Vállalkozási mérlegképes könyvelő

ELLENŐRZÉS

tantárgy

27. téma

(Az informatikai ellenőrzés)

Az informatika ellenőrzése

Informatikai rendszerek ellenőrzése: a vállalkozásnál működő informatikai rendszerek megbízhatóságának, a rendszerben tárolt adatok teljességének, megfelelőségének, szabályosságának és védelmének vizsgálata.

Több területre terjed ki:

- technikai ellenőrzés,
- alkalmazások ellenőrzése,
- biztonság, fizikai védelem vezetés ellenőrzési eljárásainak vizsgálata.

2

Informatikai rendszerek kontrolljainak ellenőrzéséhez az Állami Számvevőszék által kidolgozott módszertan segítséget nyújt az ellenőr számára annak megítélésében, hogy az informatikai környezetben elkészített pénzügyi beszámoló adatai és a beszámoló előállításához felhasznált elektronikus bizonyítékok:

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

3

IT-ellenőrzés jelentősége és szerepe:

a) Ellenőrzött szervezetek informatikai kitettsége nő
   - Nincs informatika-mentes folyamat → ~~PAPÍR~~ kontrollokat is informatikai rendszerek biztosítják.
   - Az IT-rendszerek működése a feladatellátás minőségét és jogszabályi megfelelőségét is alapvetően meghatározza.

b) Az IT-rendszerek mérete és összetettsége nő

c) A szervezetek egyre jobban támaszkodnak olyan rendszerekre, amelyek belső működését egyre kevésbé látják át
   - a komplex informatikai rendszerek megfelelősége, adatainak megbízhatósága csak speciális ellenőrzési eljárások alkalmazásával ítélhető meg

4

- általában az ÁSZ ellenőrzések részeként valósulnak meg, azokat kiegészítve;
- fontos információkat szolgáltatnak az eredendő és kontroll kockázatok értékeléséhez → befolyásolják az alkalmazandó ellenőrzési eljárásokat;
- megállapításaik általában az ÁSZ jelentésekben önállóan is megjelennek;
- megjelennek a megfelelőségi, eredményességi és hatékonysági szempontok is;
- több szervezetet érintenek, így kiterjednek az együttműködési, illetve irányítási feladatok értékelésére is.

5

Kockázati alapú megközelítés

Az informatikai ellenőrzés kockázatának három összetevője van:

- *Eredendő kockázat*: az informatikai erőforrásoknak (elektronikus adatok, fájlok, szoftverek, számítógépek, hálózati eszközök stb.) a fenyegetettségek iránti fogékonysága, azt feltételezve, hogy e fenyegetettségek kivédésére irányuló kontrollok nem léteznek.

  Fenyegetettség: minden olyan nemkívánatos esemény, amely az adatok teljességét, sértetlenségét, megbízhatóságát vagy rendelkezésre állását hátrányosan befolyásolja.

6

Fenyegetettség lehet
- külső esemény (tűz, vízkár, vírusok stb.),
- belső tényező (hanyag kezelés, rosszindulatú adatmódosítás, programhiba stb.).

- *Belső kontroll kockázat*: annak lehetősége, hogy a szervezet belső kontroll mechanizmusai nem képesek megelőzni, vagy feltárni és kijavítani a szabálytalanságot vagy tévedést. A belső kontroll kockázat → belső kontrollok fejlesztésével csökkenthető.
- *Feltárási kockázat*: annak veszélye, hogy az ellenőr nem tár fel a szervezet belső kontrollmechanizmusai által nem korrigált lényeges szabálytalanságot vagy tévedést.

7

A számítógépes ellenőrök (könyvvizsgálók) munkájának jelentős része a következő informatikai ellenőrzésekre összpontosít:
- ellenőrzési megoldások értékelése,
- ellenőrzési funkciók tesztelése,
- javaslat ellenőrzési megoldások alkalmazására.

8

Az informatikai környezet és tevékenység felmérése

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

Az informatikai környezet megmutatja, hogy az adott szervezet pénzügyi beszámolója
1) milyen számítógépes rendszereken alapul,
2) közöttük milyen kapcsolat áll fenn.

9

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

IT környezet részei:

A. Infrastruktúra:
- hardvereszközök és rendszer szoftverek,
- hálózati hardver és topológia: kérünk egy egyszerű ábrázolást, melyen azonosíthatóak a feldolgozási és felhasználói helyek, valamint a hálózati hardver elemek.

10

B. Alkalmazások:
- Alkalmazások felsorolása: külön választjuk a pénzügyi-számviteli, ill. az egyéb alkalmazásokat.
- Alkalmazások részletes információi: a pénzügyi alkalmazásokról kérünk részletesebb tájékoztatást (pl. felhasználói kézikönyv, leírás stb.)

A környezet felmérése alapján megállapítható:
- mennyire összetett a vizsgált szervezet rendszere;
- az egész rendszer mely részeire terjedjen ki a részletes vizsgálat;
- mely kontroll területek (pl. biztonságtechnikai kontrollok) ellenőrzéséhez szükséges IT szakellenőr igénybevétele.

11

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.

Az informatikai tevékenység felmérésének célja: az ellenőr megismerje azon tevékenységeket és szervezeti működést, melyek a pénzügyi-számviteli rendszerek megbízható működését befolyásolhatják → a vizsgálat közvetlenül a pénzügyi informatikai rendszerre koncentrál.

12

Az ellenőrzés területei:

1. Üzemeltetés, fejlesztés: a szervezetnek gondoskodnia kell informatikai környezetének megfelelő üzemben tartásáról.
2. Szervezeti keretek: lehetővé teszik-e az informatika - és benne a pénzügyi-számviteli rendszerek - megfelelő működtetését?
3. Magas szintű szabályozások:
   - ✓ megvan-e a magas szintű szabályozás a részletesebb kontrollok megfelelő kialakításához;
   - ✓ milyen kontrollok töltenek be lényeges szerepet a szervezetnél;
   - ✓ mely kontroll területek ellenőrzéséhez szükséges IT szakellenőr igénybevétele

13

Az általános informatikai kontrollok vizsgálata

Általános informatikai kontrollok: ahhoz a környezethez kapcsolódnak, amelyben a számítógép alapú rendszerek kifejlesztésére, fenntartására és üzemeltetésére kerülnek, és amelyek ily módon minden alkalmazáshoz kapcsolódnak.

Az általános ellenőrzési megoldások célja: biztosítsák az alkalmazások megfelelő kifejlesztését és végrehajtását, illetve a programok, az adatállományok és a számítógépes műveletek integritását → az informatikai ellenőrzés elsődleges alapszintjét képezik.

14

Az általános kontrollok az informatikai folyamatokba beágyazott kontrollok, melyek a következők:

- rendszerek fejlesztése (szoftverfejlesztés, hardverbővítés stb.)
- változáskezelés (programfrissítés, operációs rendszer frissítése stb.),
- biztonság és védelem (adatok duplikálása, adatok kódolása, hozzáférés korlátozása stb.)
- számítógép üzemeltetés (szünetmentes tápegység, szerverek hűtése stb.)

15

Az üzleti folyamat-alkalmazásokba beágyazott kontrollok a következők:

- Teljesség
- Pontosság
- Érvényesség
- Engedélyezés/Jóváhagyás
- A felelősségek elhatárolása (minden a felhasználó nevére naplóz alkalmazás)
- Ellenőrző számok, ellenőrző összegek, logikai ellenőrzés

16

Az alkalmazás kontrollokért való felelősség az üzleti területek és az informatika közös felelőssége, de a felelősségek jellege az alábbiak szerint változik:

a) Az alábbiak szabályos végrehajtásáért az üzleti területek a felelősek:
   - A funkcionális és kontroll követelmények meghatározása
   - Az automatizált szolgáltatások használata

b) Az informatika a felelős a következőkért:
   - Az üzleti funkcionális és kontroll követelmények automatizálása és megvalósítása
   - Kontrollok létrehozása az alkalmazás kontrollok sértetlenségének fenntartása érdekében.

17

Általános ellenőrzési megoldások:

1) Szervezeti ellenőrzési funkciók: áttekintésének célja annak biztosítása, hogy a számítógépes létesítményben dolgozó munkatársak:
   - megszervezése és irányítása megfelelő és hatékony módon történjen
   - világosan definiált kötelezettségekkel rendelkezzenek
   - a funkciók megosztásának alapelve alá essenek
   - kellően képzettek és támogatottak legyenek
   - megfelelő jelentéskészítési rendszerekkel rendelkezzenek.

18

Az ellenőrzés módszerei: a vezetés és a munkatársak meghallgatása, megfigyelés és dokumentációk (munkaköri leírások, a szervezeti ábra stb.).

2) Üzemeltetés-ellenőrzési funkciók: célja annak biztosítása, hogy a feldolgozás minden esetben teljes, pontos, időszerű és jogosult legyen.

3) File-ellenőrzési funkciók: célja, hogy a számítógép által olvasható adathordozón található információk a jogosulatlan felhasználással, a módosítással, a megrongálással és az adatelvesztéssel szemben védve legyenek.

19

A főbb ellenőrzési területek a következők:

A. fizikai biztonság: az ellenőröknek meg kell győződniük arról, hogy a fájlokat
   - ✓ szabályszerűen tárolják-e, így azok azonnal és pontosan beazonosíthatók és behívhatók-e,
   - ✓ lopással, vírussal való megfertőzésétől, tűztől, beázástól, idő előtti letörléstől védve tárolják-e.

B. jogosulatlan hozzáférés: meg kell győződni arról, hogy a file-okat csak engedélyezett tevékenység útján lehet feldolgozni vagy megváltoztatni, azaz
   - ✓ az adatállományok csak az engedélyezett alkalmazási programok útján kerülnek feldolgozásra,
   - ✓ A programokat csak jóváhagyott célokra és csak az arra jogosult személyek működtetik.

20

C. file biztonsági mentés (back up): minden fontos file-ról legalább egy jó másolat mindig rendelkezésre álljon → a biztonsági mentés legyen szisztematikus, legyen rendszeresen tesztelve, minden részletre kiterjedően dokumentálva, illetve lopástól, az adat elvesztésétől, fizikai sérüléstől, mágneses behatástól, tűztől, folyékonyanyagoktól stb. védve.

4) Visszaélés a számítógépes rutin alkalmazásokkal: a számítógépes csalások első kategóriája, a számítógépes rutin alkalmazások illetéktelen használata → az alkalmazási rendszerbe épített szigorú ellenőrzések útján nagymértékben megelőzhető.

21

Az ezzel kapcsolatos ellenőrzések a következőkre terjedhetnek ki:

- ✓ ki tud hozzáférni a rendszerhez és milyen célból?
- ✓ az adatbevitel teljessége (a csalások a bemeneti adatok, pl. az adósok nyomon követése eltitkolásával is elkövethetők)
- ✓ az adatbevitel pontossága (a jogosulatlan kiegészítések az output fázisban felderíthetővé váljon)
- ✓ az adatbevitel engedélyezése (dokumentumok ellenőrzése és a tranzakcióknak az azokat bevivő emberhez való naplózása útján)

22

Az általános ellenőrzési megoldások fontos szerepet játszanak a csalások megakadályozásában:

- ➢ a funkciók szétválasztása (pl. az adatbevitelért felelős személy ne legyen képes az output eltitkolására)
- ➢ a rendszerfelügyeletet (beleértve a személyi állomány moráljának, motivációjának figyelemmel követését, ill. a gyakran csaláshoz vezető esetleges személyes problémák észlelését).

IT kontrollok értékelésének főbb elemei:

a) általános kontroll környezet értékelése: feladatkörök szétválasztása, hozzáférés kontrollok, változáskezelés, külső szolgáltatók igénybevétele

23

b) alkalmazás kontrollok értékelése, tesztelése:
   - ➢ rendszer által biztosított kontrollok értékelése: adatfeldolgozási lépések, beépített ellenőrzések, riportok, adatkapcsolatok
   - ➢ rendszer adatainak megbízhatóságát biztosítókontrollok, az általános IT kontrollok érvényesülése a vizsgált rendszernél: pl. hozzáférés kontrollok, a tevékenységek nyomon követhetősége;

c) a rendszer működési környezetének és feltételeinek értékelése: folyamatos működés feltételei, tartalékolás, dokumentáció, rendkívüli helyzetek kezelése

24

d) az ellenőrzés során a dokumentum alapú vizsgálat mellett hangsúlyt kap a rendszer működésének, használatának értékelése is: bejárások, adatbevitelek, feldolgozások végigkövetése
e) kockázatelemzés alapján kiválasztott kockázatos vagy „szokatlan”tételek ellenőrzése.

25

Az információs rendszerek működtetésének kontrolljai

Az információrendszerek működésének ellenőrzése a belső ellenőrzés területe → egy vizsgálati eljárás alkalmazásával megállapítják biztonsági tulajdonságait.

Az ellenőrzés területei:

- a technikai ellenőrzés (infrastruktúra, kommunikáció),
- a menedzsment ellenőrzési eljárásainak vizsgálata,
- a szoftverfejlesztés,
- az alkalmazások ellenőrzése → nemzetközi-, hazai szabványoknak való megfelelés.

26