendszereket, akkor a szervezeti feladatok ellátásában is – kisebb vagy nagyobb – problémák léphetnek fel. Ennek elkerülése – illetve az esetleges negatív hatások elviselhető mértékűre csökkentése – érdekében az intézményeknek rendelkezniük kell:

- megfelelő eljárásrenddel annak érdekében, hogy megvédjék információs erőforrásaikat és minimálisra csökkentsék az előre nem látható üzemzavarok kockázatát;

- megfelelő tervvel, melynek alapján a szervezet kulcsfontosságú folyamatait vissza tudják állítani egy esetleges üzemzavar után.

Ez utóbbi tervet nevezzük *működésfolytonossági tervnek*. Sokszor használatos még a katasztrófa terv elnevezés is, de a működésfolytonosságot biztosító kontrollok ennél tágabb célt szolgálnak, azaz a lehetséges üzemzavarok teljes körére vonatkoznak. Beletartoznak a viszonylag kisebb feldolgozási fennakadások, hibás adatrögzítések, vagy egy rövid áramszünet ugyanúgy, mint a nagyobb katasztrófák (tűzkár, vízkár, egyéb természeti katasztrófák stb.). Ha a szervezetnél nem alakítottak ki megfelelő kontrollokat, akkor még a viszonylag kisebb feldolgozási fennakadások is *adatok elvesztéséhez vagy sérüléséhez* vezethetnek. A következményeket pedig fokozhatják a pénzügyi veszteségek, a drága helyreállítási munkák, vagy helytelen vezetői döntések a téves információk alapján.

Az üzemzavarok vagy káresemények hatásának mérséklése érdekében nagyon fontos, hogy a működésfolytonossággal összefüggő kontrollok kialakítását a felső vezetés és az alkalmazottak is megértsék és támogassák. A felső vezetés elkötelezettsége különösen lényeges annak érdekében, hogy a működésfolytonossági tervhez biztosítsák a szükséges erőforrásokat, továbbá rendszeressé tegyék a terv oktatását és tesztelését.

A működésfolytonossági kontrollok kiértékeléséhez az alábbi kulcsfontosságú feladatok végrehajtását kell megvizsgálni:

4.1. A lényeges és érzékeny számítógépes folyamatok értékelése, valamint az ezeket támogató erőforrások azonosítása

4.2. Intézkedések a potenciális károk és üzemszünetek minimalizálására

4.3. Átfogó működésfolytonossági terv kidolgozása

4.4. A működésfolytonossági terv rendszeres tesztelése és aktualizálása

4.1. A lényeges és érzékeny számítógépes folyamatok értékelése, valamint az ezeket támogató erőforrások azonosítása

A legtöbb szervezet esetében léteznek olyan számítógépesített folyamatok, amelyek az intézményi működés szempontjából kiemelt fontosságúak (pl. egy főkönyvi vagy számlavezető rendszer), ezért folyamatos üzemelésüket biztosítani kell. Ez azonban jelentős költségeket von maga után, ezért gazdaságtalan lenne minden számítógépes folyamat számára egyformán magas szintű folyamatosságot biztosítani. A vezetésnek tehát meg kell vizsgálnia, hogy mely adatok és folyamatok kiemelt fontosságúak, illetve milyen erőforrások szükségesek ezek folyamatos fenntartásához vagy üzemzavar utáni visszaállításához. Ez az első lépés ahhoz, hogy megállapítható legyen: mely erőforrásokat kell a leginkább védeni és milyen működésfolytonossági tervet kell készíteni.

A lényeges adatok és folyamatok azonosítása, osztályozása

A folyamatok és adatok lényegességének, érzékenységének meghatározását és osztályozását a szervezet egész működési folyamatát átfogó kockázatértékelés alapján kell elvégezni. (Az átfogó kockázatértékelés a szervezet biztonsági szabályzatának megalkotásához is elengedhetetlen.) Figyelembe kell venni az olyan adatok és egyéb szervezeti eszközök fontosságát és érzékenységét is, amelyeket az adott számítógépes folyamatok támogatnak vagy védenek, illetve az olyan költségeket, amelyek az adott folyamat esetleges kiesésekor keletkeznek. Például egy közigazgatási számlavezető rendszer esetében már egy napos kiesés is problémákat okozna az elszámolásokban, kifizetésekben, az informatikai rendszer hiányában csökkenne a kontroll lehetősége, továbbá az ügyfelek/állampolgárok részéről is jogos elégedetlenségek támadhatnak. Ugyanakkor egy olyan számítógépes rendszer, ami a dolgozók képzését tartja nyilván, akár hetekre is leállhat anélkül, hogy komolyabb következményekkel kellene számolni. Vannak továbbá olyan rendszerek is, amelyek hosszabb leállása nem okoz fennakadást a szervezet működésében, azonban olyan adatokat tartalmaznak (pl. személyi adatok), amelyek védelmére fokozott gondot kell fordítani akkor is, ha éppen nem üzemelnek.

A kritikus adatok és folyamatok azonosításába, osztályozásába be kell vonni a felhasználói területek képviselőit is. Az adatok *tulajdonosának* (ld. II. fejezet 2.2. pontja) és a felelős szakterületi vezetőknek kell felbecsülni az elveszett adatok vagy a félbeszakadt folyamatok negatív következményét, és meghatározni, hogy az egyes folyamatokat maximum mekkora időre tudja nélkülözni a szervezet. Ugyanakkor nagyon fontos, hogy a felső vezetés és az esetlegesen érintett egyéb szervezeti egységek is egyetértsenek ezekkel a meghatározásokkal.

A kritikus informatikai erőforrások listáját és osztályozását rendszeresen felül kell vizsgálni annak érdekében, hogy az mindig az aktuális állapotot tükrözze. A felülvizsgálatot minden olyan esetekben el kell végezni, ha változtak a szervezeti célok, a működési folyamatok, vagy a kritikus folyamatokat támogató számítógépes eszközök elhelyezkedése, felépítése.

A kritikus folyamatokat támogató erőforrások azonosítása

Ha a szervezet azonosította kritikus adatait és folyamatait, további lépésként meg kell határoznia az ezeket kiszolgáló minimálisan szükséges erőforrásokat, és elemeznie kell szerepüket. A kiszolgáló erőforrások lehetnek:

- számítógépes eszközök: hardver, szoftver, adatfájlok;
- számítógépes működéshez szükséges anyagok: nyomtatópapír, formanyomtatványok;
- telekommunikációs szolgáltatások;
- illetve bármely más erőforrás, amely a folyamatok működéséhez szükséges: dolgozók, szakemberek, irodai eszközök, vagy nem elektronizált nyilvántartások.

A felmérések során például meg kell állapítani, hogy hány merevlemezes meghajtó kell egy adott pénzügyi rendszer támogatásához, vagy milyen telekommunikációs vonalak és eszközök szükségesek egy tranzakció végrehajtásához.

Egy szervezeten belül általában a különböző erőforrásokat több különböző szervezeti egység kezeli, ezért nagyon fontos, hogy a fenti munkában mind a felhasználók, mind az informatikai dolgozók részt vegyenek.

Prioritások meghatározása a rendkívüli helyzetek esetére

A kritikus folyamatok azonosításával és osztályozásával összhangban meg kell határozni, hogy üzemzavar vagy katasztrófa esetén milyenek legyen a folyamatok visszaállításának (újbóli üzembe hozásának) prioritásai. Egyértelműen meg kell határozni a visszaállítási feladatok sorrendjét, a feladatok felelős végrehajtóját, valamint a végrehajtáshoz szükséges eszközöket vagy egyéb erőforrásokat. Ez a felmérés alkotja a működésfolytonossági alapját, illetve biztosítja, hogy egy rendkívüli helyzetben is a lehető leghatékonyabban használják fel a rendelkezésre álló számítógépes erőforrásokat. A prioritások megállapításába szintén be kell vonni mind a felhasználókat – főként az adatgazdákat és az érintett szakterületi vezetőket –, mind az informatikai vezetést.

Kérdések a 4.1. ponthoz:

4.1.1. Azonosították és osztályozták-e a lényeges adatokat és folyamatokat?

Vizsgálati szempont: Dokumentált-e a lényeges, kritikus folyamatok és adatok:

- meghatározása, osztályozása;
- ezt a dokumentumot a felső vezetés elfogadta-e;
- tükrözi-e a dokumentum az aktuális állapotot?

Vizsgálati módszer:
- A vonatkozó szabályozások vizsgálata
- Az erre a célra elkészített dokumentációk vizsgálata
- Interjú az IT és biztonsági személyzettel. Nézzük meg, hogy milyen dokumentációk állnak rendelkezésükre, és

kérdezzük meg a véleményüket az osztályozás szakmai megalapozottságáról.

4.1.2. Azonosították-e a kritikus folyamatokat támogató erőforrásokat?

Vizsgálati szempont: Meghatározták-e a lényeges, kritikus folyamatokat támogató erőforrásokat? Tekintetbe vették-e az alábbi erőforrás típusokat:

- számítógépes hardverek;
- számítógépes szoftverek;
- számítógépes eszközök ellátásához szükséges anyagok;
- rendszer dokumentációk;
- telekommunikáció;
- irodai eszközök;
- emberi erőforrások?

Vizsgálati módszer:
– A vonatkozó dokumentáció vizsgálata
– Interjú az IT és biztonsági személyzettel.

4.1.3. Megállapították-e az eljárásrendet a rendkívüli helyzetek esetére?

Vizsgálati szempont: Meghatározták-e az intézmény működési folyamatainak visszaállítási prioritásait, és ezt elfogadta-e a vezetés mind az informatika, mind a szakterületi felhasználók oldaláról?

Vizsgálati módszer:
– A vonatkozó szabályozások vizsgálata
– Az erre a célra elkészített dokumentációk vizsgálata
– Interjú az IT és biztonsági személyzettel.

4.2. Intézkedések a potenciális károk és üzemszünetek minimalizálására

A szervezetek többféle intézkedést vezethetnek be annak érdekében, hogy a rendkívüli helyzetek okozta károkat a számítógépesített folyamatokban minimalizálják. Ezeket az intézkedéseket a következőképpen osztályozhatjuk:

- az adat fájlok, számítógépes programok és fontosabb dokumentumok folyamatos duplikálása vagy rendszeres mentése (back-up), és ezen másodpéldányok elkülönített (másik épületben) tárolása;

- környezeti kontrollok kialakítása, mint például tűzoltó rendszer vagy szünetmentes áramellátás;

- alternatív feldolgozási lehetőségek kialakítása olyan esetekre, amikor a szervezet szokványos eszközei használhatatlanok (pl. számítógépes feldolgozás igénybevételéről szóló szerződés egy *másik szervezettel,* katasztrófa esetére);

- az informatikai személyzet és a felhasználók megfelelő felkészítése a rendkívüli helyzetek kezelésére.

A fenti intézkedések – különösen a megfelelő mentések (back-up) és a környezeti kontrollok kialakítása – viszonylag alacsony költségű, de hatékony megoldást jelentenek még komolyabb szerencsétlenségek esetén is. Különösen fontos, hogy a szervezet képes legyen visszaállítani (pl. egy mentésből visszatölteni) azokat az adatállományokat, amelyeket már nem lehet egyéb úton újra előállítani. Továbbá – a váratlan üzemszünetek megelőzésére – hatékony karbantartási, problémakezelési és változáskezelési eljárásokat célszerű a szervezetnek kialakítania a hardver eszközökre is.

Az alcímben említett szükséges intézkedések értékeléséhez az alábbi szervezeti kontrollokat kell megvizsgálni:

Eljárások az adatok és programok mentésére (back-up)

Ha egy szervezet csökkenteni akarja az esetleges üzemszünetekből eredő kárát, költséghatékonyság szempontjából a legjobb megoldás az adatállományok és szoftverek rendszerszerű másolása, valamint a másolatok biztonságos tárolása egy elkülönített helyen (másik épületben). Ugyanis egy vagy több számítógép meghibásodásakor maga az eszköz viszonylag könnyen cserélhető, de a költségeket jelentősen megnövelheti, ha az adatállományokat újból létre kell hozni, és a szoftvereket újra kell telepíteni. Ez utóbbi feladatok ráadásul igen időigényesek is. Sokszor az adatállományokat nem is lehet újból („nulláról", papíron tárolt dokumentumok alapján, vagy nagyon régi adatokból) létrehozni. Az adatállományok újbóli előállításának és a szoftverek újratelepítésének közvetlen költségén túl az üzemszünet hossza jelentős, további pénzügyi veszteségeket is okozhat.

Ezért egy megfelelő eljárásrendet kell kialakítani a számítógépes fájlok (törzsadatok, tranzakciós fájlok, alkalmazói rendszerek, rendszerszoftverek, és adatbázis szoftverek stb.) rendszeres mentésére, és a mentések biztonságos, elkülönített tárolására. Az elkülönített tárolás helyét körültekintően kell meghatározni: ez a hely lehetőleg távol legyen az eredeti adatokat kezelő rendszerektől azért, hogy ugyanazon káresemények (tűz, víz stb.) ne legyenek egyszerre mindkét helyre – és ezzel együtt az adathordozókra - hatással. Továbbá ennek az elkülönített helynek is védettnek kell lennie az illetéktelen hozzáféréstől és a környezeti károktól.

A fájlok mentésének gyakorisága az adatokat módosító műveletek volumenétől és gyakoriságától függ. Általában a fájlok napi mentése megfelelő biztonságot nyújt, azonban ha egy rendszer naponta több ezer tranzakciót dolgoz fel, akkor célszerű naponta többször is menteni. Fordított esetben, ha csak néhány tranzakció fut le a rendszerben egy héten, akkor a heti egyszeri mentés is megfelelő lehet.

A mentési eljárásokat mindig úgy kell megtervezni, hogy egy aktuális másolat mindig rendelkezésre álljon. Például azelőtt nem szabad törölni a régebbi mentéseket, mielőtt az új adatállomány meg nem érkezik az elkülönített, biztonságos tárolóhelyre.

Általában az adatbázis-menedzserek felelősek a fájlok rendszerek mentéséért. Azonban előfordulhat, hogy olyan számítógépeken is tárolnak érzékeny adatokat, amelyek nem az említett adatbázis-menedzsment felügyelete alá tartoznak: ekkor a szervezetnek szabályoznia kell, hogy ezen adatok mentéséért ki felel.

Az adatfájlokon és szoftvereken kívül egyéb másolatok elkülönített tárolására is szükség lehet a folyamatos üzemeltetés biztosításához. Ilyen dokumentumok lehetnek a rendszer- és alkalmazási dokumentációk, egyéni formanyomtatványok, licenszek stb. Habár az IT kontrollok vizsgálata elsősorban az elektronikusan kezelt adatokra koncentrál, nagyon fontos, hogy a lényegesebb papír alapú dokumentációk másolatait is egy elkülönített helyen tárolják.

Megfelelő környezeti kontrollok kialakítása

A környezeti kontrollok megelőzik vagy csökkentik az esetleges károk hatását, az informatikai folyamatok megszakadását. Környezeti kontrollok lehetnek:

- tűzjelző és tűzoltó rendszerek
- füstérzékelők
- víz- vagy nedvesség érzékelők
- redundáns légkondicionáló rendszerek
- alternatív áramellátás
- zárszelepek azon vízvezetékrendszerben, amely számítógépes helyiségek körül vagy felett húzódik
- olyan helyiségek, amelyeket tűzálló anyagokból építettek, és úgy tervezték, hogy megakadályozzák a tűz terjedését
- olyan szabályzatok, amelyek tiltják az étkezést, az italfogyasztást és a dohányzást a számítógépes helyiségekben.

A környezetei kontrollok csökkentik az olyan káreseményekből fakadó veszteséget, mint pl. a tűz; illetve megelőzik az káreseményeket azáltal, hogy már korai szakaszban jeleznek egyes problémákat, mint pl. a vízszivárgás vagy füst. A szünetmentes vagy alternatív áramellátás segítségével a rövidebb hálózati áramkimaradások átvészelhetőek, vagy elegendő időt biztosítanak arra, hogy a szükséges adatokat még időben elmentsék és a számítógépeket szabályos rendben állítsák le. (A számítógépek hirtelen lekapcsolása károkat okozhat az éppen használt adatállományokban.)

A személyzet megfelelően felkészült a rendkívüli helyzetek kezelésére

A rendkívüli helyzetek megelőzésére, kezelésére a dolgozókat ki kell képezni, és felelősségi körüket tudatosíttatni kell velük. Például az adatkezelő központ munkatársait ki kell képezni – és rendszeresen gyakoroltatni – hogy mi a teendőjük tűz, vízbetörés vagy a vészjelzők egyéb megszólalása esetén, hogyan kell az alternatív feldolgozási folyama-

tokat elindítani. Hasonló módon, ha szervezeten kívüli felhasználói is vannak a rendszernek, akkor őket is tájékoztatni kel arról, hogy mit tegyenek rendkívüli helyzetek esetén.

A vészhelyeztek kezeléséről és a felelősségi körök kijelöléséről szóló információkat képzéseken és szabályzatokon keresztül lehet eljuttatni a dolgozókhoz. Célszerű évente legalább egy alkalommal képzést tartani erről az alkalmazottaknak, illetve minden olyan esetben, amikor ezek a szabályzatok jelentősen megváltoznak.

Hatékony hardver-karbantartás, problémakezelés és változáskezelés a váratlan üzemszünetek megelőzése érdekében

Váratlan üzemszünetet okozhat valamely hardver eszköz (pl. hálózati elem, szerver) meghibásodása, vagy egy olyan rendszerváltoztatás, amelyről előzetesen nem értesítették megfelelően a felhasználókat. Az ilyen esetek megelőzése érdekében hatékony hardver-karbantartási, problémakezelési és változáskezelési eljárásokat kell kialakítani.

A hardver-karbantartásokat célszerű rendszeresen, ütemezve végrehajtani, ezzel is csökkentve a meghibásodás valószínűségét, illetve bekövetkezése esetén a hatását. A hardver gyártók általában meghatározzák az eszközök karbantartásához szükséges rendszerességet és műveleteket. A karbantartásokat úgy célszerű ütemezni, hogy ezek a munkálatok a lehető legkisebb mértékben zavarják a szervezet – különösen a fontosabb területek – ügymenetét. Minden karbantartási munkát dokumentálni kell, különösen a be nem tervezett javításokat. A dokumentációk elemzése során azonosíthatóak lesznek a problematikusabb területek, amelyeken esetleg további intézkedéseket kell bevezetni egy stabil működés biztosítása érdekében. A hatékony karbantartási munkálatok érdekében a számítógépes adatfeldolgozási folyamatokat is megfelelő rugalmassággal kell kialakítani, hogy mind a megelőző jellegű, mind a váratlan karbantartások, javítások elvégezhetőek legyenek. Azon alkalmazások részére pedig, amelyek a szervezeti működés szempontjából kiemelten fontosak, célszerű készenléti hardver eszközöket is beszerezni.
A hatékony problémakezelés érdekében folyamatosan nyomon kell követni az informatikai szolgáltatások teljesítményét, és dokumentálni kell a felmerülő problémákat. Az illetékes vezetőnek (az adatok illetve az alkalmazás *tulajdonosának*) meg kell határoznia, hogy az adatfeldolgozásnak és az on-line szolgáltatásoknak milyen fokú rendelkezésre állási szintet kell elérnie. Folyamatos nyilvántartást célszerű vezetni, hogy az aktuális teljesítmény mennyiben éri el a meghatározott szintet. Ehhez vezetni és elemezni kell a problémákat, a teljesítési csúszásokat és a megoldásra fordított időt annak érdekében, hogy a visszatérő mintákat és trendeket azonosítani lehessen. Az illetékes felsővezetőnek rendszeresen meg kell vizsgálnia, hogy az informatikai szolgáltatások teljesítménye eléri-e a kitűzött célokat, továbbá fel kell mérnie, hogy ez a felhasználók elvárásainak megfelel-e.

A hardver eszközök és szoftverek cseréjét célszerű ütemezett tervek alapján végrehajtani, hogy az a szervezeti működésben a lehető legkevesebb fennakadást okozzon, továbbá hogy megfelelő tesztelési lehetőség álljon rendelkezésre a felhasználói rendszerek

számára is. Ilyen esetekben a felhasználókat előzetesen is értesíteni kell, hogy nem váratlan üzemzavarról van szó.

Kérdések a 4.2. ponthoz:

4.2.1. Kialakították-e a megfelelő eljárásokat az adatok és programok mentésére?

Vizsgálati szempont: A mentéseket egy előre meghatározott ütemterv alapján, megfelelő gyakorisággal végzik és rotálják ahhoz, hogy az adatvesztéseket és komolyabb üzemzavarokat meg lehessen előzni.

Vizsgálati módszer:
- A mentésekre kialakított, írásban lefektetett szabályozások és eljárások vizsgálata.
- Vesse össze a szoftverleltárt a külső helyszínen tárolt, elmentett fájlokkal, valamint vizsgálja meg ezen fájlok „korát” (azaz mikor történt legutóbbi mentésük).
- A kritikus (érzékeny, vagy különösen fontos) fájlok egy kiválasztott csoportja esetében vizsgálja meg a mentés tartalmát. Ellenőrizze, hogy a mentett tartalomból az aktuálisan használt tartalom visszaállítható-e.
- Vizsgálja meg, hogy a külső helyszínen az előírásoknak megfelelően megtalálhatóak-e a mentések, és ezek rotációja biztonságos-e (azaz csak akkor lehet a régi, törlésre kijelölt adathordozót visszaküldeni újbóli használatra, ha a legfrissebb mentés már megérkezett).

Vizsgálati szempont: A rendszer- és alkalmazási dokumentációk megtalálhatóak-e a külső helyszínen?

Vizsgálati módszer: Vizsgálja meg a dokumentációk fellelhetőségét.

Vizsgálati szempont: A mentések tárolására szolgáló másodlagos tároló:

- földrajzilag is el van különítve az elsődleges helyszín(ek)től;
- megfelelő védettséget élvez mind a környezeti ártalmaktól, mind az illetéktelen belépéstől.

Vizsgálati módszer: Vizsgálja meg a mentések tárolására kialakított helyiséget.

4.2.2. Kialakították-e a megfelelő környezeti kontrollokat?

Az alábbi vizsgálatot célszerű a fizikai kontrollok vizsgálatával (ld. III. fejezet 2.3.) összefüggésben végezni!

Vizsgálati szempont: Alapvető kontrollok:

- Megfelelő tűzvédelmi berendezéseket (pl. füstérzékelő, tűzoltó készülék vagy tűzoltó rendszer) beszereltek, és azok működnek.
- Megfelelő kontrollok működnek egyéb környezeti tényezők elleni védekezésül, mint pl. vízbetörés, földrengés.
- A légkondicionálás redundanciája biztosított.
- Az épület közművezetékei nem veszélyeztetik a számítógépes helyiségeket (minimális követelmény, hogy legyenek megfelelő zárcsapok a vezetékekben, és ezek pontos helyét is ismernie kell a személyzetnek).
- Szünetmentes tápegységekkel vagy áramfejlesztőkkel biztosítsák annak lehetőségét, hogy a rendszereket bármikor szabályosan le lehessen állítani.

Vizsgálati módszer:

– Mérje fel a szervezet felszereléseit.
– Interjú a helyi vezetéssel.
– A helyszínen vizsgálja meg, hogy a dolgozók ismerik-e a következő elemek pontos elhelyezkedését: tűzjelző és tűzoltó berendezések, normál illetve kiegészítő elektromos kapcsolók, vízelzáró csapok, szellőző berendezések, illetve bármely más berendezés, amely vészhelyzetben fontos lehet.
– A helyszínen vizsgálja meg a légkondicionáló rendszer elhelyezését, karbantartását és az ahhoz való hozzáférési lehetőségeket.
– A helyszínen vizsgálja meg, hogy a mennyezet felől betörhet-e víz a számítógépes helyiségbe, mennek-e keresztül a helyiségen vízvezetékek, illetve vannak-e vízérzékelők a padlón elhelyezve.
– Vizsgálja meg, hogy a hő- és füstérzékelők aktiválódása riasztja-e a tűzoltóságot.

Vizsgálati szempont: A környezeti kontrollokat rendszeresen tesztelik

Vizsgálati módszer:

– Vizsgálja meg a tesztelésre vonatkozó szabályzatokat.
– Vizsgálja meg a környezeti kontrollok legutóbbi teszteléséről készült jegyzőkönyveket vagy egyéb dokumentációkat.

Vizsgálati szempont: Tiltott az étkezés, italfogyasztás, és bármely más olyan tevékenység, mely a számítógépes eszközök meghibásodásához vagy rongálásához vezethetnek.

Vizsgálati módszer:
– Vizsgálja meg a dolgozók magatartására vonatkozó szabályzatokat.
– A helyszínen figyelje meg a dolgozók viselkedésmódját.

4.2.3. Megfelelően felkészült-e a személyzet a rendkívüli helyzetek kezelésére?

Vizsgálati szempont: Alapvető kontrollok:

- Az informatikai személyzet képzésben részesült, és ismeri is a rendkívüli helyzetben rá háruló feladatokat és felelősséget.
- Az informatikai személyzet rendszeres továbbképzésben részesül vészhelyzeti (tűz, víz és egyéb riasztások) teendőiről.
- A rendkívüli helyzetek kezelésével kapcsolatos teendők megfelelően dokumentáltak.

Vizsgálati módszer:
– Interjú az informatikai személyzettel.
– A képzések jelenléti íveinek vizsgálata.
– A képzések tananyagának vizsgálata.
– A rendkívüli helyzetek kezelésére vonatkozó szabályzatok vizsgálata.

Vizsgálati szempont: A rendkívüli helyzetek kezelését rendszeresen tesztelik.

Vizsgálati módszer:
– A tesztelésre vonatkozó szabályzatok vizsgálata.
– A tesztelési dokumentációk vizsgálata.
– Interjú az IT személyzettel.

4.2.4. Kialakítottak-e hatékony hardver-karbantartási, problémakezelési és változáskezelési eljárásokat a váratlan üzemszünetek megelőzése érdekében?

Vizsgálati szempont: A vonatkozó szabályzatokat és eljárásrendeket kialakították.

Vizsgálati módszer: – A vonatkozó szabályzatok és eljárásrendek vizsgálata.

Vizsgálati szempont: A hardver karbantartások:

- előre ütemezettek;
- a gyártók által meghatározott szempontokat (rendszeresség, feladat) figyelembe véve történnek;
- a lehető legkevesebb mértékben akadályozzák a szervezet működését;

- minden esetben dokumentáltak.

Vizsgálati módszer: – Interjú az IT személyzettel és a felhasználókkal.
– A karbantartásokra vonatkozó dokumentáció vizsgálata.

Vizsgálati szempont: A számítógépes adatfeldolgozási folyamatokat megfelelő rugalmassággal alakították ki ahhoz, hogy mind a megelőző jellegű, mind a váratlan karbantartások, javítások elvégezhetőek legyenek.

Vizsgálati módszer: – Interjú az IT személyzettel és a felhasználókkal.
– A karbantartásokra vonatkozó dokumentáció vizsgálata.

Vizsgálati szempont: A szervezeti működés szempontjából kiemelten fontos alkalmazások részére készenléti hardver eszközök is rendelkezésre állnak.

Vizsgálati módszer: – Interjú az IT személyzettel.

Vizsgálati szempont: További kontrollok:

- Az illetékes szakterületi vezető (az adatok illetve az alkalmazás tulajdonosa) meghatározta, hogy az adatfeldolgozásnak és egyéb szolgáltatásoknak milyen fokú rendelkezésre állási szintet kell elérnie.
- Folyamatos nyilvántartást vezetnek, hogy az aktuális teljesítmény mennyiben éri el a meghatározott szintet.
- A felmerült problémák összesített elemzésére rendszeresen sor kerül.
- Az illetékes felsővezető rendszeresen megvizsgálja, hogy a kitűzött teljesítmény-célok megvalósulnak-e.
- A hardver eszközök és szoftverek cseréje előre meghatározott tervek szerint történik, és erről a felhasználókat is értesítik.

Vizsgálati módszer: – Interjú az illetékes felsővezetővel, az informatikai vezetővel és a felhasználói osztályok vezetőivel.
– A vonatkozó szabályzatok vizsgálata.

4.3. Átfogó működésfolytonossági terv kidolgozása

A működésfolytonossági terv meghatározza, hogyan kell a feldolgozási folyamatokat újból működésbe helyezni, alternatív feldolgozási eszközöket igénybe venni akkor, ha a szokásos eszközök működésképtelenek lesznek, elérhetetlenné válnak. Nagyon fontos, hogy ez a terv világosan és érthetően legyen megfogalmazva, az érintett dolgozók pontosan ismerjék, és mindig az aktuális viszonyokat (eljárásmenetet, eszközfelhasználást

stb.) tükrözze. Lényeges továbbá a terv rendszeres tesztelése is, amire a következő pontban térünk ki.

Aktualizált működésfolytonossági terv dokumentálása

A működésfolytonossági tervet az informatikai **és** a felhasználói osztályokkal egyetértésben kell kialakítani, az érintett dolgozókkal pedig meg kell ismertetni.

A tervnek tükröznie kell az intézménynél meghatározott kockázatokat és a szervezeti feladatok prioritását. A tervet úgy kell kialakítani, hogy a működésfolytonosság biztosításának költségei ne lépjék túl a kivédeni szándékozott károkat.

A terv legyen elég érthető ahhoz, hogy sikeres végrehajtása ne csak egy vagy két ember tudásától, szakértelmétől függjön. Ennek érdekében a következő információkra mindenképpen szükség van:

- az egyes tevékenységek végrehajtásához szükséges erőforrások (számítógépek, adathordozók, adatbázisok, emberek, stb.) meghatározása,
- a visszaállítási tevékenységbe bevonandó emberek feladat- és felelősségi köre,
- eljárásrendek az alternatív feldolgozó eszközök (amelyek lehetnek másik szervezet vagy szervezeti egység eszközei is) igénybevételére, illetve ha szükséges, a személyzet utaztatására,
- a mentések külső tárolóhelyeinek meghatározása,
- a szervezeti működés szempontjából lényeges alkalmazások újraindítási – fontossági – sorrendje.

A működésfolytonossági terv másolatát célszerű elhelyezni több – biztonságos – helyen is azért, hogy egy, az elsődleges feldolgozási helyeket ért esemény (pl. tűz) után is rögtön elérhető legyen.

Alternatív feldolgozási és telekommunikációs eszközök igénybevételére tett intézkedések

A folyamatos működés igényszintjétől függően alternatív feldolgozási lehetőségeket lehet meghatározni. Ennek egyik véglete az úgynevezett „hot site”, azaz egy teljes mértékben felszerelt, azonnal működésbe hozható eszközpark egy biztonságos helyen. A másik véglet pedig az úgynevezett „cold site”, ami egy teljesen üres helyszín, ahol a feldolgozási lehetőségek – egyes eszközök odatelepítésével – megteremthetőek. Alternatívát jelenthetnek még külső cégekkel, intézményekkel (pl. hardver-forgalmazóval, gyártóval, hasonló feldolgozásokat végző szervezettel) kötött megállapodások is.

Mint minden biztonsági intézkedés esetében, az alternatív feldolgozóhely kiválasztásánál is mérlegelni kell a költségeket és kockázatokat. Egy feltételnek azonban mindenképpen teljesülnie kell: földrajzilag is el kell különüljön az eredeti helyszíntől, hogy ugyanazon esemény ne károsíthassa mindkettőt. Például egy szervezet központi épületében kiütött tűz valószínűleg nem lesz hatással a szervezet egy másik, több utcával ar-

rébb található épületére – ahonnan így gyorsan el lehet kezdeni a folyamatok „újraélesztését”. (Árvíz kockázata esetében már azt is figyelembe kell venni, hogy a két épület egyszerre ne lehessen veszélyeztetve.) Az alternatív feldolgozóhely kiválasztásánál további fontos szempont, hogy rendelkezzen mindazon alapszolgáltatásokkal (megfelelő elektromos hálózat, telekommunikáció stb.), amelyekre rendkívüli esetekben – azaz az IT működés átvételekor – szükség lehet. A költségek csökkentése érdekében több különböző szervezetnek is lehet ugyanaz az épület az alternatív helye – ez csak akkor jelenthet problémát, ha egyszerre éri őket (akár különböző) katasztrófa.

Akármelyik lehetőséggel él is a szervezet, mindenképpen rendelkeznie kell egy formális megállapodással vagy szerződéssel, amely részletesen meghatározza a teendőket, jogokat és lehetőségeket a rendkívüli esetekre. Fontos feladat ezen dokumentumok rendszeres aktualizálása is azért, hogy bármikor megfelelően alkalmazkodjon a szervezet igényeihez.

Kérdések a 4.3. ponthoz:

4.3.1. Van-e dokumentált és aktualizált működésfolytonossági terv?

Vizsgálati szempont: A kialakított működésfolytonossági terv:

- a jelenlegi viszonyokat (hardver- és szoftver architektúra, feladatkörök stb.) tükrözi;
- az érintett felhasználói és informatikai osztályok vezetői elfogadták azt;
- egyértelműen meghatározza a feladatköröket a helyreállítási munkában;
- részletes utasításokat ad a helyreállítási munkálatok elvégzésére (mind az operációs rendszerek, mind az alkalmazások tekintetében);
- meghatározza az alternatív feldolgozóhelyet és a mentések tárolóhelyeit;
- eljárásokat tartalmaz arra az esetre, ha a központi adatfeldolgozó vagy egyéb szolgáltató kapacitások nem működnek;
- meghatározza a kritikus adatállományokat;
- elég részletes ahhoz, hogy minden érintett vezető megértse;
- meghatározza a szervezeti igényekkel kompatibilis informatikai és telekommunikációs hardvereket (azaz olyan eszközöket, amelyekkel a működésképtelen elemek helyettesíthetők);
- szervezeten belül megfelelően köröztetett és minden érintett dolgozó megismerte.

Vizsgálati módszer: – Vizsgálja meg a működésfolytonossági tervet, és a benne megfogalmazott intézkedéseket vesse össze a legutóbbi kockázatértékeléssel valamint az automatizált folyamatok leírásával.
– Interjú a felső- és informatikai vezetéssel.

Vizsgálati szempont: A terv végrehajtásában nincs egyedüliként meghatározott, kulcsfontosságú szereplő (dolgozó), hanem megjelöl alternatív humán erőforrásokat is az egyes feladatokra.

Vizsgálati módszer: – Vizsgálja meg a működésfolytonossági tervet.
– Interjú a felső- és informatikai vezetéssel.

Vizsgálati szempont: Üzemzavar esetén a folyamatok újraindításáig megfelelő kézi vagy más kiegészítő eszközök állnak rendelkezésre a felhasználói osztályokon az időszak áthidalására.

Vizsgálati módszer: – Vizsgálja meg a működésfolytonossági tervet.
– Interjú a felső- és informatikai vezetéssel.

Vizsgálati szempont: A működésfolytonossági terv több másolatban, különböző helyiségekben és épületekben is rendelkezésre áll.

Vizsgálati módszer: – A helyszínen ellenőrizze a másolatok meglétét.

Vizsgálati szempont: A működésfolytonossági tervet rendszeresen felülvizsgálják, és bekövetkezett változások (hardver, szoftver, személyzeti) alapján ha kell, módosítják.

Vizsgálati módszer: – Vizsgálja meg a tervet, és bármilyen dokumentációt, amely a legutóbbi felülvizsgálatról készült.

4.3.2. Tettek-e intézkedéseket alternatív feldolgozási és telekommunikációs eszközök esetleges igénybevételére?

Vizsgálati szempont: Az intézmény által kötött szerződések vagy szervezetközi megállapodások olyan alternatív feldolgozási helyeket és egyéb szükséges eszközöket biztosítanak, melyek:

- készültségi fokuk arányban áll a működés megszakadásának kockázatával;
- biztosítják a szükséges feldolgozó kapacitást;
- működésre készen állnak.

Vizsgálati módszer: – Vizsgálja meg az e tárgyban kötött szerződéseket és megállapodásokat.

Vizsgálati szempont: Az alternatív telekommunikációs szolgáltatásokat biztosították.

Vizsgálati módszer: – Vizsgálja meg az e tárgyban kötött szerződéseket és megállapodásokat.

Vizsgálati szempont: Az intézkedni kell a megfelelő személyzet utaztatásáról is, ha erre – az alternatív feldolgozóhely távolsága miatt – szükség lehet.

Vizsgálati módszer: – Vizsgálja meg az e tárgyban kötött szerződéseket és megállapodásokat.

4.4. A működésfolytonossági terv rendszeres tesztelése és aktualizálása

Részletes tesztelésre van szükség ahhoz, hogy a szervezet meggyőződhessen a működésfolytonossági terv helyességéről, azaz arról, hogy egy rendkívüli helyzetben az valóban megfelelően fog működni. A tapasztalatok azt mutatják, hogy a tesztelés szinte mindig rámutat a működésfolytonossági terv egy-egy gyenge pontjára –például hogy az alternatív feldolgozóhely nem képes olyan teljesítménnyel elvégezni a feladatokat, mint azt a vezetés elvárná. A tesztek után a terv hiányosságainak, hibáinak jelentős része megszüntethető.

A legcélravezetőbb teszt egy katasztrófa szimulálása, amikor a működésfolytonosság biztosításának folyamata átfogóan kipróbálható. Kipróbálható, hogy az alternatív feldolgozóhely tud-e úgy működni, ahogyan azt a vezetés elvárja; illetve hogy a kritikus adatok és programok visszaállíthatóak-e eredeti állapotukba a külső tárolóhely mentései alapján. A terv kipróbálása során a vezetés behatárolhatja a gyenge pontokat és intézkedhet a megoldásokról. A tesztek továbbá azt is megmutatják, hogy az alkalmazottak képzése mennyire volt megfelelő, azaz egy esetleges katasztrófahelyzetben mennyire vannak tisztában feladat- és hatáskörükkel.

A terv rendszeres tesztelése

A működésfolytonossági terv tesztelésének gyakoriságát a szervezet működési folyamatai – azok kritikus vagy kevésbé kritikus jellege – határozzák meg. Kiemelten fontos folyamatok esetében a működésfolytonossági tervet évente egyszer vagy kétszer átfogóan ki kell próbálni, illetve akkor is, ha a tervben jelentős változtatást hajtanak végre, vagy a végrehajtásban kulcsszerepet játszó dolgozók személyében változás áll be. Fontos, hogy a felső vezetés értékelje a terv végrehajtásának nehézségeivel összefüggő kockázatokat, szabályozza a tesztelések gyakoriságát és kiterjedését.

A teszt eredményeinek értékelése, és a terv ennek megfelelő aktualizálása

A teszteredmények nagyon jó hatékonysággal mutatják meg a működésfolytonossági terv alkalmazhatóságát. Ez nagyon fontos információt nyújt a felső vezetésnek: megmutatja milyen változtatásokra van szükség és milyen további teszteket szükséges még végrehajtani; illetve a terv alkalmazása mellett milyen kockázatok jelentkeznek a működtetés folyamatosságában.

A működésfolytonossági terv tesztelése előhozhat gyengeségeket a tervben. Nagyon fontos, hogy ezen feltárások alapján aktualizálják a tervet és minden ehhez kapcsolódó tevékenységet, mint pl. az oktatást. Ezek nélkül a tesztelés gyakorlatilag haszontalan.

Kérdések a 4.4. ponthoz:

4.4.1. Rendszeresen tesztelik a működésfolytonossági tervet?

Vizsgálati szempont: Katasztrófát vagy egyéb rendkívüli eseményt szimulálva letesztelték terv aktuális változatát.

Vizsgálati módszer:
- A tesztelésre vonatkozó szabályzatok vizsgálata.
- A teszt eredményeinek vizsgálata
- Ha lehetőség adódik rá, a helyszínen figyeljen meg egy katasztrófahelyzeti tesztelést.

4.4.2. Értékelik-e a tesztek eredményét, és aktualizálják-e ennek megfelelően a tervet?

Vizsgálati szempont: A tesztek eredményeit és az eredményekből leszűrt tapasztalatokat dokumentálják, továbbá minderről tájékoztatják a felső vezetést.

Vizsgálati módszer:
- Vizsgálja meg a legutóbbi tesztekről készült jegyzőkönyvet.
- Állapítsa meg, hogy az illetékes felső vezetés ismeri-e a teszt eredményeit.

Vizsgálati szempont: A működésfolytonossági tervet és az ezzel kapcsolatos megállapodásokat a tesztek eredményei alapján aktualizálják, korrigálják.

Vizsgálati módszer:
- Vizsgálja meg, hogy van-e olyan dokumentáció, mely alátámasztja a tesztelés utáni korrekciót.

5. Külső IT szolgáltatók igénybevétele

Egyre több intézmény vesz igénybe külső szolgáltatókat outsourcing, szolgáltatás menedzsment vagy piactesztelés formájában. A külső szolgáltatók tevékenységeit egyrészt ugyanazon kontrollokkal kell szabályozni, mintha saját alkalmazottak látnák el a feladatokat, de intézményen kívüli szereplőkről lévén szó további kontrollokat is életbe kell léptetni.

Az ellenőrzött szervezetnek tekintetbe kell vennie a külső ellenőrzés igényeit, és ezt a szolgáltatóval kötött szerződésbe bele is kell foglalnia. Ugyanis a pénzügyi ellenőrzés során előfordulhat, hogy arról kell megbizonyosodni, hogy a külső szolgáltató által nyújtott adatok, kalkulációk nem tartalmaznak lényeges hibát, és ezt a bizonyosságot általában a szolgáltatónál szerezheti meg az ellenőr közvetlen ellenőrzéssel. A külső szolgáltatónak továbbá ugyanúgy biztosítania kell a megfelelő ellenőrzési nyomvonalat, hogy a vezetés és a külső ellenőrzés kellően felügyelhesse tevékenységét.

Kérdések az 5. ponthoz:

5.1. Hogyan felügyeli a szervezet a külső szolgáltató teljesítményét

a) biztonság és

b) minőség tekintetében?

5.2 Kötöttek-e szerződést a szolgáltatóval, és ha igen, lefednek-e benne minden fontos kérdést:

a) teljesítmény vagy szolgáltatási szint megállapítása

b) biztonsági követelmények

c) adattulajdonlás meghatározása

d) a szervezet adathozzáférése

e) **ÁSZ ellenőrzési hozzáférése**

f) működésfolytonossági terv?

6. Az informatikai rendszerek működtetése

Az informatikai rendszerek működtetése alapvetően két részre osztható:

- az informatikai tevékenységek számítástechnikai hátterének biztosítása, és
- a számítógéppel kapcsolatos feldolgozási tevékenységek.

A számítástechnikai háttér biztosításának, azaz az üzemeltetés és karbantartás, a személyi és dokumentációs feltételek elsődleges elemeiről a II. fejezet 2. pontjában bemutatott kérdőívek segítségével már információkat szerezhetett az ellenőr. Ezen információk az alábbi kontrollok kiértékelésének alapját jelenthetik.

A számítógéppel kapcsolatos feldolgozási tevékenységek között azokat a folyamatokat vizsgáljuk meg, amelyeket a felhasználók végeznek informatikai környezetben, és magas eredendő kockázatuk miatt szükséges a szabályozásuk. Azonban a tevékenységi területek egy része esetében nem mindig szükséges a bemutatott szigorú kontroll. Azt, hogy a vizsgálat során mely kontroll csoportokra kell kisebb vagy nagyobb hangsúlyt fektetni, az ellenőrnek kell eldöntenie az intézményről megszerzett ismeretei alapján.

6.1. Szolgáltatási szint biztosítása

A szolgáltatási szint felmérése kapcsán a II. fejezet 2.1.1. kérdésére, kitöltési útmutatójára és értékelésére utalunk vissza. A szempontokat és kockázatokat az ellenőrzés jelen szakaszában is ugyanúgy kell figyelembe venni, de a kérdésre adott válaszok, a mellékelt dokumentumok és helyszíni vizsgálat alapján részletesebben is meg kell vizsgálni az adott kontrollok működését.

Kérdések a 6.1. ponthoz

6.1.1. Hogyan határozták meg a felhasználók számára nyújtandó szolgáltatási szintet a pénzügyi rendszerek esetében?

6.1.2. Kikérték-e a felhasználók véleményét, amikor megállapították a szolgáltatás által elérendő célokat?

6.1.3. Hogyan felügyeli a vezetés a nyújtott szolgáltatási szintet? Ki felügyeli?

6.1.4. A kialakított szolgáltatási szint megfelel-e a meghatározott szervezeti céloknak?

6.1.5. Milyen folyamatok lépnek életbe ha a szolgáltatás szintje nem megfelelő.

6.2. Problémák kezelése

A problémák kezelésének felmérése kapcsán a II. fejezet 2.1.6. és 2.1.7. kérdésére, kitöltési útmutatójára és értékelésére utalunk vissza. A szempontokat és kockázatokat az ellenőrzés jelen szakaszában is ugyanúgy kell figyelembe venni, de a kérdésre adott válaszok, a mellékelt dokumentumok és helyszíni vizsgálat alapján részletesebben is meg kell vizsgálni az adott kontrollok működését.

A "problémák" alatt a következőket érjük: szoftver hibák, hardver problémák, szoftver működésképtelensége, és egyéb felhasználói kérdések a működéssel kapcsolatban. Más szavakkal mindazon - vagy olyannak tűnő események – amelyek valamilyen formában az informatikus dolgozók beavatkozását és azonnali hibaelhárítását igénylik.

Az informatikai szolgáltatásnyújtás minősége befolyásolhatja a szervezet könyvviteli nyilvántartásának kezelését. A hardver és szoftver meghibásodások, a hálózati hibák, az alkalmazások használata közben bekövetkező problémák, vagy a számítógépes vírusok olyan példák, melyek kisebb vagy nagyobb mértékben befolyásolhatják a pénzügyi adatok sértetlenségét és/vagy rendelkezésre állását. Ebből következik, hogy az informatikai szolgáltatásnyújtás minősége javul, ha az előre nem látható informatikai események, a problémák jelentése, kivizsgálása és ha szükséges megoldása a szervezetben gyors és hatékony. A nagyobb intézményekben általában egy központi, ún. help desk szolgáltatást alkalmaznak, de egy kevésbé formális rendszer is hatékony megoldást nyújthat egy kisebb, centralizált szervezetben.

Egy ideális, váratlan eseményeket, problémákat kezelő (help desk) rendszer a következő jellemzőkkel bír:

- az előre nem látható események és problémák minden típusával ugyanazon helyre kell fordulni, ezt mindenkinek ismernie kell, és elérhető kell hogy legyen minden felhasználó számára;

- munkaidőben teljes körű felhasználói támogatás nyújtása, egyébként csak a bejelentések rögzítése;

- a problémák osztályozása (pl. a rendszer, az elhelyezkedés, a típus és a probléma nagysága szerint), ezzel segítve a fontosság szerinti visszajelzést, valamint a statisztika készítését a vezetőség számára;

- a problémák kiosztása a megfelelő technikai csoport számára, kivizsgálás és megoldás céljából;

- a kiemelkedő események rendszeres felülvizsgálata, valamint a vezetés figyelmeztetése ha a helyzet súlyosbodik;

- a megoldott problémákról készült jelentések lezárása, valamint ha szükséges a felhasználók további segítése;

- a problémákról készített jelentések rendszeres elemzése és vezetői statisztikák készítése.

A célirányos statisztikák (pl. az üzemképtelen időszak hossza, a problémákra való átlagos reagálási idő) segítik a vezetést, hogy figyelemmel kísérjék a szolgáltatásnyújtás minőségét és hogy azonosítsanak bármilyen veszélyes trendet, amely alaposabb kivizsgálást igényel. Például egy alkalmazói rendszerrel kapcsolatos felhasználói kérdések következetesen magas száma jelezheti, hogy a felhasználók képzése nem megfelelő, vagy a felhasználói dokumentáció minősége erősen hiányos; illetve a PC meghibásodásokról szóló jelentések nagy száma jelezheti, hogy gyenge minőségű PC-ket szereztek be, vagy gondok lehetnek a technikai személyzet tevékenységében.

Kérdések a 6.2. ponthoz

6.2.1. Kialakított-e a szervezet egy eljárásrendet a felhasználói problémák kezelésére?

6.2.2. Hogyan gondoskodik a vezetés arról, hogy ezt az eljárásrendet minden felhasználó ismerje és következetesen alkalmazza?

6.2.3. Létezik-e a szervezetben egy, a felhasználói problémák kezelésére kialakított csoport (help desk) , vagy egy kijelölt, ezzel foglalkozó alkalmazott?

6.2.4. Rögzítenek-e minden, a felhasználók által bejelentett problémát?

6.2.5. Rendszeresen felülvizsgálják-e a súlyos, vagy sűrűn előforduló felhasználói problémákat?

6.2.6. Készítenek-e rendszeresen a vezetés részére statisztikákat a felmerült problémákról? Felhasználják-e ezeket az IT szolgáltatás minőségének javítására?

6.3. Adatbázis adminisztráció

Ez a rész a többfelhasználós adatbázisok adminisztrációjával foglalkozik. A felmérés célja, hogy az ellenőr megbizonyosodjon arról, hogy a többfelhasználós adatbázisokban tárolt adatok megbízhatóak, és rendelkezésre állnak az igényeknek megfelelően. (Az egy felhasználós adatbázisok – amelyeket csak egy bizonyos alkalmazás tud igénybe venni és egy felhasználóval – vizsgálata az alkalmazás kontrollok keretében elvégezhető.)

Az adatbázis egymással összefüggő adatelemek *strukturált* gyűjteménye. Egy adatbázis a legtöbb esetben több különböző alkalmazást is támogat. Az alkalmazások végezhetnek háttérfeldolgozásokat vagy működhetnek on-line, azaz interaktív üzemmódban (ezekről részletesen ld. a 6.6. pontot), illetve vegyesen. Az adatbázisoknak számos típusa létezik, de az ellenőr legnagyobb valószínűséggel a következőkel találkozhat:

- **relációs:** a relációs adatbázisban az adatelemek kétdimenziós táblákba, azaz relációkba vannak szervezve, amelyek sorokból és oszlopokból állnak. Egy sor egy rekordot alkot, míg az oszlopok az egyes rekordok adatelemeit jellemzik. Minden sor egyedileg is azonosítható egy vagy több oszlop értéke alapján. Az adatbázis egy "nézetét" (azaz egy, csak logikailag létrehozott relációját) egy vagy több tábla elemeiből lehet összeállítani. A relációs adatbázis ideális olyan helyzetekben, ahol a lekérdezés hatékonysága fontosabb, mint a feldolgozás teljesítménye;

- **hálós:** a hálós adatbázisban az adatelemek hierarchiába vannak rendezve: szülő, gyermek, unoka, stb. kapcsolatokba. Például egy *orvos*ra vonatkozó rekordhoz tartoznak a *beteg* alrekordok, amelyekhez egyenként hozzá lehet rendelni a *recept* alrekordokat. Ugyanakkor a hálós hierarchiának vannak módosulatai, ahol egy adatelemnek egynél több szülője is lehet, ha szükséges. Például egy *orvos*nak több *betege* is lehet, de emellett a gyengébb hierarchia esetében a hálós modell megengedi, hogy egy *beteg*nek is egynél több *orvos*a legyen. Az adatokat ily módon szövevényes útvonalakon és kapcsolatokon keresztül lehet elérni. Az ilyen típusú adatbázisokat nagy volumenű feldolgozások esetében alkalmazzák, mivel a relációs adatbázisoknál nagyobb teljesítményre képes. Ugyanakkor struktúrája sokkal merevebb, ami rugalmatlanabbá teszi.

Függetlenül attól, hogy az adatokat milyen módon szervezik adatbázisba, az adatbázis rendszer két alapvető komponensből áll, az adatbázisból és az adatbázis-kezelő rendszerből (DBMS: DataBase Management System):

- az **adatbázis** az adatok gyűjteménye, melyeket leggyakrabban a fentebb leírt módon szerveznek össze. A felhasználóknak nem kell szükségszerűen ismerniük minden, az adatbázisban tárolt információt, csak azokat, amelyeket az ő egyedi alkalmazása használ;

- a **DBMS** az a szoftver, amelynek segítségével az adatbázis kialakítható, programozható, működtethető és kezelhető.

Egy adatbázis kialakításával nagy mennyiségű szervezeti információ gyűjthető össze egy centralizált "adatraktárban", amelyet a felhasználók elérhetnek lekérdező nyelveken, táblázatkezelőkön és számos alkalmazói programon keresztül. Ennél fogva problémák merülhetnek fel az adatokhoz kapcsolódó tulajdonjoggal, a jogosultságokkal és a felelősségekkel kapcsolatban, és ez bonyolult helyzeteket eredményezhet. Az adatok megbízhatóságával kapcsolatban az egyik legfontosabb kérdés az, hogy kire kell ráruházni a tulajdonjogot: az adatok létrehozójára, azokra, akik az adatokat a legtöbbet használják, vagy aki felelős az adatok karbantartásáért? Egyes esetekben ezeket a nehézségeket politikai döntésekkel sem sikerül megoldani, és ez oda vezethet, hogy a tulajdonosok nem tisztázottak, és ebből kifolyólag gyenge a kontroll az adatok megbízhatósága fölött.

A probléma egyik megközelítése, hogy az adat szerzője lesz a tulajdonos, ő osztja ki és ha kell, vonja vissza a jogokat az adat elérésével, módosításával és törlésével kapcsola-

tosan. Egy másik megközelítés, amikor az adatbázis adminisztrátora lesz a "megbízott tulajdonos", és az adminisztrátorra bízzák a döntést, hogy az egyes felhasználók hogyan használhatják az adatbázist.

Függetlenül attól, hogy milyen megoldást alkalmaznak, jól definiált politikát és eljárásokat kell létrehozni annak érdekében, hogy:

- azonosítsák az adatokat és együttesen elfogadott meghatározást alakítsanak ki minden tételre;
- a tulajdonosi jogokat egy alkalmas tisztségviselőhöz rendeljék;
- azonosítsák a problémákat és megegyezést találjanak az érdekelt felek között;
- azonosítsák az adatbázis struktúráját érintő változásokat és ezt közös egyetértésben tegyék;
- kikényszerítsék az eljárások betartását.

Függetlenül attól, hogy a vizsgált szervezet milyen adattulajdonosi politikát folytat, nagyon fontos hogy kialakítsák a feladatkörök koordinációját. A hagyományos megoldás - ami a nagygépes rendszereket üzemeltető szervezetek esetében ma is jellemző - egy adatbázis adminisztrátor kinevezése, aki ellátja az adatbázis kezelésével kapcsolatos feladatokat. Az adminisztrátornak gyakran kell a szervezet különböző hivatali szintjein tevékenykednie, ezért megfelelő hatáskörrel kell rendelkeznie ahhoz, hogy a feladatkörét hatékonyan elláthassa. Egy nagyobb szervezetben ez a feladatkör lehet teljes munkaidős is egy saját csoport támogatásával.

Az adatbázis adminisztrátor alapvető feladatai:

- kialakítja a sztenderdeket az adatformátumokhoz, a hozzáférésekhez, felhasználói jogosultságokhoz, az elszámoltathatósághoz és az adatok elnevezéséhez;
- megoldja az egyes felhasználók közötti érdekellentéteket;
- biztosítja hogy az elfogadott felhasználói követelmények teljesüljenek;
- biztosítja a koordinációt a felhasználók és a rendszerfejlesztő csoport között az adatokra vonatkozó követelményekkel kapcsolatban;
- karbantartja az adatbázis struktúrájának és tartalmának átfogó integritását (*azaz az értékkészlet, az egyediség és a kapcsolatok integritását* - ld. a következő bekezdést);
- biztosítja hogy az adatbázist érintő minden módosítás, változtatás, struktúraváltozás valamint az alkalmazói rendszerek üzembeállítása zökkenőmentesen menjen végbe;

- biztosítja hogy a működésfolytonossági terv követelményeinek megfelelően az adatbázisról biztonsági mentések készüljenek, hogy ezen mentések alapján az adatbázist vissza lehessen állítani;

- kapcsolatot tart az adatbázis-kezelő rendszer szállítójával a problémás ügyekben, az adatbázis-kezelő rendszer új verzióit teszteli, valamint ezek üzembe helyezésekor a koordinálja feladatokat a változáskezelési kontrollrendszer alapján.

Az adatbázis adminisztrátor feladatai közül ki kell emelnünk az adatbázis átfogó integritásának biztosítását, fenntartását. Az adatbázis integritásának három fő szempontja:

- **értékkészlet integritása:** az értékkészlet azon értékek halmaza, amelyeket az adott adatelem felvehet (azaz a lehetséges értékek halmaza). Az értékkészletet centralizáltan határozzák meg, és ha egyszer meghatározták, akkor ennek betartását az adatbázis-kezelő rendszernek ki is kell kényszerítenie, és ezt tovább is kell örökítenie minden adatelemre mely azon a bizonyos értékkészleten alapul;

- **egyediség integritása:** azt követeli meg, hogy egy adatbázis-tábla minden sora egyedileg azonosítható legyen;

- **kapcsolati integritás:** talán az adatbázis integritás legfontosabb szempontja. Ez azt jelenti, hogy minden belső kapcsolat legyen érvényes, vagy más szavakkal az adatbázis ne tartalmazzon olyan adatelemeket, amelyek egy nem megfelelő vagy nem is létező elemhez kapcsolódnak. Például egy főkönyvi számla törlése esetén nem maradhatnak a számlára könyvelt tranzakciós tételek sem.

Az ellenőrnek ezért fel kell mérnie, hogy a szervezet hogyan biztosítja az adatbázis integritásának érdekében az értékkészlet, az egyediség és a kapcsolati integritás fenntartását, és ahol problémák merülnek föl, ezeket hogyan ismerik fel és javítják ki.

Néhány szállító olyan szoftvereket is biztosít, amely felismeri az adatbázis integritási hibáit, amikor egyes adatok megsérülnek. De ha ilyen eszköz nem áll rendelkezésre, akkor is lennie kell egy mechanizmusnak az adatbázis-kezelő rendszerben, amely jelenti az előforduló hibákat. Egy pénzügyi adatbázis integritási problémáinak felfedését sokszor a könyvelési rendszeren keresztül is meg lehet oldani úgy, hogy a számítógép által készített nyilvántartást összevetik olyan kontroll számlákkal, amelyeket külső intézmények kezelnek: erre példa a banki nyilvántartásokkal való összevetés.

További kontrollok, amiket az ellenőrnek az adatbázis adminisztrációval kapcsolatban meg kell vizsgálnia:

- **feladatkörök szétválasztása:** az adatbázis adminisztrátornak rendelkezésére állnak olyan szoftver eszközök, amelyekkel visszaállítható az adatbázis integritása, ha az adatok megsérülnek. Ezek az eszközök az alkalmazói rendszerek kontrolljain kívül működnek, ezért felhasználhatóak az adatok szabálytalan megváltoztatására is. A visszaélések kockázatának csökkentése érdekében biztosítani kell, hogy a felhaszná-

lók ne férhessenek hozzá olyan szolgáltatásokhoz vagy lekérdező nyelvekhez, amelyekkel az adatok úgy módosíthatóak, hogy kikerülik az alkalmazói rendszerek kontrolljait. Ugyanakkor az adatbázis adminisztrátor feladatát sem láthatja el olyan személy, aki részletesen ismeri a pénzügyi és egyéb érzékeny alkalmazásokat, vagy fizikai hozzáféréssel rendelkezik a megfelelő pénzügyi nyomtatványokhoz.

- **hozzáférés kontroll:** egy adatbázis gyakran több felhasználót és alkalmazást szolgál ki. Ha az adatok integritását érintően a felhasználók képesek kontrollálatlan döntéseket hozni, az növeli annak kockázatát, hogy az adatok megsérülnek, vagy nem megfelelően használják őket. Ezért ki kell jelölni egy alkalmas felhasználót, aki felelős az adat tulajdonlásáért, és az egyes felhasználók hozzáférésének engedélyezéséért. Ekkor az adatbázis adminisztrátor feladata az, hogy kialakítsa a hozzáférési lehetőségeket az adattulajdonos engedélyei alapján, valamint megalkossa a szervezet adattulajdonlási politikáját.

Kérdések a 6.3. ponthoz:

6.3.1. Milyen eljárások biztosítják, hogy a pénzügyi és egyéb érzékeny információkat tartalmazó adatbázisokban (továbbiakban csak adatbázisok) tárolt minden adat forrása, leírása és jelentése ismert legyen?

6.3.2. Milyen eljárások biztosítják, hogy ne jelenhessen meg olyan adat az adatbázisokban, amelynek nincs felelőse, azaz tulajdonosa?

6.3.3. Szabályozottak-e az adatbázis elemeihez való hozzáférések? Ki felelős a hozzáférés engedélyezéséért és a hozzáférési jogosultságok kialakításáért?

6.3.4. Milyen eljárások biztosítják, hogy az adatbázis és a hozzá kapcsolódó alkalmazói programok akkor is kompatibilisek maradjanak, ha valamelyik megváltozik?

6.3.5. Milyen eljárások biztosítják, ha bármely adat vagy a logikai adatbázis-struktúra megsérül, akkor azt azonnal felismerjék?

6.3.6. Milyen eljárások biztosítják, ha az adatbázis struktúráját, tartalmát vagy fizikai tárolását megváltoztatják, akkor az csak engedélyezett és kontrollált módon történhessen?

6.3.7. Milyen gyakorisággal végeznek biztonsági mentést az adatbázisokon? Megfelel-e ez a működésfolytonossági terv előírásainak?

6.3.8. Biztosított-e, hogy az adatbázisokat a mentés alapján bármikor vissza lehessen állítani?

6.4. Működtetési leírások alkalmazása

A leírások, útmutatók, kézikönyvek fontos szerepet játszanak az informatikai rendszerek működtetésében. A világos, használható működtetési leírások egyrészt biztosítják a számonkérhetőség alapját, másrészt pótolhatják a szakértelem hiányosságait, különösen amikor az alkalmazottak ritkán előforduló feladatot hajtanak végre (pl. egy év végi pénzügyi folyamatnál). Csökkenti a működés kockázatait akkor is, amikor egy kritikus fontosságú feladat végrehajtásához szükséges lépéseket (pl. kiemelt fontosságú rendszer újraindítása) előre meghatározott, szigorú sorrendben kell végrehajtani.

Működetési leírás szükséges minden informatikával kapcsolatos tevékenység támogatására, úgy mint a rendszerek elindítására vagy leállítására, a nagy tömegű adatfeldolgozásokra, rendszer meghibásodás vagy hibás tevékenység utáni helyreállításra. Útmutatások szükségesek a rutinszerű fenntartási tevékenységekre is, mint pl. biztonsági mentések végrehajtására, ill. az ez alapján történő helyreállításra, az eszközök karbantartására.

A felhasználói útmutatóknak átfogónak, megfelelő részletezettségűnek és megbízhatónak kell lenniük. Továbbá annak érdekében, hogy ilyenek is maradjanak, a működtetési leírások megfelelő helyet kell hogy kapjanak a változáskezelési eljárásokban is (ha pl. egy alkalmazás megváltozik, akkor ennek működtetési leírását is meg kell változtatni ld. III. 3. Konfiguráció- és változáskezelés).

Kérdések a 6.4. ponthoz:

6.4.1. Rendelkezik-e minden alapvető terület dokumentált működtetési leírással:

a) a jelentősebb rendszerek indítása és leállítása;

b) biztonsági mentés és visszaállítás;

c) a nagy tömegű adatfeldolgozások ütemezése, ezek kölcsönös függőségeinek leírása az egyéb rendszerekkel, az első feladat elkezdésének és az utolsó feladat befejezésének meghatározása;

d) hibák vagy egyéb kivételes esetek kezelése, amelyek a feladatok végrehajtása során felmerülhetnek;

e) a rendszer újraindítása és a visszaállítási folyamat lépései rendszerhiba esetén;

f) a speciális output-ok, nyomtatványok kezelési folyamatai, úgy mint a pénzügyi nyomtatványok kezelése, vagy a hibás output-ok biztonságos elkülönítése?

6.4.2. Hogyan biztosítja a vezetés, hogy a rendszerváltoztatások azonnal tükröződjenek a működtetési leírásokban is?

6.5. Vírusvédelmi intézkedések

A vírusok és egyéb hasonló rosszindulatú kódok (férgek, trójai falovak stb.) elleni *folyamatos* védekezés a számítógépes biztonság fenntartásának egyik fontos eleme. A vírusok fenyegetettséget jelentenek mindenfajta számítógépre nézve, ugyanakkor kártékony hatásuk széles skálán változik: léteznek ártalmatlan, viccelődős céllal készített vírusok, de gyakran felbukkannak olyanok is, amelyek teljes hálózatokat romba tudnak dönteni. Jelenleg az Interneten és levelező rendszerekben terjedő vírusok és férgek jelentik a legnagyobb kockázatot, nagyon gyorsan, 1-2 nap alatt világméretű fertőzöttséget képesek produkálni.

A pénzügyi adatok biztonsága szempontjából a nagy fenyegetettséget jelentő vírusok és férgek „működésének" hatásai a következők lehetnek:

– adatok, adatállományok rongálódnak, vagy semmisülnek meg;

– központi számítógépek túlterheltség miatt leállnak ;

– számítógépen tárolt információkat, adatokat (beleértve akár jelszavakat is!) elküldi egy meghatározott címre stb.

A vírusvédelmi intézkedések alapját egy jól meghatározott eljárásrend kell, hogy jelentse, amely egyértelműen kijelöli a hatás- és felelősségi köröket (a felhasználókra vonatkozóan is!), gondoskodik a folyamatos felügyeletről, az értesítésekről, a legfrissebb vírusvédelmi információk adaptálásáról és a vírusirtás módjáról. A szervezetnek ehhez az eljárásrendhez igazodva kell kiépítenie a védekezés technológiai megvalósítását, azaz a vírusfelismerő és vírusirtó rendszer kiépítését, illetve annak folyamatos karbantartását és működtetését.

A vírusvédelem legfontosabb feladata, hogy a fertőző kódokat és fertőzött állományokat a lehető leghamarabb felismerje, lehetőleg még azelőtt, hogy azok bejuthatnának a számítógépes rendszerbe és elkezdhetnék káros működésüket. Ennek feltétele egyrészt, hogy a rendszerbe kapcsolt számítógépek minden bemeneti csatornáját (Internet, floppy, CD meghajtó, USB stb.) *folyamatosan és automatikusan* ellenőrizze – lehetőleg úgy, ezt a védelmet a felhasználó ne is tudja kikerülni. Tovább csökkenti a kockázatot, ha a vírusfelderítő szoftver rendszeres időközönként végigvizsgálja a már rendszeren belül tárolt állományokat is.

A hatékony felderítés másik feltétele a vírusvédelem rendszeres frissítése, hiszen ez biztosítja azt, hogy a rendszer a bemeneti csatornákon egyáltalán felismerje a legújabb vírusokat. A vírusvédelem frissítését akár napi több esetben is el kell végezni, ha a rendszert üzemeltető személyzet magas fokú vírusaktivitásról szerez tudomást.

A leggondosabban kiépített vírusvédelem sem garantálhatja azonban, hogy nem kerül ilyen rosszindulatú program az informatikai rendszerbe, ezért fel kell készülni az esetleges károsodások utáni helyreállításra is. A működésfolytonossági intézkedések (lásd: III. 4. fejezet), illetve azon belül elsősorban a mentések biztosíthatják azt, hogy ha egy

vírusfertőzés és károkozás bekövetkezett, akkor a szervezet minél gyorsabban vissza tudjon állni egy előző, sértetlen állapotába. Ugyanakkor a visszaállításnál figyelni kell arra, hogy amíg a vírusvédelmi rendszer ki nem egészül a megfelelő frissítéssel, addig a szükséges folyamatok újraindítását olyan mértékben illetve olyan módon kell elvégezni, hogy a helyreállított működést egy újabb, ugyanolyan eredetű támadás már ne veszélyeztethesse.

Kérdések a 6.5. ponthoz:

6.5.1. Kialakította-e a szervezet a vírusvédelem eljárásrendjét?

6.5.2. Az eljárásrend egyértelműen meghatározza-e a vírusvédelmi rendszer kialakításának és *folyamatos* működtetésének feladat- és hatásköreit? Ezen belül meghatározott-e:

- A frissítések módja (Internetről, postán kapott lemezek stb.)?
- A frissítések rendszeressége?
- A frissítésért felelős személye és helyettesítése?
- A frissítések és egyéb vírusvédelmi változtatások naplózása?
- A vírusfertőzések kezelési eljárásai az illetékes rendszergazdák számára?
- A vírusfertőzésekkel kapcsolatos értesítési kötelezettségek a felhasználók számára?
- Egyéb felhasználói korlátozások és kötelezettségek (a vírusvédelem a munkaállomáson nem kapcsolható ki, rendszeres vírusellenőrzés végrehajtása, kívülről kapott adathordozók vizsgálata stb.)?

6.5.3. Rendelkezik-e a szervezet a vírusvédelmi szoftver rendszeres frissítésére vonatkozó licensz-szerződésel?

6.5.4. A vírusvédelmi rendszer kiterjed-e minden, az intézmény felügyelete alá tartozó számítástechnikai eszközre:

- A központi szerverekre?
- A hálózatba kötött munkaállomásokra?
- A hálózatba nem kötött munkaállomásokra?
- A hordozható számítógépekre?
- A tűzfal(ak)ra?

6.5.5. Folyamatos és automatikus-e az informatikai rendszer bemeneti csatornáin a vírusellenőrzés:

- A levelező rendszerben?

- A munkaállomásokhoz használt hordozható adattárolók (pen-drive, mobil winchester, CD, floppy stb.) minden csatlakoztatása illetve behelyezése alkalmával?

6.5.6. A felhasználó ki tudja-e kapcsolni a saját, hálózatba kötött munkaállomásának automatikus vírusvédelmét?

6.6. Adatbevitel (input)

Az adatbeviteli kontrollok célja, hogy a feldolgozás céljából rögzített adatok érvényesek, teljesek és pontosak legyenek. A következőkben bemutatásra kerülő kontrollokat elsősorban olyan szervezeteknek kell *részleteiben* is alkalmazniuk, amelyek nagy tömegű adatot rögzítenek és dolgoznak fel, ugyanakkor az alapvető - adatbevitelhez kapcsolódó - szabályozásokat minden intézménynél életbe kell léptetni.

Az informatikai rendszerek által feldolgozandó adatok két formában juthatnak a rendszerbe: elektronikus úton, vagy a papíron beérkező információkat rögzítve.

Az elektronikus formára példák azok a tranzakciók melyek az EDI-n (electronic data interchange) keresztül, fájl-transzferrel vagy elektronikus kereskedelmi rendszerrel ("e-commerce") érkeznek. Ezek aránya a közigazgatásban – részben a jogszabályi rendelkezések hiánya miatt – ma még nem jelentős, ezért módszertanunkban az ehhez kapcsolódó kontrollokat nem tárgyaljuk.

Ahol a tranzakciók papír alapúak, a felhasználók általában a munkaállomásokon keresztül közvetlenül gépelik be az adatokat a rendszerbe. Az adatbevitel ezen formája a számítógépes alkalmazói rendszerek képernyőképein keresztül történik. A következőkben csak ezen tevékenységek szabályozására koncentrál a módszertan.

Tömeges adatbevitelnél esetén, amikor nagy mennyiségű papír alapú dokumentumot kell elektronikus formába konvertálni, az alábbi eljárások valamelyikét alkalmazzák:

- begépelés manuálisan;
- a karakterfelismerő eszközök és eljárások alkalmazása (pl. optikai, mágneses);
- a dokumentumok elektronikus képként való bevitele dokumentum szkenner segítségével.

A nagy nyilvántartásokkal rendelkező szervezetekben a tömeges adatkonverziót általában egy erre elkülönített csoport végzi. A csoport feladata, hogy a papír alapú adatokat elektronikus formájúvá alakítsa át, és az eredményként keletkezett fájlt tovább adja feldolgozásra a megfelelő alkalmazói rendszereknek. A kontrolloknak mindenképpen biztosítaniuk kell, hogy a feladatot teljesen és pontosan végrehajtsák, és a bevitt adatokon ne hajtsanak végre szabálytalan változtatást. A gyakorlat azt mutatja, hogy a számítógé-

pes rendszerekben a leggyakoribb hibázási vagy csalási lehetőség az adatbevitel közben van, ahol az adatok:

- elveszhetnek vagy teljességük csorbulhat;
- duplikáltak (kétszer rögzítettek) lehetnek;
- szabálytalanok vagy fiktívek lehetnek;
- a beviteli folyamat közben manipulálhatják őket;
- engedély nélkül közbeiktathatnak (akár véletlenül, akár szándékosan) egyéb adatokat.

Az ellenőrnek három szempontból kell megnéznie az adatbevitelhez kapcsolódó kontrollokat:

- a folyamat legyen dokumentálva;
- legyen megfelelő eljárás az input formátumok kezelésére; és
- a feldolgozás céljából a rendszerbe bevitt adatokat először ellenőrizzék a hibák és kihagyások szempontjából.

Az alkalmazói rendszereknek, amelyek a rögzített adatokat megkapják, természetesen további teszteket kell majd végrehajtaniuk, mint például: duplikáció, hézagok, vagy a számlákkal nem összeegyeztethető tranzakciók vizsgálata.

Hasonlóan a többi eljáráshoz, az adatkonverzióhoz használt eljárást is dokumentálni kell. Ez nagyon fontos annak biztosításához, hogy mindenki egyformán értelmezze a rendszert, hogy útmutatót nyújtson az új alkalmazottaknak, és hogy hivatkozási alapot teremtsen a dolgozóknak és ellenőröknek. A dokumentációban lépésről lépésre le kell fektetni az adatok útját, az alkalmazott eljárást, valamint hogy ki a felelős az egyes fokozatokban.

Ahol lehetséges, a papír alapú inputokat - kontroll célból - kötegelni kell, és egy "köteg kontroll címkét" vagy ("köteg fejlécet") kell rá készíteni. *Minél előbb alkalmazzák a köteg-kontrollt a folyamatban, annál kisebb eséllyel vesznek el dokumentumok, vagy kerülnek közéjük oda nem illők vagy szabálytalanok.* A "köteg kontroll címke" jellemzően a következőket tartalmazza:

- egy egyedi, köteg-sorszám (azonosítandó a feldolgozás alapegységét);
- dátum, a rendszer neve és a tranzakció típusa;
- a kötegben található dokumentumok száma és az ellenőrző összeg;

- a köteg feladójának aláírása, és azok további aláírásai akik azután kezelik.

A feldolgozási folyamat teljes hosszában minden köteg esetében meg kell tartani az input dokumentumokat a saját kötegében, és a kötegek ellenőrző összegét a feldolgozás minden fázisában rögzíteni és ellenőrizni kell az ellenőrzési nyomvonal biztosítása céljából.

A sikeres feldolgozás után a kötegeket érvényteleníteni kell (pl. bélyegzéssel vagy átlyukasztással), hogy csökkenjen a duplikált feldolgozás kockázata, majd a kötegeket iktatni kell.

Ahol nem működnek kötegelési kontrollok, az ellenőrnek meg kell nézni a kompenzáló kontrollokat, amelyek az input teljességét és pontosságát biztosítják. Ilyen lehet például az input dokumentumok és a rendszer által elfogadott adatok folyamatos összehasonlítása.

Az adatbevitel folyamatába célszerű beiktatni olyan, a felhasználói rendszerbe épített kontrollokat, amelyek segítségével felfedezhetőek a hiányzó vagy hibás tételek. Az érvényesítési ellenőrzés során jellemzően a következőket alkalmazzák (adattípustól függ, hogy melyiket vagy melyeket):

- **számjegyek ellenőrzése:** egy külön karaktert csatolnak az adatelemhez, mely matematikailag kapcsolódik a karaktersorozathoz, s ennek segítségével a további használat során felfedezhetőek például az elütéses hibák;

- **tartományi vagy korlát vizsgálat:** bizonyos tételek ellenőrzése annak szempontjából, hogy elfogadható korlátok közé esnek-e;

- **formátum ellenőrzés:** annak ellenőrzése, hogy a tétel a megkívánt formátumban van-e, pl. csak betűket vagy csak számokat tartalmaz-e;

- **túlcsordulás:** biztosítja hogy az adat nem lesz hibás egy olyan számítás után, amely túl nagy számot eredményezne és nem férne el az eredmény mezőben;

- **teljesség:** minden kitöltendő mezőt kitöltöttek;

- **kompatibilitás:** minden, egymással összefüggő mezőben logikusan összefüggő adatok vannak;

- **duplikáció:** annak biztosítása, hogy a tételt még nem dolgozták fel.

A beviteli folyamatnak ellenőriznie kell, hogy a köteg címkéje kontrollál, azaz az operátor által rögzített köteg-címke adatai megegyeznek a feldolgozott dokumentumok számával, és a megfelelő kontroll mezők aggregált összegével. Azon rögzített dokumentumokat, amelyeket a rendszer visszautasított, vissza kell utalni a feladóhoz korrekcióra, és a köteg ellenőrző címkéjét a változásoknak megfelelően meg kell változtatni, és szig-

nálni kell. A javított tételeket a szokásos kötegelési folyamat alapján újból fel kell dolgozni.

Kérdések a 6.6. ponthoz:

6.6.1. Léteznek-e dokumentált eljárásrendek az adatok rögzítéséhez?

6.6.2. Milyen eljárást alkalmaznak az input formátumok (formanyomtatványok, bizonylatok stb.) rögzítésére?

6.6.3. Milyen eljárások azonosítják a hiányzó, hiányos és inkonzisztens adatokat?

6.6.4. Milyen eljárások biztosítják, hogy a konverzió alatt az adatok védettek legyenek a szabálytalan változtatástól?

6.6.5. Milyen eljárások biztosítják, hogy minden adat pontosan és teljesen kerüljön rögzítésre?

6.6.6. Milyen céllal és milyen eljárásokkal tesztelik az adatokat rögzítés után?

6.7. Pénzügyi nyomtatványok kezelése

A kontrollok célja, hogy biztosítsák az értékkel bíró pénzügyi nyomtatványok biztonságos és elszámoltatható kezelését.

Az ellenőrnek meg kell vizsgálnia, hogy a szervezet milyen típusú előre készített számítógépes nyomtatványokat alkalmaz, és fel kell mérnie ezek sebezhetőségét lopás vagy csalás szempontjából. Értékkel bíró pénzügyi nyomtatványokra kézenfekvő példák a csekkek vagy utalványok, de vannak körülmények amelyek között a licenceket és engedélyeket is védeni kell. Általában az értékkel bíró nyomtatványok használatát az alábbi fő szempontok szerint kell kontrollálni:

– biztonságos fizikai tárolás;

– készlet ellenőrzés;

– a kibocsátott, kinyomtatott és törölt nyomtatványok számának felügyelete.

Űrlapokra nyomtatáskor gyakran megtörténik, hogy az adatok elcsúsznak, vagy olvashatatlanok lesznek, azaz a kitöltött űrlap selejtes lesz. Ezeket az elrontott nyomtatványokat ugyanúgy mint a nyugtákat és okmányokat felül kell bélyegezni, nyilván kell tartani és el kell velük számolni. A nyilvántartásokat rendszeresen ellenőriznie kell egy olyan személynek, aki nem felelős a nyomtatványok kibocsátásáért.

Kérdések a 6.7. ponthoz:

6.7.1. Előállítanak-e az informatikai eszközök olyan számítógépes nyomtatványformákat, amelyek önmagukban is értékkel bírnak és védelmet igényelnek?

6.7.2. Alkalmaznak-e dokumentált eljárásrendet az értékkel bíró nyomtatványok kezelésére?

6.7.3. Hogyan biztosítja a vezetés, hogy az értékkel bíró nyomtatványokat ne lehessen meghamisítani vagy ellopni?

6.8. A számítógépes output

A számítógépes output kontrollok célja, hogy a számítógépes rendszerek által rendelkezésre bocsátott bármely adat és információ teljes és pontos legyen, továbbá azok és csakis azok kaphassák meg ezeket az információkat, akiknek ez munkájához szükséges.

A számítógépes outputoknak számos formája lehetséges: kinyomtatott jelentések, mikrokártyák, optikai és mágneses fájlok, képernyős outputok, kommunikációs hálózatok közötti adattovábbítás, stb. Emiatt a különböző outputhoz különböző eredendő kockázatok is tartoznak. Egy output lehet pontatlan, hiányos, vagy készülhet szabálytalan módon. A számítógépes outputtal számos módon lehet visszaélni:

◊ csalás szándékával készpénzre váltható eszközök kibocsátása;

◊ egy értesítés eltussolása (pl. eladási számla);

◊ szabálytalanul lemásolt bizalmas jelentések megszerzése;

◊ output dokumentumokat ellophatnak vagy megsemmisíthetnek;

◊ output dokumentumokat megváltoztatnak.

Az ellenőr által megvizsgálandó alapvető output-kontroll cél az, hogy a szervezet hogyan biztosítja, hogy a feldolgozás és az ehhez tartozó output:

- pontos; és
- teljes legyen;
- valamint engedélyezett és tesztelt alkalmazói programok állítsák elő.

A számítógépes output-okat tehát kibocsátás előtt ellenőrizni kell annak biztosítása érdekében, hogy azokat engedélyezett program állítsa elő, az adatok teljesek és pontosak legyenek, továbbá nem elhanyagolható szempont a megfelelő minőség sem (pl. egy

nyomtatvány jól olvasható-e). Ahol nagyobb mértékű feldolgozási tevékenységet végeznek és nagy számítógépes parkkal rendelkeznek, ott egy elkülönült output kontroll részleg is végezheti ezt a tevékenységet egy megfelelő működtetési útmutató segítségével. A működtetési útmutatónak az említett szabályozásokon túl azt is meg kell határoznia, hogyan kell reagálni az esetlegesen keletkező hibaüzenetekre és rendellenességekre.

Az érzékeny vagy kritikus információkat tartalmazó nyomtatvány és jelentés esetében azokat oldalszámozással kell ellátni, és egy megfelelő üzenettel kell végződniük, jelezvén hogy teljesek. Olyan esetben, amikor automatikus jelentés készül, de nem jelenik meg rajta feljegyzés, az alkalmazásnak akkor is rá kell nyomtatnia egy 'nincs adat' sort jelezvén, hogy a program nem hibásodott meg, vagy a jelentés nem veszett el, csak nem tartalmaz információt.

A feldolgozás pontossága és teljessége szempontjából a leggyakrabban használt kontroll az output-ok és input-ok átfogó összevetése. Ezt az összevetést elvégezhetik a felhasználók is, amely esetben – megkönnyítendő az összevetést – ellenőrző összesítéseket kell készíteni az outputhoz legalább olyan mértékben, hogy bizonyítható legyen hogy minden input-ot teljes mértékben és pontosan feldolgoztak.

Értéktől és érzékenységtől függően a számítógépes output-okat a kiadásig biztonságosan kell tárolni. Részletesen ki kell dolgozni, hogy ki kaphat kézhez bizonyos output-okat, és minden egyéb speciális követelményt fel kell tüntetni a működtetési utasításokban.

Összefoglalásul, ha nem megfelelő a kontroll a számítógépes outputok felett, az növeli annak kockázatát, hogy:

- csalás történik (pl. lopás, pénzügyi eszközök duplikálása vagy módosítása);
- a szervezet működésében zavarok keletkeznek (a felhasználandó output-okat nem osztják ki a megfelelő helyekre vagy megfelelő időben);
- helytelen vezetői döntések születnek a hiányos output-ok alapján;
- érzékeny szervezeti vagy személyes adatok kerülnek nyilvánosságra.

Kérdések a 6.8. ponthoz:

6.8.1. Létezik-e szervezeti politika a pénzügyi és egyéb érzékeny adatokat feldolgozó rendszerek outputjainak kezelésére?

6.8.2. Dokumentált-e a felhasználók számára, hogy az egyes rendszerek milyen output-ot szolgáltathatnak (típus, forma, tartalom)?

6.8.3. Milyen eljárások biztosítják, hogy a hiányos vagy pontatlan output-okat a felhasználók felismerjék?

6.8.4. Létezik-e dokumentált eljárásrend a hiányos vagy a pontatlan output-ok kezelésének folyamatára?

6.8.5. Milyen eljárások akadályozzák meg az output-ok duplikált kibocsátását?

6.8.6. Milyen eljárások biztosítják, hogy az output-okat csak az arra engedélyezett felhasználók kapják meg?

6.8.7. Milyen eljárások biztosítják, hogy a kibocsátott output-okat - értéküknek vagy érzékenységüknek megfelelően - biztonságosan tárolják?

IV. Az alkalmazás-kontrollok felmérése

Bevezetés

Az alkalmazások olyan egy vagy több számítógépes programból álló szoftverek vagy szoftver csomagok, melyek a szervezet működési feladatait támogatják. Az alkalmazásokat fejleszthetik speciálisan egy szervezet részére (ide soroljuk a testreszabott rendszereket is), vagy megvehetőek készen is ("polcról"), különböző szállítóktól.

A leggyakoribb készen beszerezhető szoftverek, melyekkel a pénzügyi ellenőrök találkozhatnak a következők:

- integrált pénzügyi, számviteli csomagok;
- bérszámfejtési / személyzeti / TB rendszerek;
- tárgyi eszköz nyilvántartások.

A testreszabott rendszerek kifejlesztésére olyan esetekben kerül sor, amikor a piacon csak kevés tárgykörbe tartozó termék található, vagy egy sem. Testreszabott rendszereket általában még csak a nagyobb közigazgatási intézmények használnak.

Minden pénzügyi alkalmazásnak rendelkeznie kell kontrollokkal, melyek biztosítják az sértetlenséget, a rendelkezésre állást, valamint korlátozott mértékben mind a tranzakciók mind a törzsadatok bizalmasságát. Azonban az ellenőr nem várhatja el az alkalmazásoktól, hogy minden elképzelhető kontrollal rendelkezzen minden szinten. A szervezeteknek minden alkalmazásra ki kell értékelniük a kockázatokat, és megfelelő, költséghatékony kontrollokat kell kialakítania annak érdekében, hogy ezen kockázatokat egy elfogadható szintre szorítsák. Ezt a költséghatékonysági elvet nem szabad figyelmen kívül hagyni, amikor különböző fejlesztéseket javasolunk a vizsgált szervezetnek!

Az alkalmazás-kontrollok felmérése:

a) az ellenőrzött szervezet számítógépes rendszerének ismeretére épít, amelynek módszerét az I. és II. fejezet tartalmazza;

b) a pénzügyi ellenőr számára azonosíthatóvá, dokumentálhatóvá és kiértékelhetővé teszi a pénzügyi alkalmazásokhoz kapcsolódó kontrollokat és eljárásokat;

c) az ellenőr számára kiértékelhetővé teszi az egyes alkalmazásokhoz kapcsolódó átfogó kockázatot;

d) azonosítja azokat a sajátos kockázatokat, melyek befolyásolhatják mind a megfelelőségi, mind a szubsztantív ellenőrzési eljárások tervezését.

Az alábbi kontroll felmérések egy-egy alkalmazásra, önállóan kezelendők, ezért **a következő felméréseket minden egyes pénzügyi-számviteli alkalmazásra el kel végezni!**

1. A számítógépes pénzügyi alkalmazás megismerése

Az ellenőrnek meg kell értenie a lehetséges tranzakciók minden útvonalát, mely a külső környezettől egészen a szervezet pénzügyi beszámolójáig terjed. Egy adott tranzakciós folyamnak az IT rendszerek rendszerint egy részét alkotják. Az ellenőrzési dokumentációt ezért úgy kell elkészíteni, hogy lehetővé tegye a tranzakciók nyomon követését a kiindulástól, az IT rendszereken keresztül egészen a pénzügyi beszámolók összefoglalójáig.

Egy alkalmazás áttekintése keretében az ellenőrnek azonosítania és dokumentálnia kell minden számítógépes hardvert és kapcsolódó IT környezetet, mely részt vesz a pénzügyi jelentéshez köthető adatbevitelben, feldolgozásban, (adat)tárolásban vagy output készítésben. A dokumentációnak azonosítania kell továbbá minden olyan egyéb IT alkalmazást, mely adatokat továbbít a pénzügyi beszámolókhoz. Az ellenőrnek dokumentálnia kell minden jelentős pénzügyi alkalmazást vagy folyamatábra formájában, vagy szavakban megfogalmazva:

- az irodai és az IT működés közötti felület (interfész), kapcsolat;
- IT berendezések és alkalmazások, melyek közreműködnek az ellenőrzött pénzügyi jelentés elkészítésében;
- a feldolgozott tranzakciók volumene és értéke minden alkalmazásra;
- a vonatkozó rendszerek beviteli, feldolgozási, output és tárolási elemei; valamint
- adatfolyamok a tranzakció kiindulópontjától az ellenőrzött pénzügyi beszámolókig.

Ha IT szakellenőr is közreműködik az ellenőrzésben, akkor az alkalmazás kontroll folyamatok áttekintését a szervezet számviteli rendszerét legjobban ismerő szakági (pénzügyi, számviteli) ellenőrrel együttműködve kell elvégezni. Ez biztosítja azt, hogy az áttekintés során nem marad figyelmen kívül a manuális és egyéb kompenzáló kontrollok megléte és hatékonysága sem. A szakági ellenőr jelenléte lehetővé teszi továbbá az IT ellenőr számára, hogy gyorsabban megértse a rendszert, és csak a különösen kockázatos területekre kelljen koncentrálnia.

A pénzügyi szoftver-iparág fejlődésének eredményeként széles körben elterjedtek az integrált számviteli csomagok, melyek képesek a különböző típusú tranzakciók végrehajtására is. A szervezet így üzembe állíthat olyan pénzügyi alkalmazásokat, melyek kezelik a bevételi és kiadási tranzakciókat, a havi bérfeladást, munkaköltség számítást és tárgyi eszköz nyilvántartást is. Ily módon lehetséges, hogy egy alkalmazás számos különböző számviteli terület számára hajt végre tranzakciókat.

A számviteli területek meghatározása után az ellenőrnek azonosítania kell a főbb tranzakció folyamokat mindegyik alkalmazáson belül. Az ellenőrnek minden egyes folyamaton belül ki kell értékelni az ellenőrzési kockázat mértékét az alábbi három faktor segítségével:

a) a pénzügyi információk sértetlenségének és rendelkezésre állásának **fenyegetettsége**;

b) a pénzügyi információk **sebezhetősége** az azonosított fenyegetettség alapján; valamint

c) lehetséges **hatások** az ellenőrzési célok tekintetében.

Kérdések az 1. ponthoz:

Az alkalmazások megismerését az I. fejezet 1.2. kérdőívei segítik.

2. Ellenőrizhetőség

A számítógépes alkalmazásnak képesnek kell lennie arra, hogy azonosítsa, melyik felhasználó mit csinált és mikor. Ha a felhasználókat azonosítani lehet, és meg lehet állapítani milyen műveleteket végeztek, akkor sokkal kisebb az esélye annak, hogy szabálytalan vagy illetéktelen tevékenységet hajtanak végre. Az elszámoltathatóságot olyan kontrollokkal lehet biztosítani, melyek összefüggésbe tudják hozni a felhasználókat az egyes műveletekkel, és ezeket az információkat el is tudják tárolni egy ellenőrzési naplóba.

A felhasználói tevékenységek naplózása önmagában nem elegendő ahhoz, hogy a szabálytalan vagy illetéktelen tevékenységek kockázata csökkenjen. A vezetésnek rendszeres időközönként át kell tekintenie a napló (ellenőrzési nyomvonal) alapján elkészített jelentést a szokásostól eltérő eseményekről, és ha kiugró vagy kivételes eseteket tapasztalnak, meg kell tenni a szükséges lépéseket.

A naplók akkor megbízhatóak, ha azokat nem lehet megváltoztatni. Megfelelő kontrollokat kell kialakítani annak biztosítására, hogy a dolgozók, akik betáplálják vagy végrehajtják a tranzakciókat, a saját tevékenységük naplóját ne tudják megváltoztatni. Az ellenőrzési napló sértetlensége biztosítható titkosítással, vagy ha a naplóról másolat készül egy védett könyvtárba vagy fájlba.

Bármely pénzügyi számviteli rendszer ellenőrizhetősége attól függ, hogy létezik-e elegendő és megfelelő ellenőrzési bizonyíték. Ahhoz, hogy a számítógépes rendszer ellenőrizhető pénzügyi beszámolókat készítsen, a következőket kell teljesíteni:

- a tranzakciós rekordokat eltárolják, és azok teljesek legyenek az egész beszámolási időszakra;
- a tranzakciós rekordok elegendő információt tartalmazzanak az ellenőrzési nyomvonal kialakításához; valamint
- a tranzakciós végösszegek összeegyeztethetőek legyenek a pénzügyi beszámolókkal.

Ha ezen feltételek bármelyike hiányzik, akkor az ellenőrnek döntenie kell, hogy a számítógépes rendszer megfelelő-e ahhoz, hogy a pénzügyi beszámolók alapjául szolgáljon. Ilyen körülmények között az ellenőrnek mérlegelnie kell azt is, hogy milyen lépések szükségesek a probléma kijavításához. Az ellenőrnek ki kell derítenie, hogy vannak-e alternatív, nem számítógépes számviteli rekordok, és lehetséges-e a számítógépes rendszer környezetében végrehajtani az ellenőrzést.

Kérdések a 2. ponthoz:

2.1 Az alkalmazás részletes áttekintése előtt az ellenőrnek meg kell vizsgálnia, hogy az alkalmazói rendszer ellenőrizhető-e. Az ellenőrnek meg kell győződnie az alábbiak meglétéről:

- Teljes tranzakciós rekordok az egész beszámolási időszakra vonatkozóan.
- Ellenőrzési nyomvonal.

Az ellenőr nem tud elegendő, vonatkozó és megbízható ellenőrzési bizonyítékot összegyűjteni, ha a rekordok nem teljesek, vagy ha az ellenőrzési nyomvonal nem megfelelő. Ilyen körülmények mellett az ellenőrnek a számítógépes rendszeren kívül is kell vizsgálódnia.

3. Számítógéppel segített ellenőrzési technikák (CAAT) használata

Az ellenőr megvizsgálhatja annak lehetőségét, hogy használjon-e számítógéppel támogatott ellenőrzési technikákat az ellenőrzési bizonyíték megszerzésére, mint pl. az IDEA. Ha szándékozik, célszerű IDEA szakértőkkel is konzultálnia.

Kérdések a 3. ponthoz:

3.1 Előállít-e az alkalmazás olyan pénzügyi adatokat, melyeket CAAT-tal vizsgálni lehet? Elő tudja-e állítani a program az egész beszámolási időszakra vonatkozóan a tranzakciós adatokat?

3.2 Letölthetőek-e a szükséges adatok használható formátumban, hogy azt egy ellenőrzést segítő szoftverrel kezelni lehessen (pl. IDEA)?

3.3 Összeegyeztethetőek-e a mintavételezett adatok a főkönyvvel, a próbamérleggel és a pénzügyi beszámolóval?

3.4 Van-e az alkalmazásnak beépített ellenőrzési modulja? Ha igen, akkor ezt fel tudja-e használni a külső ellenőrzés az ellenőrzési bizonyítékok megszerzésére?

4. Alkalmazás dokumentációja

A dokumentációs kontrollok célja, hogy naprakész és megfelelő alkalmazói rendszerdokumentáció álljon a felhasználók és az informatikai dolgozók rendelkezésére. A megfelelő dokumentáció az alábbi előnyökkel jár:

- csökken annak kockázata, hogy az alkalmazottak hibákat követnek el;
- elősegíti a munkavégzéssel párhuzamos képzéseket;
- megkönnyíti a szoftver karbantartását és fejlesztését;
- segíti az ellenőrt, hogy megértse a rendszert.

Az alkalmazások megfelelő dokumentáltsága csökkenti annak kockázatát, hogy a felhasználók hibákat követnek el, vagy túllépik hatáskörüket. Átfogó és aktualizált dokumentáció áttekintésével az ellenőr megértheti az egyes alkalmazások működését, és egyben segít azonosítani bizonyos ellenőrzési kockázatokat. A dokumentációnak tartalmaznia kell:

- egy rendszer áttekintést;
- felhasználói követelmény specifikációt;
- program specifikációt;
- input/output specifikációt;
- a fájlok tartalmának specifikációját;
- felhasználói kézikönyvet; valamint
- instrukciókat hibák, vagy kivételes események kezelésére.

Kérdések a 4. ponthoz:

4.1 Megfelelő-e az alkalmazás dokumentációja? Átfogó és naprakész-e? Tartalmazza-e:

- A rendszer áttekintését?
- A program leírását, specifikációját?
- Input/output leírását, specifikációját?
- Adatbázis/adatszótár leírását, specifikációját?

- A kontroll eljárásokat?

A nem megfelelő dokumentáció növeli a hibázások kockázatát. Továbbá növeli annak kockázatát is, hogy az alkalmazás nem az igényeknek megfelelően fogja a feldolgozásokat elvégezni.

4.2 Megkapják-e a vonatkozó dokumentációkat azok az alkalmazottak, akiknek ez szükséges?

A rendszer állandó használóinak dokumentációt kell rendelkezésre bocsátani. A dokumentációnak például nem sok haszna van, ha az a Pénzügyi Osztály könyvszekrényében van elzárva.

4.3 Milyen útmutatók állnak rendelkezésre a rendszeres felhasználóknak, ha problémákba ütköznek?

A szabvány "gyári" kézikönyvek sokszor nem felhasználó-orientáltak. Ezért célszerű ilyen célra egy speciális útmutatót is készíteni.

4.4 Van-e biztonsági másolat a rendszer-dokumentációról, egy esetleges katasztrófa utáni program-visszaállítás esetére?

5. Alkalmazás biztonság: fizikai és logikai hozzáférés

A hozzáférési kontrollok célja, hogy biztosítsák az input és tárolt adatok, valamint a feldolgozási eredmények bizalmasságát, sértetlenségét és rendelkezésre állását. Az alkalmazási szintű hozzáférés kontrollok vizsgálata támogatja az általános IT környezet hozzáférés kontrolljainak átfogó értékelését (II. fejezet 2. pont) is. A megfelelő alkalmazás kontrollok elősegítik:

- A tranzakciók és a tárolt adatok sértetlenségének biztosítását azáltal, hogy csak az arra felhatalmazott felhasználóknak biztosít hozzáférést bizonyos alkalmazási funkciókhoz és adatokhoz.

- Kikényszeríti a feladatkörök szétválasztását azáltal, hogy különböző jogosultsági szinteket és menüket biztosít az egyes felhasználók számára.

- A felhasználók számonkérhetőségét megoldja azáltal, hogy naplózza azonosítójukat és a hozzájuk rendelt műveleteket.

Az általános IT kontroll környezet felmérésével az ellenőr megismerte a számítógépekre vonatkozó általános hozzáférés kontrollokat addig a pontig, hogy a felhasználó kiválaszt egy alkalmazást. Az alkalmazás-biztonság áttekintése folyamán egy lépéssel tovább kell tekinteni a kontrollokat, és azt kell vizsgálni, hogy azon felhasználók, akik hozzáférnek az alkalmazáshoz, hogyan vannak kontrollálva. Például: egy pénzügyi osztály minden dolgozója - az általános kontrollokon keresztül - hozzáfér az on-line pénzügyi alkalmazáshoz. Ezután már az alkalmazáson belüli további hozzáférés kontrollok szabályozzák, ki érheti el az eladási főkönyvet, a beszerzési főkönyvet, a jelentésírást, a bérszámfejtési modult, stb.

Kérdések az 5. ponthoz:

5.1 Milyen fizikai kontrollokat alkalmaznak annak érdekében, hogy illetéktelenek ne férjenek hozzá a terminálokhoz?

A nem megfelelő fizikai kontrollok növelik a hardver rongálás / sérülés, lopás és a pénzügyi adatokhoz való illetéktelen hozzáférés kockázatát.

5.2 Milyen logikai hozzáférés kontrollokat alkalmaznak annak érdekében, hogy ezen alkalmazáshoz való hozzáférést korlátozzák?

- Alkalmazás-specifikus bejelentkezés (azonosító) és jelszó.

- Felhasználótól függő, korlátozott menük alkalmazása a programban.

- Felhasználói profile-ok alkalmazása.

- Engedélyezési eljárások alkalmazása minden felhasználó esetében.

A jól megtervezett logikai hozzáférés kontrollok csökkentik az illetéktelen hozzáférés, adatváltoztatás és törlés kockázatát. A logikai hozzáférés kontrollok kikényszeríthetik továbbá a feladatkörök szétválasztását is.

5.3 Létezik-e a szervezetnél naprakész lista az engedéllyel rendelkező felhasználókról? Tartalmazza-e ez a jogosultságokat is?

Ha a felhasználókról vezetett listák nem naprakészek, akkor nő annak kockázata, hogy az alkalmazottak hozzáférési jogosultsága túllépi a munkájuk által megkívánt mértéket.

5.4 Milyen logikai kontrollok korlátozzák a felhasználók tevékenységét azután, hogy hozzáférést kapott az alkalmazáshoz? Pl. korlátozott menü-hozzáférés.

Az alkalmazáson belüli kontrollálatlan hozzáférés kihasználható a feladatkörök átlépésére. A korlátlan hozzáférés növeli továbbá annak kockázatát, hogy a felhasználók hibákat követnek el.

5.5 Milyen eljárással vesznek fel, ill. törölnek felhasználókat? Ki adminisztrálja a felhasználókat, és az adminisztrátorokat hogyan kontrollálják?

A nem megfelelő eljárások növelik annak kockázatát, hogy illetéktelen felhasználó fér hozzá az alkalmazáshoz. Pl. ha nem megfelelő az összhang az alkalmazottak és az alkalmazás adminisztrátora között, akkor lehetnek olyan már elküldött és elégedetlen dolgozók, akik megtartják - immár illetéktelen - hozzáférésüket.

5.6 Milyen kontrollok működnek az alkalmazáson belül azért, hogy azonosítani lehessen az egyes felhasználók tevékenységeit?

- Egyedi felhasználói azonosítók használata
- Naplózás (ellenőrzési nyomvonal)
- Elektronikus aláírás alkalmazása

Ha a felhasználók egyenként azonosíthatóak és elszámoltathatóak a tevékenységeikért, akkor kisebb valószínűséggel követnek el hibákat vagy hajtanak végre jogosulatlan műveleteket.

5.7 Milyen módon tekintik át az egyes felhasználók műveleteit? Például a vezetés megnézi a naplózás (ellenőrzési nyomvonal) eredményeit?

A felhasználói tevékenység naplózása csak akkor lehet eredményes, ha azt a vezetés rendszeresen áttekinti. Nincs értelme a naplózásnak akkor, ha a feltárt eltérésekről nem készül jelentés és nem teszik meg a szükséges lépéseket.

5.8 A naplózás eredményét megfelelően védik az illetéktelen változtatástól?

- A napló titkosítása
- Írásvédett napló
- A napló védett könyvtárban való tárolása

A vezetés csak akkor tekintheti megbízhatónak az ellenőrzési jelentést (a naplózásról), ha az megfelelően védett az illetéktelen másolás ellen. A védelem elérhető titkosítással, vagy azáltal, hogy a naplót egy védett könyvtárban tárolják.

6. Input kontrollok

Az input kontrollok célja, hogy biztosítsa a rendszerbe bevitt adatok pontosságát, teljességét és ellenőrzöttségét. Az input adatok kontrollja a manuális és az alkalmazásba beépített számítógépes kontrollok kombinációja.

A leggyakrabban alkalmazott manuális kontrollok:

- a már bevitt dokumentumok fizikai érvénytelenítése,
- az aláírások összevetése egy hitelesített aláírás-listával,
- egyéb, a hibás input adatok kezelésére vonatkozó eljárások, valamint
- az input dokumentumok vezetés általi áttekintése (felülvizsgálata).

Az automatizált kontrollok lehetnek:

- sorozatszám ellenőrzés,
- javítások felismerése, automatikus összeegyeztetések, valamint
- a kivételes esetek jelentése.

A feldolgozandó adatokat különböző formában lehet rögzíteni. A számítógépes alkalmazások egyre növekvő mértékben használják a legújabb technológiákat, úgy mint az EDI-t, vagy az optikai vagy mágneses karakter felismerő eszközöket. Az adatbevitel akármilyen formáját is alkalmazzák, az általános beviteli kontroll célok ugyanazok maradnak. Ezek biztosítják, hogy:

- minden tranzakciót **pontosan** és **teljesen** rögzítsenek;
- minden tranzakció **érvényes** legyen;
- minden tranzakció **szabályos** legyen; valamint
- minden tranzakciót **elmentettek** a megfelelő beszámolási időszakhoz.

Annak biztosítására, hogy csak érvényes tranzakciók rögzítését fogadja el az alkalmazás, fizikai és logikai hozzáférés kontrollokat kell igénybe venni. Fizikai hozzáférés kontrollok lehetnek pl. zárak a pénzügyi szobák ajtaján, vagy kulccsal is lezárható számítógépes terminálok.

A logikai hozzáférés kontrollok alkalmazhatósága függ attól, hogy a számítógépes rendszer tudja-e azonosítani az egyes felhasználókat és az azonosítójukhoz hozzá tudja-e rendelni azt az előre meghatározott listát, mely az általuk szabályosan végrehajtható műveleteket (vagy művelet csoportokat) tartalmazza. A bejelentkezési és hitelesítési

kontrollok után az alkalmazásnak kontrollálnia kell az egyes felhasználók jogosultságait. Ez azt jelenti, hogy minden jogosult felhasználó, vagy csoport számára előre, egy ún. "profile"-ban rögzítik a hozzáférési jogokat és privilégiumokat. Például: ha egy felhasználónak „eladási főkönyv felhasználói” profile-t adnak, azzal kivédhetik annak lehetőségét, hogy a beszerzési főkönyvhöz, vagy más modulhoz hozzáférjen.

További biztosítékok nyerhetőek a számítógép által kikényszerített feladatkörmegosztással. A "profile"-ok kialakíthatóak oly módon a felhasználók számára, hogy a rendszer csak akkor dolgozza fel a rögzített adatokat, ha azt már engedélyezte az arra felhatalmazott dolgozó. *A felhasználói "profile"-okat úgy kell kialakítani és részletezni, hogy egyazon dolgozó ne legyen képes végigvinni egy pénzügyi tranzakciót a kezdetektől a végéig.*

A bevitel teljessége biztosítható például a tranzakciók kötegelésével. Ekkor a tranzakciók számának és értékének összesenjét össze kell vetni egy független számítás eredményével. Ahol az alkalmazások a rögzítéshez nem alkalmaznak kötegelési kontrollokat, az ellenőrnek alternatív bizonyítékot kell szereznie a teljességről.

Az alkalmazások képesek lehetnek megerősíteni a rögzítés érvényességét azáltal, hogy összehasonlítják az adatokat a rendszerben már eltárolt információkkal. Például egy eladási és beszerzési főkönyvi rendszerben az érvényesítés működhet a cím és az irányítószám alapján. A számítógép előhívhatja a fájlokban eltárolt címet, és az operátor összehasonlíthatja azt a rögzítendő dokumentumon található értékkel.

A számlaszámok vagy egyéb kulcs mezők tartalmazhatnak ellenőrző számjegyeket is. Az ellenőrző számjegyek egy algoritmus segítségével, a mező tartalmából számíthatóak, és jól használhatóak a rögzített mező helyességének ellenőrzésére.

A pénzösszeget tartalmazó mezőkre alkalmazható az intervallum ellenőrzés (alsó és/vagy felső) annak érdekében, hogy kiszűrhetőek legyenek a szabálytalan vagy irracionális összegek. Azon rögzített adatokat, melyek túllépik az előre megállapított intervallumot, vissza kell utasítania a rendszernek, és ezt a visszautasítást be kell írnia az ellenőrzési naplóba.

A tranzakciók sorszámozásával elkerülhető, hogy kimaradjanak tranzakciók, hogy többszörösen kerüljenek rögzítésre, illetve könnyebben felfedhetőek a szabálytalan tranzakciók. Mindemellett ez ellenőrzési nyomvonalat is biztosít.

Ha az adatok alkalmazáson kívülről is módosíthatóak, a fentiekben körvonalazott kontrollok megkerülhetőek. Ezért az ellenőrnek meg kell vizsgálnia, hogy működnek-e automatikus ellenőrzések az alkalmazásban, melyek felismerik és jelentik, ha az adatokban bármilyen külső változtatás történik (pl. ha egy rendszergazda az adatbázis-kezelőn keresztül megváltoztatta az adatokat). Az ellenőrnek meg kell vizsgálnia a telepítési kézikönyvet, hogy megbizonyodhasson arról, hogy az alkalmazás módosításra képes eszközei, mint pl. az editorok, megfelelően kontrolláltak.

Kérdések a 6. ponthoz:

6.1 Milyen eljárások/kontrollok biztosítják, hogy az input adatok ellenőrzöttek és pontosak legyenek?

- Nyilvántartás vezetés az engedélyezett felhasználókról
- Szabványos beviteli űrlapok
- Formátum ellenőrzés
- Számtartomány ellenőrzés
- Logikai ellenőrzés
- Függőségi ellenőrzés
- Ellenőrző számjegyek használata

A nem megfelelő input kontrollok növelik annak kockázatát, hogy hibás adatok kerülnek bevitelre, vagy csalás történik.

6.2 Milyen szabályozásokat vezettek be annak érdekében, hogy kivédjék a tranzakciók duplikált bevitelét?

- Egyedi hivatkozási számok használata
- A forrás dokumentumok fizikai érvénytelenítése
- A duplikált bevitel logikai visszautasítása

Manuális és/vagy számítógépes kontrollokat kell alkalmazni a duplikált bevitel kockázatának csökkentése érdekében.

6.3 Hogyan győződnek meg arról az alkalmazottak, hogy minden érvényes tranzakció bevitelre került? Milyen kontrollok biztosítják, hogy minden input dokumentum megérkezzen (pl. teljességi és pontossági ellenőrzés)?

- Kötegek címkézése
- Ellenőrző összegzések alkalmazása
- Sorozatszám ellenőrzések

A teljességi és pontossági kontrollok csökkentik a hiányos vagy hiányzó adatok kockázatát.

6.4 Milyen eljárásokat alkalmaznak a visszautasított tranzakciók esetében?

A nem megfelelő eljárások növelik a hiányos pénzügyi beszámoló kockázatát.

6.5 Mit tesz a vezetés az input adatok monitorozása (felügyelete) érekében?

A vezetés monitoringja és áttekintései csökkenti annak kockázatát, hogy szabálytalan adatok kerülnek rögzítésre. A vezetés áttekintése biztosítja továbbá, hogy a kialakított adatbeviteli eljárásokat betartják.

6.6 Kell-e konvertálni (átalakítani) az adatokat rögzítés előtt? Ha igen, milyen eljárások biztosítják, hogy az átalakított adatok pontosak és teljesek?

Ha adatokat továbbítanak egyik számítógépes rendszerből egy másikba, akkor egyes esetekben az adatok a bevitel előtt átalakítást igényelhetnek. Ha az átalakítás nincs megfelelően kontrollálva, az növeli a kockázatát, hogy az átvitt adatok nem lesznek pontosak és teljesek.

7. Adatátviteli kontrollok

Az adatátviteli kontrollok biztosítják, hogy az adatok átvitele - akár helyi, akár a külső hálózaton keresztül - érvényes, pontos és teljes legyen. A hálózatot használó szervezeteknek megfelelő kontrollokon keresztül biztosítaniuk kell, hogy az adatvesztés, a szabálytalan tranzakciók végrehajtásának és az adatok sérülésének kockázata egy elfogadható szintre csökkenjen.

Számos számítógépes rendszer csatlakozik valamilyen hálózatra: helyire (LAN) vagy akár a világhálózatra (WAN). Ily módon külső, távolabb eső helyekre is küldhetnek, illetve onnan kaphatnak adatokat. A legáltalánosabb adatátviteli közeg a telefonvonal, a koax kábel, infra-vörös sugár, optikai kábel és rádióhullámok. Bármely módját is választják, megfelelő kontrollokkal biztosítani kell a közvetített tranzakciós adatok integritását.

Azon alkalmazásoknak, melyek információkat közvetítenek hálózaton keresztül, a következő kockázatokkal kell szembenézniük:

- az adatok elfoghatóak („megcsapolhatóak") vagy megváltoztathatóak mind az átvitel, mind a közbülső tárolás közben;
- a kommunikációs csatlakozások kihasználásával illetéktelen adatok kerülhetnek bele a tranzakciós adatfolyamba; valamint
- az adatok megsérülhetnek az átvitel alatt.

Az ellenőrnek meg kell bizonyosodnia arról, hogy az illetéktelen tranzakciók felismerésére és kivédésére kontrollokat működtetnek. Ez például elérhető a kommunikációs kapcsolatok tervezésének és kialakításának kontrollálásával, vagy az egyes tranzakciók elektronikus aláírással való összefűzésével.

A továbbított adatok kommunikációs hibák miatt is megsérülhetnek. Az ellenőrnek meg kell bizonyosodnia arról, hogy megfelelő kontrollokat működtetnek mind a hálózati rendszeren belül, mind a pénzügyi alkalmazásokban, hogy azonosítsák a sérült adatokat. Ez lehet a hálózati kommunikációs protokoll, vagy előre kialakított szabályok meghatározhatják az átvitt adatok formátumát és jelentését, amivel már együtt tud működni egy automatikus hibafelismerő és -javító funkció.

Technikailag nem túl bonyolult dolog elfogni a továbbított adatokat a legtöbb hálózaton. A nem megfelelő hálózati védelem növeli a illetéktelen adatmódosítás, adattörlés és adat-duplikálás kockázatát. Számos kontroll létezik a probléma megoldására:

- az elektronikus aláírásokat használják annak ellenőrzésére, hogy a tranzakció érintetlen (hiánytalan), valamint hogy a tranzakció az arra felhatalmazott személytől származik;

- az adatok titkosítását arra használják, hogy kivédjék a tranzakciók elfogását és megváltoztatását;

- a tranzakciók sorszámozása segíti a duplikált vagy törölt tranzakciók elleni védelmet, illetve ezek felismerését, valamint segít felismerni a szabálytalan vagy illetéktelen tranzakciókat.

Kérdések a 7. ponthoz:

7.1 Ahol hálózatot, mágnesszalagot vagy lemezt alkalmaznak adatok átvitelére, hogyan biztosítják, hogy az átvitel teljes **és** pontos legyen?

- Digitális aláírás használata

- Adatok titkosítása

- Tranzakciók sorszámozása

A nem megfelelő kontrollok növelik a nem teljes, pontatlan, sérült vagy hibás tranzakciók kockázatát.

7.2 Használja-e a vizsgált szervezet az EDI technológiát? Ha igen, akkor azonosították-e és figyelembe vették-e az ennek megfelelő kockázatokat?

Az EDI alkalmazása jelzi az ellenőrnek a megnövekedett ellenőrzési kockázatot. Az EDI számos lehetséges kontroll-kérdést felvet, így ott, ahol ennek használata jelentős, szükséges lehet IT szakértő igénybevétele.

8. Feldolgozási kontrollok

A feldolgozási kontrollok célja annak biztosítása, hogy:

- a feldolgozott tranzakciók **pontosak** legyenek;
- a feldolgozott tranzakciók **teljesek** legyenek;
- a tranzakciók **egyediek** legyenek (pl. duplikáció nem megengedhető);
- minden tranzakció **érvényes** legyen; valamint
- a számítógépes feldolgozás **ellenőrizhető** legyen.

A feldolgozási kontrollok alkalmazhatóak az eredeti input adatokra, és a további származtatott adatokra is. A feldolgozási kontrollok további feladata, hogy védje ki vagy ismerje fel a feldolgozás ideje alatt az adatokon végrehajtott véletlen vagy szándékos (rosszindulatú) változtatásokat. Ezért az alkalmazáson belüli feldolgozási kontrolloknak biztosítaniuk kell, hogy csak érvényes adatokat és program fájlokat használhasson a program, továbbá a feldolgozott adatokat a megfelelő fájl-ba mentse el.

A feldolgozás pontossága és teljessége például oly módon biztosítható, hogy a bevitt tranzakciókból számított végösszeget összehasonlítják a folyamat által kezelt fájlok változásaival. Az ellenőrnek meg kell bizonyosodnia arról, hogy működnek olyan kontrollok, melyekkel felismerhető a hiányos vagy pontatlan adatfeldolgozás.

Az alkalmazás további érvényesítési folyamatokat is alkalmazhat a tranzakciókra, mint például az adatok ellenőrzése, hogy nincs-e bennük duplikáció; valamint vizsgálhatja a rendszer egyéb részeiben tárolt információkkal való összefüggést is. A folyamatnak ellenőriznie kell az általa kezelt adat sértetlenségét, például az adatokból számított ellenőrző összegek alkalmazásával. Ezen kontrollok célja, hogy felismerje az adatok kívülről történő megváltoztatását, ami lehet egy rendszerhiba következménye, de elérhető olyan rendszerszolgáltatások használatával is, mint például az editorok.

A számítógépes pénzügyi rendszereknek naplót kell vezetniük a végrehajtott tranzakciókról. A tranzakciós naplónak, mely szolgálhat egyben ellenőrzési nyomvonalként, elegendő információt kell tartalmaznia minden egyes tranzakció forrásának megállapításához.

Olyan környezetben, ahol kötegelt feldolgozás folyik, a feldolgozás során felismert hibákra fel kell hívnia a felhasználó figyelmét. A visszautasított kötegről naplót kell vezetni, és vissza kell irányítani az eredeti rögzítőhöz. Az on-line rendszerekben olyan kontrollokat kell működtetni, melyek figyelik a feldolgozatlan vagy elszámolatlan tranzakciókat (pl. részlegesen kifizetett számlák). Alkalmazni kell olyan folyamatokat is, melyek lehetővé teszik a vezetés számára, hogy azonosítsa és áttekintse a már egy bizonyos idő óta elszámolatlan tranzakciókat.

Az alkalmazásokat úgy kell megtervezni, hogy hogy meg tudjanak birkózni a – például áramszünet vagy hardver hiba miatt bekövetkező - üzemszünetekkel. A rendszernek fel kell ismernie minden hiányos (nem teljes) tranzakciót, és a hiba pontjától újra kell tudnia kezdeni a feldolgozást.

Kérdések a 8. ponthoz:

8.1 Milyen kontrollok biztosítják, hogy minden tranzakció feldolgozásra kerüljön?

- Input/output egyeztetés (összevetés)
- Sorozatszám ellenőrzés
- Ellenőrző összegek

A feldolgozott adatok nem megfelelő kontrollja növeli a hiányos vagy hibás tranzakciók kockázatát.

8.2 Milyen kontrollok biztosítják, hogy a megfelelő fájlok kerüljenek feldolgozásra (pl. a havi bérszámfejtésnél)? A kontrollok lehetnek fizikai vagy logikai természetűek is.

- Felcímkézett lemezek/kazetták
- Fejlécek használata a fájloknál
- A már lefuttatott feldolgozások megjelölése

Az adatfájlok nem megfelelő kontrollja növeli annak kockázatát, hogy nem megfelelő adatok kerülnek feldolgozásra.

8.3 Hogyan kezeli a feldolgozási hibákat maga az alkalmazás és a dolgozók? Visszautasítja-e az érvénytelen tranzakciókat, és értesíti-e erről a felhasználót?

Ha a visszautasított tranzakciókat nyomon követő kontrollok nem megfelelőek, akkor nő annak kockázata, hogy visszautasított, de egyébként érvényes tranzakciók maradnak kizárva a pénzügyi jelentésből.

8.4 Milyen kontrollok biztosítják a feldolgozások pontosságát?

- Ellenőrző összegek
- Tartományi és érvényességi ellenőrzések
- Ellenőrző számjegyek alkalmazása

A nem megfelelő kontrollok növelik a fel nem derített és ki nem javított feldolgozási hibák kockázatát.

8.5 Milyen kontrollokat alkalmaznak a duplikált feldolgozás felismerésére, kivédésére?

A nem megfelelő kontrollok növelik annak kockázatát, hogy egyes tranzakciók kétszer vagy többször kerülnek feldolgozásra.

9. Output kontrollok

Az output kontrollok célja annak biztosítása, hogy az alkalmazások által kibocsátott adatok, eredmények, jelentések stb.:

- **teljesek** és
- **pontosak** legyenek; valamint
- **kiosztásuk megfelelő** legyen.

Megfelelő kontrollokkal kell biztosítani továbbá, hogy az alkalmazás által output-ként előállított jelentéseket áttekintsék és felülvizsgálják.

Az output-tal összefüggő lehetséges kockázatok:

- engedély nélküli pénzügyi jelentés kibocsátása,
- hiba-jelentések és kivételes helyzetekről szóló jelentések elvesztése, vagy
- a pénzügyi jelentések - pl. próbamérlegek, adósok listája, stb. - szabálytalan megváltoztatása.

Működnie kell olyan mechanizmusnak, mely biztosítékot nyújt a befejezett feldolgozások teljességéről és pontosságáról azok számára, akik a tranzakciós adatok rögzítéséért és engedélyezéséért felelősek. Ennek egyik módja, hogy a feldolgozás során felismert hibákat az alkalmazás egy feldolgozási naplóba gyűjti, vagy az ellenőrző összegeket veti össze a rögzítés alatt generáltakkal (gyakorlatilag összehasonlítja mi ment be és mi ment ki).

Az output teljessége és sértetlensége attól is függ, hogy korlátozott-e az output megváltoztathatósága, és van-e az alkalmazásban teljesség-ellenőrzés, mint például lapsorszámozás vagy ellenőrző összegek.

A számítógépes output-oknak - lehetőség szerint - rendszeresnek és ütemezettnek kell lenniük. Ugyanis a felhasználók nagyobb valószínűséggel fedezik fel a hiányzó output-ot, ha a rendszerességen alapulva várják azt. Ezt még ott is meg lehet valósítani, ahol a számítógépes jelentések tartalma egyenetlen (mint például a kivételes esetek jelentésénél): egy üres jelentés előállításával.

Ahol az output egy kulcsfontosságú kontroll részét képezi, az ellenőrnek meg kell vizsgálnia, hogy megerősítést nyer-e hogy a címzetthez megérkezik, és ő el is fogadja.

Az output file-okat védeni kell annak érdekében, hogy csökkenjen az illetéktelen vagy szabálytalan változtatás kockázata. A számítógépes output megváltoztatásának lehetséges indítékai lehetnek:

- szabálytalan vagy illetéktelen feldolgozás elleplezése, vagy
- nem kívánatos pénzügyi adatok "kozmetikázása".

Ha a számlakezelő rendszerben az output fájlok védtelenek, az kihasználható például a fizetendő összegek vagy a rendelvényes megváltoztatására. A számítógépes output sértetlenségének védelmére fizikai és logikai hozzáférés kontrollok kombinációját célszerű alkalmazni.

Egy alkalmazás output-ja része lehet egy másik alkalmazás bemenő adatainak is, mielőtt az véglegesen belekerülne a pénzügyi jelentésekbe. Például a bérszámfejtés outputja bemeneti adatként szolgál a főkönyvi alkalmazásba. Ahol ilyen eset áll fent, az ellenőrnek meg kell vizsgálnia azon kontrollokat, melyek biztosítják, hogy az output pontosan kerüljön át az egyik feldolgozási szintről a következőre.

Kérdések a 9. ponthoz:

9.1 Milyen kontrollok biztosítják a számítógépes output-ok (nyomtatványok, csekkek, számlák stb.) szabályszerű tárolását, valamint azt, hogy a feladott vagy elküldött outputok rendben megérkezzenek a címzettekhez?

A nem megfelelő kontrollok növelik annak kockázatát, hogy a feldolgozás során bekövetkező hibák nem keltik fel a vezetés figyelmét.

9.2 Alkalmaznak-e megfelelő kontrollokat a számítógépes nyomtatványok tárolására?

- Váltók/értékpapírok
- Szoftver licencek

A nem megfelelő kontrollok növelik a csalás és a hiányos könyvelés kockázatát.

9.3 Milyen logikai, pontossági és teljességi ellenőrzést végeznek az output-okon?

Ezen kontrollok célja a feldolgozási hibák és/vagy a szabálytalan feldolgozás felismerése.

9.4 Alkalmaznak-e megfelelő kontrollokat a pénzátutalási rendszerek esetében ?

A nem megfelelő kontrollok növelik a szabálytalan kifizetések kockázatát.

10. Törzsadatok kontrollja

A törzsállományban tárolt információk a legtöbb esetben kritikusak a pénzügyi adatok feldolgozása és a beszámoló szempontjából. A törzsállományban tárolt információ befolyásolhatja számos pénzügyi tranzakció eredményét, ezért ezeket megfelelően védeni kell. Például az adó-vagy TB kulcs változtatása a bérszámfejtő rendszerben megváltoztathatja minden alkalmazott fizetését is. A leggyakrabban előforduló törzsadatok: számlakeret, bérlista, szállítói és vásárlói adatok vagy termék árlisták.

A törzsadatok kontrolljainak célja annak biztosítása, hogy:

- a törzsadatokat csak **engedélyezett** módon lehessen megváltoztatni;
- a felhasználó legyen **felelős** a változtatásokért; valamint
- a **sértetlenséget** fenntartsák.

A hozzáférés kontrollok biztosítják annak alapját, hogy törzsadatokat létrehozni, megváltoztatni, helyreállítani vagy törölni csak az arra felhatalmazott dolgozók legyenek képesek. Az ilyen kontrollok akkor a leghatékonyabbak, ha az operációs rendszer szintjén működnek, mivel így megakadályozható, hogy az alkalmazási kontrollokon kívüli környezetből - az operációs rendszer szolgáltatásait kihasználva – illetéktelenek megváltoztassák az adatokat.

A törzsállományokat (mint pl. a szállítói adatokat, átváltási árfolyamokat stb.), védeni kell anna érdekében, hogy az érvényes tranzakciók helyesen fussanak le. Például a szállítói adatok megváltoztatása egy érvényes kifizetést eredményezhet egy illetéktelen rendelvényesnek. Ennek érdekében a hozzáférés kontrolloknak kell biztosítani a feladatkörök szétválasztását azok között, akik a törzsadatokat kezelik, és akik rögzítik a tranzakciókat. Ezért az ellenőrzési naplónak rögzítenie kell olyan információkat, mint pl. a törzsadatokat érintő változtatások dátuma és időpontja, a felelős személy azonosítója, valamint a változtatásban érintett adatmezők. A fontosabb törzsadatokról mindig biztonsági mentést kell végezni, mielőtt változtatást hajtanak végre rajtuk.

Azon alkalmazások, melyek kontrollálják a felhasználói hozzáférési jogosultságokat, a jogosultsági adatokat törzsállományokban tárolják. Ezen fájlokat különösen védeni kell az illetéktelen vagy szabálytalan változtatásoktól. A kiváltságokkal való visszaélések elkerülése érdekében a vezetésnek független ellenőrzési módszert kell alkalmaznia az alkalmazások hozzáférés kontroll rendszerének kezelésére. A vezetésnek célszerű rendszeresen kilistázni a törzsállományok (pl. a felhasználók biztonsági profile-jai) tartalmát ellenőrzés céljából.

Kérdések a 10. ponthoz:

10.1 Engedélyhez kötött-e a törzsadatok megváltoztatása? Hogyan zajlik az engedélyeztetés?

A nem megfelelő kontrollok növelik a törzsadatok szabálytalan megváltoztatásának kockázatát. A szabálytalan változtatások többszörösen hibás tranzakciókat idézhetnek elő.

10.2 Milyen kontrollok védik a törzsadatokat a szabálytalan hozzáféréstől és változtatástól?

A beépített logikai hozzáférés kontrollok jól alkalmazhatóak arra, hogy csak a felhatalmazottak férhessenek hozzá az adatokhoz. Ez csökkenti a szabálytalan változtatások kockázatát.

10.3 Milyen beépített fájlszerkesztő eszközzel rendelkezik az alkalmazás? Hogyan kontrollálják ennek használatát?

A fájlszerkesztő eszközökhöz való korlátlan hozzáférés növeli a szabálytalan és nehezen feltárható változtatások kockázatát.

10.4 Milyen kontrollokat alkalmaznak a törzsadatok szabálytalan megváltoztatásának felismerésére?

- Ellenőrző összegek
- Más forrásból származó törzsadatokkal való összevetés
- Rendszeres vezetői felügyelet

Azok a beépített kontrollok, melyek azonosítják a szabálytalan változtatásokat, csökkentik annak kockázatát, hogy ezek a változtatások észrevétlenek maradnak.

Alapfogalmak magyarázata

Batch (kötegelt) feldolgozás: amikor a felhasználó által már elindított feldolgozásba annak teljes lefutásáig már nincs beavatkozási lehetőség. A kötegelt feldolgozás futhat háttérben (azaz a felhasználó közben egyéb feladatokat is tud végezni a számítógépen), vagy arra a futási időre teljes egészében le is foglalhatja a gép kapacitását.

Gateway: hardver és szoftver kombinációja, melyet egymással inkompatibilis hálózati architektúrák összekapcsolására használnak.

Interaktív feldolgozás: a felhasználó kapcsolatban marad egy programmal és közvetlenül kezeli annak működését (mint például egy szövegszerkesztő használatakor.)

Kliens-szerver modell: hálózatok esetében alkalmazott modell, ahol az alkalmazói feldolgozások az egyes munkaállomások (kliensek) és a szerver(ek) együttműködésében történnek. Ebben a modellben a feladatok egy részét a kliens munkaállomások, más részét a szerverek hajtják végre. Jellemzően a szerver a centralizált, többfelhasználós szolgáltatásokat végzi.

Mainframe: Olyan nagy kapacitású számítógép, mely az adatok központi feldolgozását végzi. A mainframe-ek több felhasználót is képesek kiszolgálni egyszerre, végezhetőek rajtuk párhuzamos feldolgozások (azaz több feladatot ellát egyidőben), és számos perifériális eszköz (pl. nagy teljesítményű nyomtatók, szalagos háttértárolók) kapcsolódhat hozzájuk.

On-line: a feldolgozási műveletek elvégzésének azon módja, amikor a számítógép közvetlenül és azonnal vezérelhető. Az interaktív és az ún. real time (valós idejű) rendszerek on-line rendszerek.

Profile: meghatározza az egyes felhasználók vagy felhasználói csoportok számára, hogy mely eszközökhöz, milyen mértékben és milyen módon férhetnek hozzá.

Protokoll: Olyan sztenderdek és szabályok, melyek meghatározzák a számítógépes hálózaton közvetített adatok jelentését, formátumát és típusát.

Real-time (valós idejű) rendszer: olyan számítógépes rendszer, mely azonnal reagál az eseményekre (billentyű leütése, tranzakció befejeződése stb.). Az ilyen rendszerek általában interaktívak, és a tranzakciók feldolgozásával egyidejűleg a fájlok-at is módosítják.

Router: olyan hálózati eszköz, mely biztosítja, hogy a hálózaton elküldött adatok optimális útvonalon érkezzenek célhoz.

Szerver: számítógép, amin egy olyan adminisztratív szoftver működik, mely szabályozza a hálózat egészére vagy részeire való belépést, a hálózathoz kapcsolt eszközökhöz (nyomtatók, lemezes egységek, stb.) való hozzáférést. A szerverként működő gép lehetővé teszi a hálózathoz kapcsolódó egyéb számítógépek számára, hogy munkaállomásként működhessenek.

Terminál: olyan számítógép, mely nem tartalmaz saját háttértárat (winchestert).

Tükrözött rendszer: egy alkalmazói feldolgozó rendszer pontos másolata, ami ugyanolyan hardveren, ugyanazon szoftvert és adatokat tartalmazza. A tükrözött rendszert biztonsági célokból alkalmazzák, olyan esetekre, amikor az aktuális használt rendszer üzemképtelen.

Irodalomjegyzék

Financial Audit Field Manual Module T9 Audit in an IT Environment, NAO 1996

Review of Information System Controls For NAO, 905 Version1 1999.

Federal Information System Controls Audit Manual, GAO/AIMD-12.19.6 1999.

Handbook of IT Auditing PricewaterhouseCoopers L.L.P 2000.

Control Objectives for Information and Related Technology (COBIT) 1996.

Az informatikai stratégia kialakításának és megvalósításának irányelvei ITB 2.sz ajánlás,1996.

Informatikai biztonsági módszertani kézikönyv ITB 8.sz ajánlás, 1994.

Informatikai rendszerek biztonsági követelményei ITB 12.sz ajánlás, 1996.