Információrendszerek auditálása

Az informatika és az információrendszerek ellenőrzési és irányítási módszerei

Molnár Bálint
Kő Andrea

Corvinno Technology Transfer Kft

ISBN 978-963-06-7254-2

A kiadásért felel a Corvinno Technology Transfer kft
ügyvezetője, Budapest, 2009

Szerkesztette: Molnár Bálint, Kő Andrea
Szakmai lektor: Dobay Péter, Sántáné-Tóth Edit
Borítóterv: Tóth Ferenc

Tartalomjegyzék

Előszó

Napjaink fontos jellemzője az informatikai infrastruktúra meghatározó szerepe. A fejlődés ezen a téren töretlen, senki nem tudja megmondani most, hogy milyen rendszereket fogunk használni néhány tíz év múlva. Különösen igaz ez napjainkban a virtuális szervezetek egyre nagyobb térhódítása, az Internet és egyéb hálózati alkalmazások egyre jelentősebbé válása miatt. Az informatikai megoldások által elérhető kényelemnek ára van: a felhasználók kiszolgáltatottabbak a különböző típusú szándékos és nem szándékos informatikai károkozásokkal szemben. A számítógépek használata veszélyeket is hordoz magában, de erre ritkán hívják fel a felhasználók figyelmét. Bizalmas adatok megsérülése, elvesztése, illetéktelenekhez kerülése komoly anyagi és erkölcsi károkat okozhat. Ellentétben a hagyományos, papír-alapú iratkezelés áttekinthető szabályrendszerével, az elektronikus megvalósítás során új követelmények fogalmazódtak meg. Kialakult egyfajta függőség az informatikai rendszerekkel szemben, és ez a tény megnövelte az informatikai biztonság, ezzel együtt az ellenőrzés szerepét. Az informatikai rendszerek üzemeltetése nehéz feladat: a fejlődés gyors, újabb és újabb fenyegető tényezőkkel kell szembesülni és megfogalmazni a megfelelő intézkedéseket. A versenyképesség fenntartása és az üzleti környezetben való túlélés megköveteli az informatikai ellenőrzésre fordított figyelem és erőforrások növelését.

Az informatikai, információrendszer ellenőrzés kialakulásának és kifejlődésének legfontosabb okai a következők:

- a technológia fejlődése;
- pénzügyi veszteség az informatikai rendszerek nem megfelelő működése miatt, többek között a belső informatikai részleg programozóinak „kreatív és eredeti" megoldása miatt;
- bizalmas adatok nyilvánosságra kerülése;
- nem megfelelő belső ellenőrzési és irányítási eljárások;
- hacker és cracker támadások;
- a vállalati belső információrendszerek, a hálózat használatának engedélyezése a munkatársak vállalati asztali számítógépéről, otthonról, vagy a szervezeten kívülről (távoli, illetve mobil elérés lehetősége);
- az informatikai rendszerekben felhalmozódott hatalmas mennyiségi adat manuális módon már nem is ellenőrizhető, ezért a vizsgálatok (pénzügyi és informatikai) számítógéppel támogatott ellenőrzést igényelnek (CAAT – Computer Assisted Audit Technique);
- a számítógépes rendszereken végrehajtott (elsősorban pénzügyi) vizsgálatok nem megfelelőek az adatok informatikai megbízhatóságának értékelése tekintetében;
- a számítógépes, informatikai rendszereket körülvevő munkafolyamatokba beépített ellenőrzési eljárások és mechanizmusok megbízhatósága egyre kérdésesebbé vált;
- az adatok biztonsága, az adatok védelme többé már nem kényszeríthető ki a hagyományosan bevált eszközökkel.

A könyv célja

Ez a könyv az informatika és az információrendszerek ellenőrzésének és irányításának témakörét, az információrendszerek auditálási módszereit tárgyalja. Az alapképzésben, a mesterképzésben részt vevő gazdaságinformatikus, mérnök informatikus és programtervező informatikus hallgatóknak kíván segítséget nyújtani abban, hogy megismerkedhessenek az információrendszerekkel, információtechnológiával, informatikával kapcsolatos ellenőrzés, vizsgálat, (auditálás) módszereivel, technikáival, az auditra vonatkozó irányelvekkel és szabványokkal. Külön fejezetekben tárgyaljuk az ellenőrzés jellemzőit az egyes informatikai részterületekre vonatkozóan. Ezek a részterületek a következők: az informatika irányításának alapelvei, az auditálással összefüggő menedzsment eljárások, az informatikai eszközök védelme, katasztrófa-elhárítás tervezése és az üzletmenet folytonosság biztosítása, a rendszerfejlesztés, beruházás és karbantartás területei, a projektek ellenőrzése. A könyvet a szakirányú képzések és a speciális tanfolyamok résztvevői, valamint gyakorlati munkájuk során nap, mint nap ellenőrzési feladatokkal találkozó szakemberek is haszonnal forgathatják.

A könyv szerzői többféle képzési formában oktatattak és oktatnak az informatikai audithoz kapcsolódó tárgyakat a Budapesti Corvinus Egyetemen (és elődjén, a Budapesti Közgazdaságtudományi Egyetemen). Ebben a könyvben a felhalmozódott, mintegy ötéves oktatási tapasztalatot is hasznosítjuk.

A könyv szerkezete

A könyv alapfokú informatikai és rendszerfejlesztési ismeretekre épít. A terminológiai megalapozás alapvető ezen a szakterületen, mivel többféle és nem egységes fogalomrendszerek terjedtek el. Ezért hangsúlyosan megjelennek a könyv első fejezeteiben olyan informatikai fogalmak is, amelyek az ellenőrzéshez kapcsolódó informatikai részterületek alapfogalmait tisztázzák. Ahol a mondanivaló elméleti hátterét vagy mélyebb megértését célzó magyarázatok megzavarták volna a folyamatos olvasást, ott azok lábjegyzetbe kerültek, míg a részletek iránt érdeklődők számára gyakran található ajánlott irodalom is. Az egyes anyagrészek mélyebb megértését célzó példák, részletesebb leírások, illetve bizonyos témák rövid ismertetése a könyvhöz csatolt függelékekben található. Az anyagban való eligazítást segíti, hogy a fontosabb fogalmak meghatározásai (az angol nyelvű változattal együtt) vastagon szedett betűvel vannak kiemelve. Minden fejezetet ellenőrző kérdések sora zárja.

A könyv *1. fejezete* áttekintést nyújt információrendszerekkel, információtechnológiával, informatikával kapcsolatos ellenőrzés, vizsgálat alapfogalmairól, az ellenőrzési és irányítási eljárásokról, az auditálás végrehajtásáról, az auditor szerepéről. Már itt megjegyezzük, hogy az „audit” kifejezéssel szinonimaként használjuk a szövegben az „ellenőrzés” fogalmát; és az angol nyelvben használatos „kontroll” („control”) kifejezés helyett az „ellenőrzési és irányítási eljárás”-t alkalmazzuk (a kontroll kifejezés bővebb, mint az ellenőrzési eljárás, ezért a magyar fordítás is

összetettebb). Részletesen bemutatjuk a kontrollok különböző fajtáit és azok jellemzőit. Összefoglaljuk a kockázat-alapú auditálás lépéseit, és tárgyaljuk az auditjelentés felépítését. Végül az auditor munkáját segítő tényfeltáró technikákkal is foglalkozunk.

A *2. fejezet* az auditálással kapcsolatos szabványokkal, szabályozási környezettel foglalkozik. A terület meghatározó szabványa a COBIT (jelenleg már a 4. verzió is elérhető magyarul[1]), amely egységes keretrendszert nyújt az auditálás végrehajtásához; ezért a fejezet első nagyobb témaköre a COBIT bemutatása. Foglalkozunk az informatikai biztonság, a minőségbiztosítás és a szoftver életciklus szabványaival is.

A *3. fejezet* az auditálással összefüggő szervezeti és vezetési szempontokra koncentrál. A fejezet első részében az informatika irányításának (IT Governance) alapelveit mutatjuk be. A fejezet második része a belső ellenőrzés témakörét járja körül. Végül az auditálással összefüggő menedzsment eljárásokat összegezzük.

A *4. fejezet* az informatikai vagyon, infrastruktúra védelmével foglalkozik. Részletezi a fizikai, környezeti és logikai hozzáférési ellenőrzési eljárásokat, valamint az auditor szerepét a folyamatban.

Az *5. fejezet* az üzletmenet folyamatosságának biztosítását, a katasztrófa elhárítás tervezését tárgyalja. Ismerteti a folyamatos tevékenység fenntartás (FTF) életciklusát, szakaszait, a katasztrófa elhárítási alapváltozatokat, az auditor feladatait az üzletmenet folytonosságának biztosításában és a katasztrófa elhárítás tervezésében.

A *6. fejezet* áttekintést ad a rendszerfejlesztés, beruházás, karbantartás ellenőrzéséről. Részletesen bemutatja az információrendszer fejlesztési projektek ellenőrzési feladatait. Mivel az informatikai projektek sok esetben zárulnak sikertelenül, különösen fontos az auditor támogatása a projektek korai szakaszaiban. Ezért mutatunk be olyan technikákat (lásd funkciópont meghatározás), amelyek segítik a kialakítandó információrendszer jellemzőinek (méretének, költség és erőforrásigényének) megállapítását. Illetve ha projekt auditálásnál, informatikai részleg, szervezet auditálásánál egy adott információrendszer (akár adatközpontú, akár tranzakció-központú) értékét, beruházás megtérülését, pénzügyi ésszerűségét kell vizsgálni az auditornak, akkor a funkciópont elemzés segédeszközként szolgál annak vizsgálatára, hogy vajon az információrendszer-beruházás megéri-e azt a pénzt, amibe kerül.

A *7.fejezet* az előző fejezetek anyagára támaszkodó, összetett esettanulmányt tartalmaz. A célja, hogy támogatást nyújtson abban, hogy egy valós esetben hogyan alkalmazhatóak az előző elméleti ellenőrzési részek ismeretei. Ez az esettanulmány felhasználható az oktatásban csoportmunka feladatként, a tanultak ellenőrzésére, vagy önellenőrzésre is.

A könyv *függelék*ei az egyes fejezetekben mondottak mélyebb megértését célzó ismertetések mellett további konkrét ellenőrzésben alkalmazható segédanyagokat

[1] Ld. www.isaca.org, www.isaca.hu

tartalmaznak, illetve speciális rendszerek ellenőrzési támogatását adják meg.

A csatolt *angol-magyar fogalom és szójegyzék* a könyvben használt fontosabb szakkifejezések angol–magyar szószedetét tartalmazza. Célja az angol nyelvű szakirodalom olvasásának segítése.

A könyvben hivatkozott forrásanyagok referenciáit az irodalomjegyzék tartalmazza. Az egyes fejezetek kidolgozása során felhasznált forrásanyagok, hivatkozott könyvek, egyéb munkák referenciáit a hivatkozások rész tartalmazza, míg az egyes témák klasszikusan hivatkozott, eredeti forrásai külön részbe kerültek. A könyvben a felhasznált fontosabb kulcsszavak keresésében egy *név- és tárgymutató* segít.

Hogyan olvassuk a könyvet?

A könyv szerzői az egyes fejezeteket az ismeretek logikai sorrendjének megfelelően fűzték össze, alapul véve olyan meghatározó szakmai testületek ajánlásait, mint az ISACA (Information Systems Audit and Control Association). Az egyes fejezetek együttes ismerete ad teljes képet a területről, de akinek nincs lehetősége a teljes könyv elolvasására, annak javasoljuk, hogy tanulmányozza át az előszót és az ellenőrzési alapismereteket összefoglaló 1. fejezetet. A 1. fejezet több olyan informatikai meghatározást is tartalmaz, aminek megadása, inkább az egységes informatikai alap megteremtése miatt volt fontos (pl. az információtechnológia fogalma).

Fontosnak tartottuk, hogy az olvasóval közös informatikai alapról indulva tárgyaljuk az audit ismereteket. Akik most kezdenek ismerkedni ezzel a területtel, azoknak ajánljuk, hogy a fejezetek után található kérdéseket, esettanulmányokat tanulmányozzák át; szándékaink szerint ez segíti a megértést. Ugyanezt a célt szolgálják az egyes fejezetek vastagon kiemelt kulcsfogalmai is, amelyek egyfajta keretet adnak az egyes részterületek feldolgozásához. A könyv egyes fejezetei speciális ellenőrzési helyzetekben is hasznos segítséget nyújthatnak, pl. az auditálással kapcsolatos szabványok felhasználásánál és az ellenőrzés végrehajtásánál. A függelékben adott segédletek, ellenőrzést támogató táblázatok elsődlegesen az ellenőrzési projektekben hasznosíthatók.

Köszönetnyilvánítás

Köszönjük Gábor Andrásnak és Gábor Miklósnak a könyv megjelenéséhez nyújtott támogatását, szakmai segítségét. Köszönet illeti Dobay Pétert és Sántáné-Tóth Editet értékes észrevételeikért, javaslataikért. A könyv szerkesztésében sok segítséget kaptunk Halász Gézától, köszönjük neki. Végül köszönjük azoknak a hallgatóknak a támogatását, akik észrevételeikkel hozzájárultak az egyes témák érthetőbb tárgyalásához.

1 Áttekintés az ellenőrzés, auditálás fogalomköréről

Az információrendszerek auditálása a hagyományos *auditálás* egyfajta kiterjesztéseként alakult ki [Gallegos et al., 1999]. A hagyományos értelemben vett auditálás szó jelentése „vizsgálat". Általában egy működő rendszerre, folyamatra, termékre vonatkozik, megvizsgálva, hogy az mennyire felel meg az elvárásoknak, előírásoknak. A szó latin eredetű és a jelentése „hallgat", ami arra utal, hogy a vizsgálatot végző meghallgatta a vizsgálat alanyát majd ezt is felhasználva végezte el a vizsgálatot. A gazdálkodás, pénzügyek területén eredetileg az Itáliai kereskedő városokban alakult ki a számvitel, könyvelés tudományosan is megalapozott formája. Erre az időre vezethető vissza az ellenőrzéshez szükséges vizsgálat fogalmának és az audit szónak az eredete. Az ellenőrzési igénynek az információrendszerek körében való megjelenését a következő tényezők indukálták:

- Az információtechnológia fejlődésével a hagyományos auditálás tevékenységek elválaszthatatlanokká váltak a számítástechnikai környezettől, tevékenységektől.
- A vállalati vezetők felismerték, hogy az adatvagyon, az informatikai infrastruktúra a szervezet versenyképességét alapvetően meghatározó tényezők, így azok védelme, ellenőrizhetősége, biztonsága kulcsfontosságú.
- A szakmai szervezetek és egyesületek, valamint kormányzati szervek felismerték az információrendszer és informatikai auditálás szükségességét.

Az **információrendszerek auditálása** gyűjtőfogalom, amely magában foglalja a következő részterületeket:[2]

- technikai szempontú ellenőrzés (infrastruktúra, kommunikáció)
- a vezetés információtechnológia ellenőrzési eljárásainak auditálása
- az informatikai funkció/részleg szervezeti folyamatainak ellenőrzése, beleértve a szoftverfejlesztés és megvalósítás folyamatait, valamint az alkalmazási rendszerek ellenőrzését is és
- a nemzetközi és nemzeti szabványoknak való megfelelés vizsgálata.

A pénzügyi-gazdasági, pénzügyi és információrendszer illetve informatika területén végrehajtott ellenőrzések, vizsgálatok - angolszász eredetű szóval auditálások - sok rokon fogalmat használnak, azonban az értelmezésük jelentősen függ a környezettől. A pénzügyi illetve információrendszer vizsgálat estében is egyes fogalmak eltérő jelentést kapnak. Ezért a következőkben áttekintjük a nemzetközi és magyar szakirodalomban a határterületekkel kapcsolatban is előforduló kifejezéseket és szóhasználatot.

A nagy tanácsadó szervezetek[3] tipikusan két szolgáltatás nyújtanak az egyik a

[2] Informatikai auditálás

[3] Deloitte & Touche, Ernst & Young, KPMG, PricewaterhouseCoopers. Ezek a cégek korlátozott felelősségű partnerség vagy társulás formájában működnek általában (Limited Liability Partnerships, LLP), amire a magyar cégjogban a legközelebb eső forma talán az ügyvédi irodák működése; a betéti társaság és korlátozott felelősségű

tanácsadó[4] szolgáltatás, a másik *értékelés, biztosíték vagy garancia nyújtása*,[5]. Ezeknél a szervezeteknél, az alkalmazottak szakmai gyakorlata és szakértelme főképpen a következő területekre terjed ki:

- Hites könyvvizsgálók;
- Aktuáriusok (az aktuárius olyan szakember, aki a kockázatok kvantifikált pénzügyi hatásait elemzi és alkalmazza a gyakorlatban);
- Szervezési, vezetési szakemberek;
- Államigazgatási szabályozás szakértői;
- Információ feldolgozási szakemberek;
- Alkalmazottak szociális juttatásai és humán erőforrás gazdálkodás szakértői.

A *tanácsadó szolgáltatás* tipikusan két cég között jön létre azzal a céllal, hogy az információ felhasználására tegyen ajánlásokat a tanácsadó cég. A nagyvállalatok esetében tipikus példa nagyvállalat irányítási információrendszerek, illetve egyes elemeik bevezetésének támogatása, a folyamat elősegítése. Jellemző feladat a logisztikai feladatok, a logisztika, a szállítási tevékenységek eredményességének és hatékonyságának fokozása. Egy tanácsadó cégnek egy adott vállalatnál például az lehet a feladata, hogy hogyan lehet minimalizálni a költségeket, ha ismertek a raktárak elhelyezkedése, a raktárkészletek, a szállítási határidők, a rendelkezésre álló szállítási módok és a szállítmányok végcélja. Egy tanácsadási projektben a tanácsadó cégnek tehát az a feladata, hogy ajánlásokat dolgozzon ki arra, hogy hogyan lehet a rendelkezésre álló információkat felhasználni, de semmilyen értékelést nem ad, biztosítékot vagy garanciát nem nyújt azoknak az információknak a minőségére, amelyeket a javaslatai kidolgozásához felhasznál. Az előbb említett példában tehát az a tény, hogy a raktárkészletekre vonatkozó adatok korrektek-e vagy sem, nem ismertek a tanácsadó cég előtt, és ennek a kérdésnek a vizsgálatával nem is foglalkozik. Tehát egy tanácsadási projektben nem az információ minőségével, hanem annak használatával, felhasználásával foglalkoznak. Ezzel szemben az *értékelési* (*assurance*) (biztosíték vagy garancia nyújtási) projektek, általában háromoldalú szerződés keretében folynak le és céljuk az, hogy az *információ minőségét értékeljék*, illetve annak *valóságtartalmára, korrektségére, helyességére adjanak biztosítékot, garanciát*.

Ilyen szervezet Magyarországon például KERMI Minőségellenőrző és Szolgáltató Kft, amely bizonyos termékek minőségtanúsítását végzi, vagy a fogyasztók védelmét szolgáló egykori „Teszt magazin" illetve hasonló kiadványok valamint a, világhálón levő honlapok. Ezek a szervezetek a gyártóktól függetlenül tanúsítják a gyártók által megadott információkat, adatokat. A független minőségvizsgáló szervezet az egyik fél, a fogyasztók a másik fél, míg a gyártók a harmadik fél a szerző-

társaság jellemzőiből is tartalmaz bizonyos elemeket, a cég és a partner között jön létre egy cégjogi megállapodás. A partner anyagi kártérítési felelőssége a céggel szemben a saját befektetésének erejéig szól, noha az esetleges peres felek a partner magánvagyonával szemben is felléphetnek anyagi igényekkel. Egyik előnye többek között ennek a partnerségnek, hogy nagy kártérítési felelősség esetén a céget alkotó hálózatot viszonylag gyorsan fel lehet számolni anélkül, hogy az elemeknek jelentős kártérítési felelősséget kellene viselni. Lásd Andersen és Enron története, Andersen átalakulása Accenture-ré.

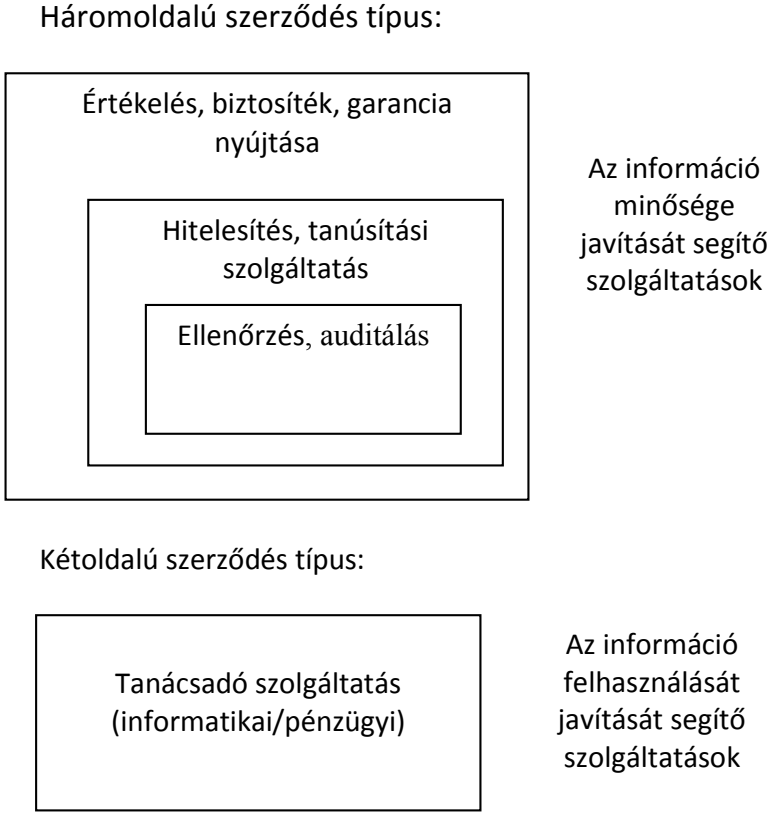
[4] Consulting

[5] Assurance

désben. Hasonlóak a minőségtanúsító szervezetek (pl. ISO 9000:2000), illetve az egyes tanúsító szervezeteket akkreditáló szervezetek. Ezek a szervezetek lehetnek könyvvizsgáló cégek, tanácsadó szervezetek, non-profit szervezetek, stb., amelyek nem fogadnak el pénzt az értékelő vizsgálatukért, és ezért általában a fogyasztók értékesnek találják az általuk közölt információkat. A nagy könyvvizsgáló cégek meglehetősen agresszív piaci magatartást és marketing stratégiát mutattak az utóbbi időben, amikor kialakították az *értékelő, biztosíték, garancia nyújtó szolgáltatásaikat* és ezek értékesítését igyekeztek megvalósítani [Telberg, 1996]. Például a PricewaterhouseCoopers felügyelte az Oscar díj átadásával kapcsolatos szavazásokat és *szavatolta* azok tisztaságát. Egy másik tanácsadó cég egy sport szervezet dopping szerekkel kapcsolatos programjának felügyeletét és korrektségének *szavatolását* végezte. Több másik cég a világhálón az elektronikus üzletvitellel kapcsolatban megjelenő üzlet-ügyfél (B2C, business-to-consumer) kapcsolatot támogató szoftver megoldások állításainak helyességét, azaz az üzleti folyamatok és az üzleti tranzakciók sértetlenségét, belső ellentmondás-mentességét *szavatolták*. Az értékelési és biztosítéknyújtási szolgáltatásokon belül egyeseket **hitelesítésnek (attestation)** hívnak, néhány hitelesítési szolgáltatást pedig **ellenőrzésnek, auditálásnak (audit)**. A *hitelesítés* egy olyan szavatosságot, biztosítékot nyújtó szolgáltatás, amelyben a hitelesítő valamilyen szavatosságot vagy garanciát nyújt egy olyan területre, esetleg írásbeli állításra vonatkozóan, amely terület egy másik fél felelősségi körébe tartozik.

Az Egyesült Államokban például, a PricewaterhouseCoopers hitelesítette egy egyetemi, főiskolai vizsgára felkészítő teszt sorozatot előállító és felkészítő tanfolyamokat indító cég meghirdetett eredményeit. Nevezetesen azt, hogy az egyetemre, főiskolára jelentkezők eredményei 115 ponttal javulnak a Nemzeti Vizsgáztató Testület pontszámításai alapján, és ha ez az eredményjavulás nem sikerülne, akkor a felkészítő tanfolyamot ingyenesen újra el lehet végezni. Ennek az állításnak a hitelességét *hitelesítette* PricewaterhouseCoopers, és a tanfolyamok tartásával foglalkozó cég írásban rögzített nyilatkozatát támogatta ezzel. A tanfolyamokat indító cég ezzel a támogatással fordulhatott a felvételizőkhöz és hirdethette tanfolyamait. Ebben a szerződéses viszonyban az *ügyfél* és az *állításokért felelős cég (client and responsible party)* a tesztekre felkészítő cég volt, a *hitelesítő,* pedig PricewaterhouseCoopers.

Azonban nem minden eset ilyen egyszerű. Például egy cég felvásárlása esetén, a felvásárló cég (ügyfél) alkalmaz egy olyan céget, amely egy olyan összefoglaló jelentést készít a felvásárolni szándékozott cégről (felelős fél), amelyben a jogszabályoknak és egyéb szabályozásoknak való megfelelőséget vizsgálja azokon a területeken, ahol a felvásárlás tárgyát képező cég nem bocsátott ki semmilyen hivatalos nyilatkozatot.



1. ábra. A biztosítéknyújtás, a hitelesítés, az auditálás és a tanácsadó szolgáltatások közötti viszonyrendszer

Az elmúlt évek folyamán az eredetileg könyvvizsgáló cégek az írásbeli nyilatkozatok és állítások széles spektrumát hitelesítették, amelyeknek semmi köze sem volt a számvitelhez, illetve a könyveléshez: nevezetesen szoftver specifikációk megbízhatósága, biztosítási kárigények, hipermarketek gondoláinak polcain az adott gyártó termékei által elfoglalt területek nagysága stb. tartoztak ide.

A gyakorlatban a cégek vizsgálatával, könyvvizsgálattal foglalkozó szervezetek két fajta hitelesítési szolgáltatást nyújtanak a pénzügyi, illetve pénzügyi-gazdasági területen. Az egyik az **átvilágítás (review, negative assurance)**, amit angolszász területen „negatív garanciaként" is emlegetnek. A másik a gazdasági eredményekről készített beszámoló, amely tartalmazza a *mérleget*, az *eredmény-kimutatást* és a *pénzalapforrás és felhasználás kimutatást*, helyesség ellenőrzését (angolszász eredetű kifejezéssel auditálását), és amelyet **pozitív garanciaként** is emlegetnek. *Átvilágítás* az, amelyre nem fordítanak annyi időt, mint egy alapos ellenőrzésre. Alapos *ellenőrzés*, részletes *értékelési* eljárás az, amire a viszonylag sok időt fordítanak a megalapozott hitelesítés, írásbeli nyilatkozat kibocsátása előtt. A fentiek alapján a **pénzügyi-gazdasági ellenőrzés, auditálás** meghatározása a következő:

A gazdasági eredményekről készített beszámoló (mérleg; eredmény-kimutatás, pénzalap forrása és felhasználása kimutatás) hitelesítése, amelynek során a pénzügyi vizsgálatot végző személy, cég szavatolja, biztosítékot illetve garanciát nyújt a vizsgált szervezet vezetése által kibocsátott gazdasági eredményekről szóló nyilatkozat helyességéről.

Egy ilyen szerződéses viszonyban a vizsgálatot végző cég *ügyfele* nem a vizsgált cég vezetősége, hanem a vizsgált cég *igazgatótanácsa*, akik a tulajdonosok és a részvényesek érdekeit képviselik.

A *pénzügyi-gazdasági ellenőrzés, auditálás* egy olyan szisztematikus eljárás, amelynek során a gazdasági eseményekről és tevékenységekről objektív módon gyűjtenek információt, és objektíven értékelik azokat. Ennek az eljárásnak az a célja, hogy az állított tények és az előírt vizsgálati szempontrendszer közötti bizonyos fokú megfelelőséget állapítsanak meg és az érdekelt feleket, felhasználókat tájékoztassák erről a megállapításról.

A fenti meghatározásból következik, hogy egy auditálás két részből áll: vizsgálatból és jelentés készítésből. A *vizsgálat* jelenti az adatok, tények, bizonyítékok összegyűjtését, amelyek a jelentés alapját alkotják. A *jelentés* az ellenőrzés megállapításait tartalmazza, vagyis azt, hogy vajon a vezetés pénzügyi-gazdasági beszámolója megfelel-e az általánosan elfogadott szakmai gyakorlatnak és jogszabályokban szabályozott számviteli, könyvelési szabályoknak [Nyikos, 2000]. A tudományos vizsgálat, az ellenőrzés és az auditálás módszere sok hasonlóságot mutat:

1. táblázat A tudományos vizsgálat és az auditálás

TUDOMÁNYOS VIZSGÁLAT	ELLENŐRZÉS, AUDITÁLÁS
A probléma megfigyelése és megértése	Egy szervezet azt kéri, hogy véleményezzék azt, hogy vajon a pénzügyi-gazdasági eredmény beszámoló adatai helyesen tartalmazzák-e az összes lényeges gazdasági mutatót tekintettel a pénzügyi helyzetre, az üzemi eredményekre és pénzáramlásra
Hipotézis felállítása	Hipotézis: a pénzügyi-gazdasági eredmény beszámoló adatai helyesek
Adatok, bizonyítékok, információk gyűjtése	Kockázat értékelése, az ellenőrzés folyamatának megtervezése
A bizonyítékok és tények kiértékelése és következtetések levonása	Azt kell kiértékelni, hogy vajon az adatok, bizonyítékok, információk alátámasztják-e, vagy visszautasítják-e a hipotézisben megfogalmazott állítást, vagy pedig nem vonható le megalapozott következtetés a rendelkezésre álló adatokból

1.1 Az informatikával, információrendszerekkel, információtechnológiával kapcsolatos ellenőrzés, vizsgálat (auditálás) fogalma

Mielőtt részletesen tárgyalnánk az auditálással kapcsolatos alapfogalmakat, az egységes értelmezés érdekében megadunk néhány olyan informatikai alapfogalmat, amely a tárgyalás keretét biztosítja. A továbbiakban az ellenőrzés, vizsgálat és audit, auditálás fogalmak szinonimaként szerepelnek.

Informatika (Informatics) alatt, az *információ* rendszeres és automatikus – elsősorban számítógépek segítségével történő – *rögzítésével*, *tárolásával*, *feldolgozásával* és *továbbításával* foglalkozó tudományt értjük [Molnár, 1997], [Breuer, 1995].

Ezért az informatika fogalma átfogja a számítógépek kivitelezhetőségével, megvalósíthatóságával kapcsolatos kutatásokat, a számítógépek és a szoftverek továbbfejlesztését, a számítógépek alkalmazását, és egyéb területeket is. Az Európában elterjedt informatika fogalma lefedi az USA-ban használt *computer science (számítástudomány)* és *data processing (elektronikus adatfeldolgozás)* fogalmát.

Az angolszász eredetű **információtechnológia,** röviden IT **(Information Technology)** [web 1.1], illetve a német eredetű információtechnika (Informationstechnik, Informationstechnologie) fogalma az informatikában a technológiai elemekre helyezi a hangsúlyt, vagyis a hardver, szoftver, távközlési, telekommunikációs és hálózati elemekre, amelyek a számítógépek fogalmát jelentős mértékben kiterjesztették [Molnár, 1997].

Az információtechnológia fogalma felölel minden, az információ és adatfeldolgozásra vonatkozó technológiai elemet. Vagyis idesorolható minden olyan eljárás, amely az adat- és információfeldolgozással foglalkozik, de idekapcsolódnak az egyetemi képzési formák és azok a szakmák, hivatások, amelyek ezzel a területtel foglalkoznak. Ide tartoznak olyan szakképzettségek, mint: alkalmazásfejlesztők, számítástechnikai szakember, számítógép-technikus, információrendszer tanácsadó, szakterületi informatikus (a rendszerintegráció és az alkalmazási rendszer szakterületétől függő, pl. gazdaságinformatikus, orvosinformatikus, stb.), médiumtervező (WEB designer), szoftverfejlesztő, rendszergazda, rendszeradminisztrátor, rendszerintegrátor.

Az **információrendszer (Information System)** azon eljárások, tevékenységek összessége, amelyek a szervezet működtetéséhez és irányításához szükséges információkat tárolják, előállítják és szétosztják [Molnár, 1997], [web 1.2].

A szervezetek tipikus információ típusai:

- a szervezet napi működéséhez szükséges, operatív információk (pl. számított bér)
- vezetői (döntéstámogató) információk.

Az információrendszer fogalmába szélesebb értelemben minden információ, illetve adatfeldolgozással, telekommunikációval foglalkozó rendszer is bele tartozik.

Az *informatikai ellenőrzés, auditálás* azonban nem pénzügyi-gazdasági vizsgálat. Egy ilyen ellenőrzés során a pénzügyi, gazdasági beszámoló vagy bármely hasonló jelentés helyességét nem vizsgálják. Az *informatikai ellenőrzés* nem hitelesítés (attestation).

> Egy **informatikai ellenőrzés (IT Audit)** célja az, hogy olyan bevizsgálási eljárásokat (teszteket) alkalmazzanak, amellyel meggyőződhetnek arról, hogy a vizsgált információrendszerekben alkalmazott *ellenőrzési és vezérlési mechanizmusok* (controls) helyesek-e.

Az ellenőrzési és vezérlési mechanizmusoknak szavatolniuk kell, garanciát kell nyújtaniuk a vezetés számára például arra vonatkozóan, hogy:

- a könyvelési és egyéb adatok helyesek-e;
- a programok helyesen és pontosan dolgozzák-e fel az adatokat;
- az alkalmazottak betartják-e az előírt irányelveket, szabályokat, és eljárásokat;
- a biztonsági, adatmentési és egyéb eljárások megfelelnek-e annak a célnak, hogy megakadályozzanak katasztrofális következményekkel járó adatvesztést, vagy az adatok helytelen módosítását.

Információrendszerek fejlesztésénél az informatikai vizsgálatnak azt kell biztosítania, hogy az ellenőrzési és irányítási mechanizmusok garantálják azt, hogy a projekt időben és a költségterven belül készül el, valamint az új rendszer kielégíti a projekt elején megállapított tervezési követelményeket.

> **Információrendszerek ellenőrzése, auditálása** egy olyan eljárás, amelynek során arról gyűjtenek adatokat, tényeket, bizonyítékokat, hogy a számítógéprendszer gondoskodik-e az informatikai vagyon (asset), védelméről, az adatok sértetlenségéről, lehetővé teszi-e, hogy a szervezet céljait ténylegesen és eredményesen megvalósítsa, és az erőforrásait hatékonyan felhasználja.

Az információrendszer vizsgálat céljai között szerepel egy tanúsítási cél, különösen a külső auditorok esetében, hogy vajon az informatikai vagyon és az adatok sértetlenségének védelme megfelelő-e, valamint a vezetés célkitűzései megvalósulásának a vizsgálata, amely nem csak a célok helyességének igazolásáról, hanem az eredményességi és hatékonysági kérdésekről is szól. Az informatikai vizsgálat elsődleges célja megbizonyosodni arról, hogy megfelelő, megbízható belső ellenőrzési és irányítási eljárásokat és mechanizmusokat alkalmaznak-e az adott szervezetben és ezek kielégítik-e az eredményességi és hatékonysági követelményeket. Az informatikai rendszerek, a gyakorlat és az üzemeltetés ellenőrzése általában magában foglalja a következőket is:

- a belső irányítási és ellenőrzési eljárások értékelése az érvényesség, megbízhatóság és biztonság szempontjai szerint

- az informatikai környezet eredményességének, hatékonyságának gazdasági szempontú értékelése.

Az auditálást végző szervezettel szemben fontos követelmény a függetlenség, vagyis a gyártó, szoftverfejlesztő nem értékelheti saját termékeit. Vannak olyan szervezetek, amelyek ezen a területen széleskörűen elismertek, meghatározzák a követendő szabványokat. Ilyen az ISACA (Information Systems Audit and Control Association, www.isaca.org), az auditorok nemzetközi szakmai szervezete, amely 1969-ben alakult, Chicagói székhellyel. Valamennyi földrészen, szinte minden államban vannak tagszervezetei, így Magyarországon is (1993 óta) [web 1.3], [web 1.4]. A nemzetközi szervezet alapvető célja az informatikai termékek és rendszerek auditálásának támogatása egyrészt a terület szabványosítási törekvésein keresztül, a képzés elősegítésével, valamint az auditorok szakmai hátterének biztosításával. A szervezet kidolgozta az információrendszerek ellenőrzésének és irányításának egységes keretbe foglalt módszertanát (COBIT - Control Objectives for Information and related Technology) [web 1.5], amely lefedi az összes fontosabb ellenőrzési szempontot, valamennyi fontosabb ellenőrizendő területet. Az auditálás kiterjedhet egyedi alkalmazásokra, adott munkafolyamathoz kapcsolódó rendszerekre, vagy összetett informatikai rendszerekre, megoldásokra.

1.2 Az audit jellemzői

Ebben a fejezetben az auditálás különböző típusait és azok jellemzőit tekintjük át. Megkülönböztetünk belső és külső ellenőrzést vagy auditot.

A **belső auditálás (Internal Audit)** a rendszerek biztonsági állapotának, megbízhatóságának, a biztonsági követelmények meglétének; a szervezet biztonságpolitikájának a megvalósulásával kapcsolatos követelmények teljesítésének; a belső szabályozók megfelelőségének, alkalmazásának folyamatos ellenőrzését jelenti.

A **külső auditálás** függetlenül és elfogulatlanul ellenőrzi a belső auditálást, a belső ellenőrzési és irányítási rendszer működését, a vizsgált rendszer biztonsági állapotát.

A biztonsági auditálást minden esetben egy olyan szervezet, szakértő, cég végzi, amely a vizsgált rendszer szervezetétől független (tehát nem befolyásolható) és az adott szakterület specialistája. Az audit terület egyik legfontosabb alapfogalma a kontroll, ami informatikai ellenőrzési és irányítási eljárást (vagy informatikai ellenőrzési és irányítási mechanizmus) jelent. A továbbiakban a kontroll meghatározásánál és használatánál a magyar megnevezést használjuk.

Informatikai ellenőrzési mechanizmusnak, kontrollnak (Control) hívjuk az informatikai rendszer kockázatainak mérséklésére szolgáló eljárásokat. Például: rendszerbe épített ellenőrzési eljárások, belső szabályozások, irányítási, vezetési tevékenységek stb.

A kontroll fogalma, kulcsfogalom az informatikai ellenőrzésben, központi sze-

repe van az audit szabványokban, így a COBIT-ban is. Ezért közöljük a COBIT szerinti kontroll fogalom meghatározását is:

„ellenőrzési mechanizmus, kontroll mindazon szabályok, eljárások, gyakorlati módszerek és szervezeti struktúrák összessége, amelyeket arra a célra terveztek, hogy kellő megerősítést nyújtsanak arra vonatkozóan, hogy az üzleti célkitűzéseket megvalósítják, és a nem kívánatos eseményeket megelőzik, vagy felderítik és korrigálják" [COBIT, 2007].

1.2.1 Az auditálás lehetséges céljai

A különböző területek ellenőrzése más és más célból történhet. A kívülről, *hatóságilag kötelezővé tett auditálás* a külső érintetteket informálja a vállalat működéséről, a működés felügyeletéről, adott korlátok és szabályok alkalmazásáról. Ezek az előírások minden hasonló tevékenységű vállalatra egyformán érvényesek, így a megbízhatóság és a felügyelet mellett az egyenlőbb esélyek, a tisztességesebb verseny kialakulása felé is hatnak. Más a helyzet az *önként vállalt és folytatott auditálás*sal. Itt a vállalat a saját jól felfogott érdekében törekszik az önellenőrzés és fejlődés minél magasabb szintjére kerülni. Így nagyobb mértékben tudja kontrollálni a folyamatait és a terveinek megvalósítását. A hatóságilag előírt auditálások végrehajtója a külső, független auditor, bár még ez sem garancia a tökéletes objektivitásra. Saját kezdeményezésre végzett auditálásnál sem ritka a külső megvalósítás. Ennek előnye a nagyobb objektivitás és a többirányú tapasztalat, viszont nem biztos, hogy egy kívülálló számára kellően átláthatóak a belső folyamatok.

1.2.2 Az információrendszer-ellenőr, az auditor

Az auditor[6] akár külső, akár belső ellenőrzést végez, munkája során nemzetközi és nemzeti szabványokra kell támaszkodnia. Az információrendszer-ellenőrök nemzetközi szakmai szervezete, az ISACA és annak nemzeti szervezetei nyújtanak elsődlegesen támogatást a képzéssel és a minősítés megszerzésével kapcsolatosan (ISACA Model Curricula). Több szakmai tanúsítvány szerezhető meg, de az általánosan, nemzetközileg is elfogadott a *CISA (Certified Information Systems Auditor)* képesítés. A képzésbe több szinten is be lehet kapcsolódni, így egyrészt a szakmai szervezetek által szervezett szemináriumokon való részvételt, a hagyományos egyetemi oktatást kell megemlíteni. Az elméleti ismeretek megszerzésén túl hangsúlyos szerep jut a gyakorlati tapasztalatoknak. Az auditoroknak a technikai szabványok betartásán túl alkalmazniuk kell az *ISACA szakmai etikai kódex*ének ajánlásait (ISACA Code of Ethics, www.isaca.org) is.

---

[6] Példák egyéb pénzügyi ellenőrzéssel és auditálással foglalkozó nemzetközi és magyar szervezetekre (a felsorolás nem teljeskörű):
AICPA, *American Institute of Certified Public Accountants* – Okleveles Könyvvizsgálók Amerikai Egyesülete
CICA, *Canadian Institute of Chartered Accountants* – Okleveles Könyvvizsgálók Kanadai Egyesülete
A Magyar Könyvvizsgáló Kamara, Pénzügyi-Gazdasági Ellenőrök Egyesülete

1.3 Az információrendszerek ellenőrzési és irányítási céljai és eljárásai

Az ellenőrzés eredménye többféle módon nyilvánulhat meg:

- A működés kockázatainak csökkenése.
- A vállalat belső előírásainak ellenőrzése javul, biztosíthatják a környezeti és belső kockázatok minimalizálását, a károk, balesetek és katasztrófák elkerülését, valamint a külső előírásoknak való megfelelést.
- Jobban megállapítható, hogy a vállalat mennyire tud ma, illetve mennyire lesz képes a jövőben megfelelni a piac által diktált feltételeknek és az érvényes jogi előírásoknak.
- A vállalatról kialakított vélemény javítása.
- A vállalat fogyasztóinak, partnereinek biztosítása a magas megbízhatóságról, ezáltal piaci előnyök szerzése a konkurensekkel szemben.
- Pénzügyi megtakarítások elérése.

A jobb ellenőrzés nagyobb hatékonyságot jelent. Emellett például egyes bankoknál kedvezőbb hitelfelvételre nyílhat lehetőség, valamint környezeti kockázatokra vonatkozó biztosítás kötése esetén a biztosítási díj megállapításánál figyelembe veszik az auditálás eredményét. Az ellenőrzési eljárások (controls) csoportosítása többféle szempont szerint történhet. Megkülönböztetünk általános informatikai ellenőrzési eljárásokat; és alkalmazáshoz kötött, alkalmazás-specifikus ellenőrzési eljárásokat.

1.3.1 Az általános informatikai ellenőrzési eljárások (control)

Az **általános ellenőrzési eljárások (General Controls))** azok az ellenőrzési mechanizmusok, amelyeket azért terveztek és valósítottak meg, hogy biztosítsák a szervezet ellenőrzési rendszerének stabilitását és magas színvonalú irányítását, továbbá erősítsék az alkalmazási szintű ellenőrzések eredményességét.

A szervezet vezetésének felelőssége és feladata a működési tevékenységek irányítása és ellenőrzése, továbbá a szervezeti irányelvek és a járulékos eljárások felállítása, ismertetése az alkalmazottakkal, valamint a megvalósulás nyomon követése. Ki kell alakítani az *ellenőrzések szükségességének tudatát*, amely az ellenőrzési rendszer alapját alkotja. A szervezeti működési szabályzattal együtt kell megfogalmazni olyan etikai és viselkedési elveket, normákat, amelyek elősegítik a fegyelmezett ellenőrzési környezet eredményes működését. Az ezeket tartalmazó *etikai kódex*nek ki kell terjednie az automatizált, számítógépes rendszerekre is. Sok szervezetnél rendszeresen (félévente, évente) aláíratnak egy etikai nyilatkozatot minden alkalmazottal, hogy a számítógépet, automatizált rendszereket csak a szervezet céljaira lehet felhasználni és bármilyen illetéktelen használat, csalás, vagy visszaélés büntető feljelentést von maga után. Az automatizált rendszerek ellenőrzésének kialakításánál figyelembe kell venni, hogy a számítógép sebessége, az adatok közötti ellentmondás-mentesség, belső konzisztencia, a rugalmasság a következő kérdéseket veti fel:

- A hibák sokszorta nagyobb károkat okozhatnak, mint egy manuális rendszerben. (Pl. a munkanélküli segély kifizetéseknél az adóelőleg, vagy TB járulék számításnál rossz százalékokat vagy számokat használnak fel, mert egy korábbi változathoz nyúlnak valamilyen okból vissza, akkor az összes kifizetést rosszul fogják számfejteni. Ez a példa az automatizált rendszeren belüli konzisztencia fontosságát emeli ki.)

- A manuális tevékenységek csökkenése a rendszeren belül esetleg a szervezeti működési, funkcionális területek nem megfelelő szétválasztásához vezethet.
- A nyomkövetési, ellenőrizhetőségi tevékenység napló (audit trail) szerepe lényegesen csökkenhet, esetleg megszűnhet, vagy csak egy rövid időre létezik számítógéppel olvasható formátumban [BLANCO, 2002].
- A pénzügyi adatok illetve a programok változtatását esetleg olyan hozzá nem értő személyek végzik el, akik nem értik teljesen a pénzügyi folyamatokat, szabályokat, ellenőrzési mechanizmusokat, további veszély az, hogy megfelelő tesztelési eljárások illetve, a vezetés tudomása nélkül hajtják végre a változtatásokat.
- A pénzügyi adatokhoz sokkal többen férhetnek hozzá, mint a korábbi manuális rendszerek esetében volt.

Egy szervezet számára az adatfeldolgozási rendszer fölötti ellenőrzési mechanizmusok bevezetésének két legfontosabb célkitűzése az, hogy ésszerű biztosítékot jelentsenek a következők tekintetében:

- a programok fejlesztése, változtatása a használatba vétel előtti előzetes engedély, felhatalmazás, alapos tesztelés, és ezek fényében történő végleges jóváhagyás után történhet;
- az adatállományokhoz csak korlátozottan, az arra felhatalmazott felhasználók és programok férhetnek hozzá.

1.3.2 Az alkalmazás-specifikus informatikai ellenőrzési eljárások (application controls)

Az **alkalmazás-specifikus ellenőrzési eljárások (Application Controls)** egy-egy alkalmazáshoz kötődnek. Egy lehetséges csoportosításuk a következő:

- bemeneti adatok ellenőrzési eljárásai
- adatfeldolgozási ellenőrzési mechanizmusok
- kimenő adatok ellenőrzési eljárásai.

A **bemeneti adatok ellenőrzési eljárásai (input controls)** esetében a cél annak a biztosítása, hogy a rendszerbe bevitt adatok pontosak, teljesek, és ellenőrzöttek legyenek. A bemenő adatok (input) ellenőrzése, a manuális és az alkalmazásba beépített számítógépes ellenőrzési eljárások kombinációja. Manuális ellenőrzési eljárás például a hibás bemenő adatok kezelésére vonatkozó eljárás. Számítógépes ellenőrzési eljárások lehetnek például a sorozatszám ellenőrzése, automatikus egyeztetések, stb.

Az **adatfeldolgozási ellenőrzési mechanizmusok (process controls)** célja

annak biztosítása, hogy az érvényes bemeneti adatokat pontosan és teljes körűen dolgozzák fel. További feladatuk a feldolgozás ideje alatt az adatokon végrehajtott véletlen, vagy szándékos változtatások elleni védelem. Céljuk tehát annak a biztosítása, hogy a

- feldolgozott tranzakciók pontosak és teljesek legyenek
- minden tranzakció egyedi és érvényes legyen
- valamint a számítógépes feldolgozás ellenőrizhető legyen.

A **kimenő adatok ellenőrzési eljárásai**nak **(output controls)** a célja, hogy a számítógépes kimeneti adatok (outputok) teljesek és pontosak legyenek és szétosztásuk megfelelően szabályozott módon történjen. Lehetséges kockázatok: bizalmas anyagok illetéktelen kezekbe jutása, esetlegesen megváltoztatása. Az alkalmazások által kibocsátott kimeneteknek tehát ki kell elégíteniük a következő követelményeket:

- teljesség
- pontosság
- szétosztás szabályozottsága.

Az alkalmazásokra vonatkozó fontosabb ellenőrzési eljárások a függelékben található alkalmazás szintű ellenőrzést támogató mátrixokban, összefoglalva láthatóak.

1.3.3 Megelőző, észlelő és helyreállító informatikai ellenőrzési eljárások és mechanizmusok

Az ellenőrzési eljárások egy másik lehetséges csoportosítása, a betöltött funkciók alapján a következő:

- megelőző
- észlelő és
- helyreállító eljárások.

A **megelőző ellenőrzési eljárások (Preventive Controls)** megelőzik és korlátozzák a hibák, hiányosságok, valamint a nem engedélyezett hozzáférés és használat előfordulását, felmerülését. Ilyen eljárás a minőségi személyzet alkalmazása (kiküszöböli a hozzá nem értésből származó problémákat), a fizikai hozzáférés korlátozása, a hozzáférés-jogosultsági szoftverek használata, a dokumentáció alapos tervezése, a felelősségi körök szétválasztása.

Az **észlelő ellenőrzési eljárások (Detective Controls)** a hibák, hiányosságok, nem engedélyezett hozzáférés és alkalmazás detektálására használatosak. Példaként említhetjük a számlák feldolgozása során használatos „mindösszesen" ellenőrző összeget (control totals), a számítások duplikált ellenőrzését, a telekommunikációban használatos visszhang ellenőrzést (echo controls[7]).

[7] Az echo control vonalhibák ellenőrzésére szolgál. Az adatokat visszaküldik annak az eszköznek, ahonnan kapták, majd összehasonlítják az eredeti továbbítás jellemzőivel.

A **helyreállító ellenőrzési eljárás (Corrective Controls)** a hibák, hiányosságok nem engedélyezett hozzáférés és használat észlelése után támogatja a korrekciót. Ilyen eljárás a katasztrófa utáni helyreállítási terv, újrafuttatási eljárások, visszatöltési eljárások, hálózati tartalékvonalak konfigurálása.

1.4 Az audit végrehajtása

Az információrendszerek auditálása összetett feladatot jelent. Az auditornak a kockázatok felmérése után olyan auditálási programot kell meghatároznia, amely tartalmazza az ellenőrzés céljait és azokat az eljárásokat, amelyekkel ezek a célok elérhetők, kielégíthetők. Az auditor feladata eldönteni, hogy az auditálás során mely ellenőrzési mechanizmusok vizsgálata szükséges. Az auditálás megfelelő tervezése az a szükséges előkészítő tevékenység, amely hatékony végrehajtást eredményezhet.

Az auditálás tervezése során az első feladat a kockázatok felmérése, majd kezelése. Ehhez először szükség van annak az üzleti környezetnek az értelmezésére, megismerésére, amelyben a szervezet működik. Ennek alapján azonosíthatók és kategorizálhatók azok a kockázatok, amelyek meghatározzák az auditálás lefolytatását.

A **belső kockázat (Inherent Risk),** olyan hiba előfordulásának kockázata, amelyre nincs helyettesítő ellenőrzési eljárás.

Az **ellenőrzési mechanizmus**ból eredő kockázat **(Control Risk),** annak a kockázata, hogy a belső ellenőrzési eljárások során fel nem tárt, vagy nem megelőzött hibák, hiányosságok maradnak.

Az **észlelési kockázat (Detection Risk),** annak a kockázata, hogy az auditor nem megfelelő teszt eljárást alkalmaz az auditálás során és így figyelmen kívül hagy lényeges hiányosságokat, hibákat.

Az **audit kockázat (Overall Audit Risk)** összetevői a belső (inherens) kockázat, az ellenőrzési mechanizmusból eredő kockázat, és az észlelési kockázat.

Az auditálandó területek meghatározása előtti kockázatfelmérésnek számos oka lehet:

- támogatja a vezetést a források hatékony csoportosításában, elkülönítésében;
- segíti az auditálási célok beillesztését az üzleti tervekbe, megfelelteti azokat a szervezeti céloknak;
- megalapozza az auditálási részleg vezetését, irányítását;
- megbízható információkkal szolgál a magas üzleti kockázatú területekről.

A kockázatok felmérésére számos eljárást használnak. Az egyik lehetőség a mutatószámrendszerek (scoring system) alkalmazása az auditálandó területek prioritási sorrendjének megállapítására. Egy másik megközelítés olyan döntésen alapul az auditálási terület kijelölésében, amely a vezetői irányelveket, előző tapasztalatokat, az üzleti környezetet veszi figyelembe.

1.4.1 A kockázat-alapú audit lépései

A **kockázat-alapú audit (Risk-based Audit Approach)** legfontosabb lépései a következők:

- információk gyűjtése
- belső ellenőrzési eljárások megértése
- megfelelőségi teszt
- részletes vizsgálat
- az auditálás lezárása.

Az **információgyűjtés (Gather Information and Plan)** célja, hogy az auditor a vizsgálandó ellenőrzési eljárásról, annak üzleti és szervezeti környezetéről minél többet tudjon meg. Így azonosításra kerülnek az érintett egyének, folyamatok, helyszínek, és azok az eljárások, amelyek érintettek az ellenőrzési mechanizmusban. A kellő információhoz belső anyagok, és személyes interjúk révén lehet hozzájutni. Az *információ**gy**űjtés* lehetséges témakörei:

- üzleti elvárások és a kapcsolódó kockázat
- szervezeti struktúra
- feladatok és felelősök
- vállalati politika és eljárások
- jogok és szabályok
- ellenőrzési mechanizmus (control) eszközök
- riportok
- érintett IT erőforrások.

A lépés során nagyon fontos a részletes dokumentálás, ami biztosítja a teljes megértést és a további munka gördülékenységét. A megválaszolandó kérdések:

- ki végzi az ellenőrizendő feladatot,
- hol végzi,
- mikor végzi,
- melyek a feladathoz szükséges bemenetek,
- milyen kimeneteket kell szolgáltatnia a feladatnak,
- hogyan történik a megvalósítás az elképzelések szerint.

A **belső ellenőrzési eljárások megértése (Obtain Understanding of Internal Controls)** során az auditor vizsgálja az ellenőrzési eljárások összességét és azok környezetét, értékeli az észlelési kockázatot, felméri a teljes audit kockázatot.

A **megfelelőségi teszt (Compliance Test)** a külső előírások betartásának, a szabványok szerinti működésnek, a szabályszerűségnek a vizsgálata, a tesztelésre kiválasztott ellenőrzési mechanizmusok megfelelőségének értékelésén keresztül.

A kockázat-alapú auditálás következő lépése a **részletes vizsgálat (Substantive Test).** A részletes vizsgálat során történik meg a lényegi szempontok tesztelése, a helyesség és a sértetlenség ellenőrzése (például tranzakcióké stb.).

Az **auditálás lezárása (Conclude the Audit)** során véglegesítik az audit jelentést, megfogalmazzák a javaslatokat és az auditot követő tevékenységeket. Az **audit jelentés (Audit Report)** az audit folyamat terméke, az ellenőrzés során kialakított alapdokumentum. Az audit folyamat értékelése a következő szempontok alapján történhet [Gallegos, 2002]:

- *Teljesség* (Completeness) – az audit során az összes ellenőrzésre kiválasztott alkalmazás vizsgálatra került.
- *Helytállóság* (Pertinence) – az audit csak a tárgyhoz tartozó elemekre terjed ki.
- *Pontosság* (Accuracy) – az audit valamennyi része precíz, hibamentes.
- *Megfelelő tények, következtetések és ajánlások* (Appropriate Conclusions, Findings and Recommendations) – az audit során feltárt tények, következtetések az audit célokhoz illeszkedő, a költségeket kézben tartó, kivitelezhető és megfelelően ütemezhető megoldásokat eredményeznek, a menedzsment számára érthető nyelvezeten.
- *Követő tevékenységek* (Follow-up) – az audit folyamat hozzáadott értéket eredményez a vizsgált szervezet számára.

1.4.2 Az audit program

Az audit program támogatja az audit céljainak kielégítését, foglalkozik az audit tárgyával, céljával, vizsgálati körével, az adatgyűjtési eljárásokkal, az eredmények kiértékelési eljárásaival.

Az **audit program (Audit Program)** olyan dokumentált auditálási eljárások összessége, amelyek a tervezett auditálás célok kielégítését szolgálják.

Az audit program egy tipikus felépítését mutatja a 2. táblázat [CISA Review Technical Information Manual, 2005]. Az audit programnak a táblázatban bemutatott felosztása nem szükségszerű, de adhat egyfajta iránymutatást az auditálás során. Az auditor tevékenysége összetett, manuálisan gyakran nem kivitelezhető. Az ellenőrzésben gyakori a számítógépes támogató alkalmazások használata, ezzel foglalkozik a következő fejezet.

2. táblázat Az audit program szakaszai

AZ AUDIT SZAKASZ	LEÍRÁS
Az audit tárgya	Az auditálandó területek meghatározása
Az audit célja	Az auditálás céljának meghatározása
Az audit hatásköre	A vizsgálatba bevont rendszerek, szervezeti egységek, funkciók azonosítása
Az előzetes auditálási terv	Az audithoz szükséges erőforrások és szakértelem azonosítása A tesztek elvégzéséhez szükséges információforrások, valamint helyszínek azonosítása
Az adatgyűjtés eljárásai	Az interjúba bevont személyek körének megállapítása

	Azoknak az auditálási eljárásoknak a meghatározása, amelyekkel az ellenőrzési mechanizmusok tesztelése és verifikálása történik
Az eredmények kiértékelésének eljárásai	Szervezet-specifikus
A menedzsmenttel való kommunikáció eljárásai	Szervezet-specifikus
Az audit jelentés kialakítása és tartalma	Az üzemeltetési hatékonyság és eredményesség tesztelésére és kiértékelésére szolgáló eljárások Az ellenőrzési mechanizmusok tesztelési eljárásai A dokumentáció, eljárások és gyakorlat áttekintése és kiértékelése A további lépések, követő eljárások meghatározása

1.4.3 Tényfeltáró technikák

Az auditálási folyamat egyik kulcslépése az ellenőrzési bizonyítékok, tények összegyűjtése, a tényfeltárás. Ezt a részfolyamatot számos technika támogatja. A szervezeti felépítés vizsgálata például segítheti a felelősségi körök megfelelő szétválasztásának ellenőrzését. Az információrendszer dokumentációs szabványok, valamint rendszerdokumentációk vizsgálata során ellenőrizhetők többek között a rendszerfejlesztés auditálás vonatkozású kérdései, a dokumentációs követelmények betartása. Az auditor munkáját elsődlegesen a megfelelő személyekkel készített interjúk felhasználása, a működés megfigyelése, a kulcs ellenőrzési eljárások (kontrollok) tesztelése támogatja. Az auditor támaszkodhat (bizonyos esetben támaszkodnia kell) a statisztika által kínált eszköztárra, így pl. a mintavételezés statisztikai megoldásaira. Ugyanakkor az auditor személyes döntésén alapuló nemstatisztikai típusokra is (pl. attribútum mintavételezés, „fix méretű" („mennyi?"), stop-or-go, felfedező eljárások) [CISA Review Technical Information Manual, 2005]. Az audit során gyakran használnak fel számítógépes eszközöket, megoldásokat. Ezek a megoldások a számítógéppel támogatott audit kategóriába tartoznak, angol rövidítésük *Computer Assisted Audit Techniques, CAAT*.

A **számítógéppel támogatott audit (Computer Assisted Audit Techniques, CAAT)** körébe tartozik minden olyan szoftver amelyet az audit folyamatban felhasználnak. Elsődlegesen az adatgyűjtésen és elemzésben alkalmazott szoftvereket említhetjük példaként, így az Excel, SAS, Access, Business Object által kínált funkciók tipikusak. Vannak olyan szoftverek is amelyeket kifejezetten az ellenőrzés céljainak megfelelően fejlesztettek ki, ilyen pl. az Audit Command Language (ACL) és az Interactive Data Extraction and Analysis (IDEA). Néhány további CAAT példa:

- teszt generátor
- szakértő rendszer
- pillanatfelvétel (snapshot)

- nyomon követés (SCARF).

Használatuk előnyei közé tarozik, hogy csökkentik az auditáló személyétől való függést, mérséklik az ellenőrzés kockázatait, megkönnyítik a kivételek kezelését, gyorsabb hozzáférést tesznek lehetővé a vizsgált adatokhoz, rendszerekhez, általában költségkímélő megoldások.

Ellenőrző kérdések

1. Mit értünk informatikai és információrendszer ellenőrzés (audit) alatt, milyen célból történik (történhet) a különböző területek ellenőrzése?
2. Milyen részekből épül fel az ellenőrzés (auditálás)?
3. Milyen auditálási típusokat ismer?
4. Mit értünk ellenőrzési eljárás (control) alatt és milyen típusait ismeri? Mindegyik típusra adjon példákat is!
5. Mi az ACL és GAS, és mire használják őket az auditorok?
6. Milyen körülmények motiválják a GAS használatra az auditorokat?
7. Soroljon fel CAAT-ket és csoportosítsa azokat! Vegyen igénybe Internetes forrásokat is!)
8. Hogyan kell az IT Audit riportot összeállítani, mire kell fokozottabban figyelni?
9. Milyen szempontok érvényesülnek az auditor értékelésekor?
10. Milyen az auditot követő tevékenységeket tudna említeni?

Internetes feladatok

1. Keresse fel az ISACA web (www.isaca.org) oldalát és ellenőrizze milyen támogatást nyújtanak az felsőfokú oktatás résztvevői számára!
2. Nézzen utána, milyen az auditálással összefüggésbe hozható törvények születtek hazánkban az utóbbi időben!
3. Keressen információkat az elektronikus kereskedelem és az auditálás összefüggéseiről!
4. Keressen példákat CAAT-re! Mi a Generalized Audit Software és mire használják az ellenőrzés során?
5. Keressen auditálással foglalkozó független szervezeteket! Készítsen rövid összefoglalót tevékenységi és felelősségi körükről!
6. Keressen felsőoktatásban részt vevő hallgatóknak szóló auditálással kapcsolatos szakmai rendezvényeket, továbbképzési lehetőségeket (www.isaca.org, www.isaca.hu)!