Pető Dávid

Információrendszerek Tanszék

Témavezető: Dr. Gábor András

Budapesti Corvinus Egyetem

Gazdálkodástani Ph. D. program

Aki mér, az nyer

Kockázatértékelési metrika az információtechnológiai auditálásban

Ph. D. értekezés

Pető Dávid

Budapest, 2006.

Tartalomjegyzék

Ábrák jegyzéke

Köszönetnyilvánítás

Ezúton szeretném kifejezni köszönetemet mindazoknak, aki a kutatás végrehajtása és a dolgozat megírása folyamán mellettem álltak. Köszönettel tartozom elsősorban témavezetőmnek, Dr. Gábor Andrásnak, aki szakmai tudásával, átfogó szemléletével, és nem utolsó sorban empátiájával mindig segített túljutni a holtpontokon.

Köszönöm kollégáimnak, akikkel a különböző kutatásokban és a COBIR projektben együtt dolgozhattam. Ezek során a dolgozatban is hasznosítható elméleti és gyakorlati tudást szerezhettem tőlük.

Köszönöm továbbá családomnak, akik türelmükkel és odaadásukkal lehetővé tették, hogy egész idő alatt a kutatásra összpontosítsak, és akik mindvégig bíztak bennem.

I. FEJEZET
Bevezetés

I.1. Az értekezés áttekintése

A dolgozat célja a vállalati informatika vizsgálatában használható kockázatértékelési metrika kutatásának ismertetése. Megvilágítja a megfogalmazott célokat, a kutatás jelentőségét, a felmerülő problémákat, a megoldás módszerét és az elért eredményeket.

Az értekezés elején a megoldandó feladatot ismerhetjük meg: az átfogó informatikai kockázatértékelési mutató előállítását. Bemutatásra kerülnek a tervezett módszer előnyei is, illetve azok a megoldandó problémák, amelyeket a munka során figyelembe kellett venni. A fejezet továbbá kitér arra is, hogy a kockázatértékelési metrika milyen módon segítheti a vállalati informatikai funkció hatékonyabb működését.

Szintén a II. fejezetben szerepelnek a kutatás során ellenőrzött kérdések, és a vizsgált hipotézisek. Ezek a feltevések a kockázatértékelési metrika megalkotásához és használatához kapcsolódnak. A kutatás megközelítése újszerű, eddig kevéssé volt elterjedt. A kockázatok mértékének megítélésekor ugyanis a javasolt módszer figyelembe veszi az egyes tényezők közötti kölcsönhatásokat is.

A III. fejezet mutatja be azt a környezetet, amelyben a felvetett probléma értelmezhető. Megismerhetjük az információtechnológiai auditálással kapcsolatos főbb megállapításokat, illetve az eddigi kutatások eredményeit. A rész elsőként az auditálás áttekintésével foglalkozik, bemutatja a főbb fogalmakat, amelyek a kutatáshoz kapcsolódnak. Előtérbe kerül az informatikai ellenőrzés és az auditálás definíciója, illetve az auditálási területek viszonyai.

Ebben a fejezetben az informatikai auditálás kialakulásának útja is ismertetésre kerül. A kutatás jelentőségének alátámasztása céljából a dolgozat

kitér a fejlődés egyes lépcsőire és bemutatja, hogy az auditálás fejlődésében milyen jelentősége van a kutatásnak.

Az informatikai auditálás fontosabb módszereit, és a kapcsolódó előírásokat a IV. fejezetben ismerhetjük meg. Az értekezés megkísérli összehasonlítani őket, elsősorban a kutatás során való használhatóságuk szempontjából. Nagyon nehéz teljes képet adni a szóbajövő módszerekről, de feltétlenül szükséges legalább az elterjedtebb, ismertebb és nagyobb területeket, átfogó módszereket röviden bemutatni.

Ezek után következik a kockázatok értékelésének tárgyalása. Az V. fejezetben áttekintést kapunk a kockázatértékelés szerepéről az informatikai auditálásban, és arról, hogy a kutatás céljaként kitűzött metrikának milyen szerepe lehet ezen a területen. Megismerhetjük a kitűzött feladat elvégzése során felmerülő nehézségeket, illetve azokat a problémákat, amelyekkel a kutatás kivitelezése során kellett szembesülni. A fejezet bemutatja azokat a legelterjedtebb többtényezős eljárásokat, amelyek a kockázatértékeléshez kapcsolódóan a metrika megalkotását szolgálhatják, és amelyeket a kutatás során kiindulópontként lehet felhasználni.

A VI. fejezet tartalmazza a kutatás tervezetét, a hipotézisek operacionalizálását (tehát azt az eljárást, amellyel ellenőrizhetők), továbbá egy rövid áttekintést azokról a meglévő eredményekről, illetve felhasználhatóságukról, amelyek a feladat megoldását lehetővé teszik.

A megoldás menetét, a kutatás végrehajtásának módját a VII. fejezetben olvashatjuk. Itt kerül sor a kutatás részletes bemutatására, a megalkotott kockázati mutatószám ismertetésére, majd a metrika használatának szimulálásával kapott eredmények közlésére. A fejezet végén találhatók a kutatási hipotézisek ellenőrzésének eredményei.

A dolgozat végén az elért eredmények ismertetésén túl a további kutatási irányok és feladatok számbavételére kerül sor. Az értekezést a függelékben elhelyezett részletes statisztikai kimutatások és grafikonok teszik teljessé.

I.2. A kutatási területről

Az információtechnológiai auditálás – mint a számítógépekhez kapcsolódó tudományok általában – viszonylag rövid múltra tekint vissza. Üzleti felhasználású számítógépek mindössze fél évszázada léteznek, és az ezekhez kapcsolódó ellenőrzések természetesen az információtechnológia térhódításával kerültek előtérbe. A pénzügyi ellenőrzés azonban – mint látni fogjuk – igen komoly hagyományokkal rendelkezik, több évszázados, egyes felfogások szerint több évezredes múltra tekint vissza. Az információtechnológiai auditálás pedig nem független a pénzügyi ellenőrzéstől, hanem amint szintén látni fogjuk, szervesen illeszkedik annak fejlődési vonalába. Az IT audit tehát valójában egy viszonylag új szegmense egy hosszú ideje létező eljárásnak, és annak részeként – vagy kiegészítéseként – kezelendő.

Az információtechnológiai audit célja valamely szoftvertermék, szoftverfejlesztési eljárás vagy vállalati információrendszer biztonsági szempontokból történő módszeres értékelése. Az auditálás az előre rögzített szabályoknak való megfelelést vizsgálja.

A számítógépes információrendszerek auditálása több módon történhet. Már meglévő rendszerek esetében az aktuális állapotból kiindulva kell felmérni annak kockázatait, és a felállított szabályoknak való megfelelését. Folyamatban lévő fejlesztések, rendszerbevezetések esetén pedig célszerű ellenőrizni, hogy azok a kontrollok, amelyek a rendszer ellenőrizhetőségét lehetővé teszik, megfelelő módon beépítésre kerülnek-e a rendszerbe. Ellenőrizhető maga a projektszervezet is abból a szempontból, hogy a fejlesztés során milyen eljárásokat követnek, és eleget tesznek-e a biztonsági kívánalmaknak. Az auditálás látókörét természetesen a vizsgált probléma természetétől függően kell megválasztani.

Az auditálás eredménye egy audit beszámoló (*report*), amely tartalmazza a vizsgált területekre vonatkozó megállapításokat. Ennek részeként a fennálló vagy várható kockázatok elemzésére is ki kell térni. Be kell mutatni,

hogy az egyes kockázati tényezők milyen súlyúak a vizsgált terület esetében, és bekövetkezési valószínűségüket célszerű a körülmények figyelembevételével előre jelezni.

Az informatikai kockázatok értékelése, mint bármely kockázatértékelés, rendkívül nehéz feladat. A kockázat valamely véletlen esemény bekövetkezését jelenti, és így mérése közvetlenül kapcsolódik a bekövetkezési valószínűségekhez. Ugyanakkor az egyes tényezők kockázata sokféleképpen adódhat össze, és egymással kölcsönös függésben lévő események láncolata bekövetkezési valószínűségeinek becslését feltételezi. Ráadásul az IT audit esetében a kockázatok megítélése is rendkívül szubjektív lehet, és ez tovább nehezíti azok számszerű mérését.

Feltehetőleg ez az oka, hogy egyelőre nem létezik széleskörűen elterjedt eljárás, amellyel a vállalati informatikában rejlő kockázatokat számszerűen értékelni lehet. Bár történtek kísérletek ilyen metrikák megalkotására, ezek egyrészt csak valamely részterület értékelését tűzték ki célul, másrészt többnyire megállapodásos, vagy éppen véletlenszerű mértékeket alkalmaznak. A szubjektív, emberi tényező szerepe túlságosan nagy az értékelésben ahhoz, hogy az összehasonlíthatóság minden esetben fennálljon.

Az információtechnológiai auditálásnak nincs általános érvényű szabványa, bár számos szabványosítási kezdeményezés létezik. A legelterjedtebb szempontrendszer a COBIT, amely bizonyos értelemben egyesíti a többi előírást, és a gyakorlatban is használható útmutatást biztosít az ellenőrzési tevékenységhez. Ez a módszertan valójában felette áll az összes többi eljárásnak, hiszen gyakorlatilag minden szóba jöhető területre kiterjed, és megalkotása során folyamatosan figyelemmel kísérik az egyéb ajánlásokat is. A COBIT azonban önmagában nem teszi lehetővé a kockázatok számszerűsítését. A kockázatok megfogalmazása, és különösen azok számszerűsítése túlmutat a kvázi-szabvány keretein. A kutatás célja egy olyan metrika létrehozása, amellyel az információtechnológiai auditálás során feltárt

kockázatokat számszerűsíteni lehet, és amelynek segítségével összehasonlítható eredmények nyerhetők.

A kockázatértékelésnek azonban nem csak utólagos szerepe van az auditálások értékelő megállapításainak meghozatalakor. Az auditálás tényleges folyamatát megelőzően el kell dönteni, hogy pontosan milyen területekre terjedjen ki az ellenőrzés. Ennek megítélésekor is hasznos valamilyen kockázatszint-elemzés, amely megállapítja, hogy mely területeket, mely alrendszereket érdemes vizsgálni, melyek a leginkább kritikusak az üzletvitel szempontjából. Bár ezekben az esetekben a számszerűsítés az információk hiánya miatt általában nem lehetséges, a kockázati tényezők számbavétele fontos kiinduló lépés.

I.3. A kutatás jelentősége

Az informatikai kockázatok értékelésére számtalan eljárás létezik, és ezek jelentős hányadát különböző szoftvertermékek formájában is el lehet érni. Mivel az informatika a ma működő vállalatok túlnyomó többségét teljesen átszövi, természetes, hogy nagy az érdeklődés a kockázatok értékelése iránt. A számítógépes információrendszerek ugyanis nem csak új lehetőségeket, hanem számtalan új fenyegetést is jelentenek a vállalatok számára (Hale – Landry – Wood, 2004).

Az értékelési eljárások szinte mindegyike a kockázatok bekövetkezési valószínűsége, és a kifejtett hatás/ bekövetkező kár/ pénzbeli veszteség szorzataként kezeli a kockázatokat (Covert – Nielsen, 2005). Az eddigi kutatások többnyire ezen értékelések finomítását, például a pénzben kifejezett értékek pontosabb meghatározását vagy az egyes tényezők súlyozásának javítását (Liu et al., 2005) tűzték ki célul.

Az itt bemutatott kutatás nagyban támaszkodik az eddigi kutatási eredményekre, elsősorban a COBIR kutatási projektre, amely egy auditálási szoftver segédeszköz megalkotását tűzte ki célul. Ugyanakkor a kitűzött célok elérése érdekében újfajta megközelítést alkalmaz: Elsősorban nem a korábbi kutatások során többé-kevésbé feltárt egyes kockázati értékek pontosítását

célozza, hanem a különböző kockázati tényezők együttes fennállásának hatásait vizsgálja. Az volt a cél, hogy számba lehessen venni azokat az előnyöket, amelyeket egy ilyen – a kölcsönhatásokat is figyelembe vevő – értékelési eljárás nyújthat.

A kutatás során elkészült egy olyan értékelési módszer, amely alkalmas ezeknek a kölcsönhatásoknak a figyelembevételére. Sikerült megalkotni egy kockázati mutatószámot, amely képes a vizsgált területek kockázatainak összesítésére az egyes tényezők kölcsönhatásainak figyelembevételével. Ezen túlmenően a megalkotott eljárás gyakorlati alkalmazhatóságát is sikerült felbecsülni.

A kockázati tényezők azonosításánál és mértékük megállapításánál elsősorban a széles körben elterjedt COBIT módszertan, illetve az ezzel teljes összhangban álló képesség-érettségi modellek jelentették az alapot. Az értékelési eljárás kidolgozását pedig a többtényezős döntési modellek felhasználásával sikerült megvalósítani.

A kutatás eredményeként bizonyítást nyert, hogy a tényezők közötti összefüggéseket is figyelembevevő megközelítésnek van létjogosultsága. Az együttes hatások felhasználásával megalkotott mutató segítségével olyan területekre is rá lehet irányítani a figyelmet, amelyek a hagyományos értékelésekben rejtve maradnak. Ezen túlmenően világossá vált, hogy ha már a tervezés során figyelembe vesszük azt a tényt, hogy az informatikai ellenőrzés valójában egy, a gyakorlati tapasztalatok hatására folyamatosan fejlődő terület, akkor az egyes kockázati tényezők együttes hatásaival kiegészített kockázati mutató arra is felhasználható, hogy a vizsgálandó területeket jobban behatároljuk, és az auditálási tervek pontosabbá váljanak.

Remélhető, hogy a dolgozatban bemutatott kutatási irány és az elért eredmények hosszabb távon a gyakorlati életben is hasznosak lehetnek. Mivel az eljárás lehetővé teszi az informatikai kockázatok objektívabb értékelését, fontos eszköz lehet a vállalati informatikával kapcsolatos döntések előkészítésében és a vizsgált területen az erőforrások allokációjában. Továbbá

felhasználható az adott iparágon belüli összehasonlítások alapjául is, és segítségével a menedzsment reálisabb képet alkothat a vállalat informatikai kockázati szintjéről. Bár felmerülhet, hogy a kutatás eredményei jelenlegi állapotukban közvetlenül csak korlátozottan használhatók fel, ugyanakkor előreláthatólag a kutatás folytatásával és a módszer finomhangolásával már a gazdasági élet szereplői által is értékelhető eredményre lehet jutni.

II. FEJEZET
A kutatás célja, hipotézisek

II.1. A kutatás célja

A tervezett kutatás célja kettős: egyrészt gyakorlati jellegű módszerekkel megalkotni azt a kockázatértékelési metrikát, amelynek segítségével az információtechnológiai auditálás során felmerülő, a kockázatok elemzésére vonatkozó feladatok megoldhatók; másrészt az így előállított metrika gyakorlati használhatóságának, és az IT auditra gyakorolt pozitív hatásának igazolása.

A feladat egy, az eddigieknél pontosabb, megbízhatóbb és elfogulatlanabb kockázatértékelési metrika megalkotása. Egy ilyen metrika használatával a vállalati információrendszerek kockázatai jobban becsülhetők. A megfelelő értékelések alapján a vállalatok informatikai erőforrásaira vonatkozó döntések megalapozottabbak lehetnek, és az erőforrásokkal való gazdálkodás hatékonysága növekedhet.

II.1.1. Kockázatértékelési módszer létrehozása

Az IT auditálások során a felmérések kiterjedhetnek a vállalat valamennyi területére, amely a számítógépes információrendszerekkel kapcsolatba hozható. Az, hogy az aktuális auditálás során mely területek ellenőrzése, és milyen mélységig történik meg, a módszertől és az elvárásoktól függ. Ennek megállapítása igen fontos a vizsgálat hasznossága szempontjából, és a vizsgálat folyamatának lehetőség szerint be kell épülnie a vállalat stratégiájába a hatékonyság érdekében (Coles – Moulton, 2003; Olson, 2005, Parker, 2001). Az auditálás során számos kérdést megvizsgálnak, és a megállapításokat egy audit beszámolóban rögzítik. Ez alapján eldönthető, hogy a vállalati működés mely területeit találták problémásnak, és az auditornak lehetőség szerint ki kell térnie a megoldási lehetőségekre.

Az auditálás során azonban a legtöbb esetben nem történik meg a felmerülő kockázatok számszerűsítése. Az auditor – legyen akár külső, akár belső – a legritkább esetben készít akciótervet az auditálás során felmerült hiányosságok kiküszöbölésére. Ez a feladat általában az auditálás megrendelőjére, az informatikai beruházásokért felelős döntéshozóra, vállalati tisztségviselőre hárul.

Ma már mindenki számára világos, hogy tökéletes informatikai biztonság nem létezik. Ennek elérése azonban nem csak a mindig megjelenő új fenyegetések és a kiszámíthatatlanság miatt nem valósítható meg. A vállalatok erőforrásai – elsősorban anyagi lehetőségei – korlátozottak. Amikor egy informatikai vezető döntést hoz a támogatandó, megerősítendő területekről, akkor mérlegeli a kockázatokat, és az ezek kiküszöböléséhez szükséges lépések erőforrásigényét. A cél az, hogy a lehető legkevesebb ráfordítással a lehető legnagyobb előrelépést lehessen elérni a biztonság területén. Ehhez pedig szükség van a pontos adatokra mind a kockázatok mértékét, mind az anyagi vonzatukat illetően.

A kockázatok kezelésének költségei általában a közgazdaságtan hagyományos eszközeivel kiszámíthatók. A kockázatok pontos értékelésére, az egyes területekre vonatkozó kockázati mértékek meghatározására azonban nincs széleskörűen elterjedt megoldás. A kutatás gyakorlati része egy ilyen módszer előállítása, amellyel az auditálás során feltárt kockázatok számszerűen értékelhetők, és egy-egy érintett terület, illetve az auditálási módszertan egy-egy alapelvének érintettsége tekintetében összesíthetők.

Az eddigiekben említett kockázatok ebben az esetben nem csak a szigorúan vett információbiztonsági kockázatokat jelentik, hanem az auditálás során felmerülő szervezési, IT-menedzsment, illetve az esetleges szoftverfejlesztési minőségbiztosítással kapcsolatos problémákat is.

II.1.2. Kockázatértékelés alkalmazása

Az audit beszámolók célja az, hogy a vállalat felelős vezetőit tájékoztassa a felmért helyzetről, az esetleges hiányosságokat megismertesse

velük, és lehetőleg megoldási lehetőségeket is kínáljon. A döntéseket azonban természetesen a vezetőknek kell meghozniuk.

Komoly problémát jelent napjainkban, hogy a vezetők gyakran nem kapnak elegendő információt az IT-t érintő döntések meghozatalához. Az audit beszámolókból kiolvasható ugyan a kockázatos területek leírása, az itt tapasztalt kockázati tényezők és sok esetben a megoldás is. Nem nyújtanak segítséget azonban abban a fontos kérdésben, hogy a vállalat korlátozott erőforrásait mely területek kezelésére érdemes elsősorban fordítani. A döntéshozók sok esetben *ad hoc* módon döntik el, hogy az erőforrásokat milyen módon allokálják a különböző problémák megoldására. Ebben elsősorban tapasztalataikra, esetleg megérzéseikre, gyakran pedig csupán a véletlenre támaszkodnak.

Egy másik probléma, bár az oka eredendően azonos, hogy a különböző auditálási eljárások által megállapított eredmények, elsősorban a kockázati szintekre vonatkozóan, valójában nem összehasonlíthatóak egymással. Mivel nincs általánosan elfogadott szabály a kockázatok értékelésére, ez általában rendkívül szubjektív módon történik meg (Ozier, 2003b). Így, még ha vannak is számszerű mutatók egy-egy területtel kapcsolatban, az a gyakorlatban más esetekkel nem összevethető, hiszen egy másik auditor, másik kockázatértékelő egészen más számadatokat kap esetleg olyankor is, ha ugyanazt a problémát ugyanazzal a módszerrel vizsgálja. Az ugyanannál a szervezetnél különböző időpontokban, illetve egy-egy iparágon belül különböző vállalatoknál történő auditálások eredménye – a kockázatok mértékére vonatkozóan – nem mérhető össze.

A kutatási feltevés szerint egy olyan metrika létrehozása, amely egy széles körben elterjedt módszertanra alapozva képes a különböző kockázatok pontosabb mérését és összehasonlíthatóságát biztosítani, egyaránt elősegíti a vállalati erőforrás-allokáció optimalizálását az érintett területen, valamint ennek és a *benchmarking* képességek növekedésének köszönhetően a vállalatnál meghozott – az auditálás eredményeire támaszkodó – döntések eredményességét, számszerűsíthetőségét és ellenőrizhetőségét.

Az információtechnológiai auditálásnak, a többi ellenőrzéshez hasonlóan az az alapvető célja, hogy a megfelelőséget vizsgálja. Tehát azt, hogy a vizsgált terület folyamatai, szabályozása és működése megfelelnek-e valamely előre rögzített szabályoknak. Ezért az auditálás eredménye alapvetően kétféle lehet: megfelel, vagy nem felel meg.

A vállalati működés szabályozása azt a célt szolgálja, hogy a különböző operatív kockázatokat mérsékelni lehessen a stratégiai célok elérése érdekében. Természetesen ahhoz, hogy a megfelelőséget kellőképpen mérni lehessen, szükség van arra, hogy a kontrollokat (a COBIT esetében a kontroll célkitűzésekből levezetve) a vállalati eljárásokba beépítsék. Felmerül azonban a kérdés, és ez jelen kutatásnak központi témája, hogy a kontrollok (kontroll célkitűzések; MTA-ITA, 2000) megfelelő kiválasztása mennyiben járul hozzá a kockázatok mérsékléséhez. Vajon, ha megfelelő módon szűkítjük a vizsgálandó területet, illetve azokat a kérdéseket, amelyekre koncentrálni kell, akkor ezzel a vállalat informatikából eredő kockázatai csökkenthetők költséghatékony módon? Amennyiben a korábbi auditálások során szerzett ismereteket felhasználjuk az értékelési rendszer önreflexiójára, akkor az segíti-e a helyes kontroll célkitűzések kiválasztását?

II.2. A kutatás során vizsgált kérdések

Az eddigiekben ismertetett célok elérését több feltevésben lehet megfogalmazni. Egyrészt meg kell vizsgálni, hogy létrehozható-e olyan metrika, amely az információtechnológiai auditálás eredményeire támaszkodva, a kockázatok értékelésére használható. Ez alatt azt kell érteni, hogy létezhet olyan mérési, osztályozási eljárás, amelynek segítségével az auditálás során feltárt kockázatok számszerűsíthetők, és az egyes tényezők közötti összefüggések, kölcsönhatások ábrázolhatók. A számszerű értékek az egyes kockázati területek jellemzésére használhatók.

Meg kell vizsgálni, hogy a kockázatértékelési metrika kalibrálható-e oly módon, hogy az értékelési eljárás összehasonlítható eredményeket adjon. Az előállított mérési rendszer mérési szintjeinek oly módon kell

meghatározhatónak lenniük, hogy azok a különböző időpontokban, és különböző szervezeteknél végzett vizsgálatok esetében biztosítsák a megismételhetőséget, és a kockázati mérőszámok a különböző mérések között összehasonlíthatók legyenek. Azaz olyan objektív értékelést eredményezzenek, amely a vállalatok széles körében alkalmazható, és lehetővé teszi az egyes mérések egymáshoz való viszonyítását.

Egy további feltételezés szerint a kockázatértékelési metrika használatával az audit tevékenység objektivitása növelhető. A fent említett módon megalkotott metrika felhasználása segít abban, hogy az auditálások során végrehajtott kockázatértékelések eredménye az auditorok személyétől és személyes véleményétől kisebb mértékben függjenek. Amennyiben a kockázatok egyértelműen számszerűsíthetők, akkor az auditálás folyamata és eredménye is jóval objektívebbnek tekinthető.

Ráadásként feltételezhető, hogy a kockázatértékelési metrika alkalmazásával az auditálás eredményei alapján meghozott menedzsment-döntések jobban számszerűsíthetők, és így könnyebben ellenőrizhetők. Amennyiben a kockázatértékelési metrika működőképes, és azt felhasználják az auditálás során, úgy a kockázatok kiküszöbölésére hozott intézkedések jobban ellenőrizhetők, hiszen a visszacsatolás az egyes döntésekkel kapcsolatban jobban számszerűsíthető és objektívebbé tehető. Ilyen módon a meghozott döntések pontosabb számonkérése válik lehetővé.

Feltételezhető, hogy a kockázatértékelési metrika alkalmazása az információtechnológiai auditálás során elősegíti a vállalatok erőforrás-allokációjának optimalizálását. Az információtechnológiai irányításért felelős vállalati vezetők, menedzserek nehéz helyzetben vannak, amikor a kockázatok kiküszöbölésével kapcsolatban kell dönteniük (Trites, 2004). Megfelelő mérési módszer nélkül az erőforrások kívánatos felhasználása nehezen határozható meg pontosan. A metrika megteremti a lehetőséget, hogy az erőforrások felhasználásával kapcsolatban optimális döntések szülessenek.

A fentiekre támaszkodva a kutatás célja az alább következő hipotézisekben fogalmazható meg. A vizsgálat eredményeként lehetővé válik a hipotézisek elfogadása vagy elvetése, és ezen keresztül a kockázatértékelési metrika alkalmazhatóságának elemzése.

Hipotézis 1.: Létezik a vállalatok informatikai működésére vonatkozó olyan összesített kockázati mutatószám, amely az egyes kockázati területek közötti interakciókat is figyelembe veszi, és hitelesen orientál.

Az eddigi kutatások kevéssé célozták meg azt a kérdést, hogy az egyes kockázati tényezők milyen módon hatnak egymásra. Bár a kölcsönhatások fennállása nyilvánvaló, ezek általában csak másodlagosan jelennek meg az értékelési eljárásokban. A kutatás során felhasználjuk azt a feltételezést, hogy kialakítható olyan értékelési eljárás, amely ezeket az összefüggéseket nem csak rejtetten tartalmazza, hanem ténylegesen felhasználja a vállalati kockázat értékelésében.

Ezen túlmenően az indexnek a gyakorlatban is használhatónak kell lennie, és biztosítania kell, hogy az ennek használatával kapott eredmények reális képet adjanak az informatikai kockázatokról.

Hipotézis 2.: Ha az informatikai auditálás végrehajtásának önreflexív jellegét explicit módon megfogalmazzuk, akkor az ebből származó eredményeket vissza lehet vezetni az audit terv javítására, pontosítására.

Az informatikai ellenőrzés alapvetően a korábbi tapasztalatokon alapszik. A legtöbb módszertan valójában a „legjobb gyakorlatok" gyűjteménye[1], tehát az egyes esetekben felmért területeken végrehajtott auditálások során felhalmozott tudást tartalmazzák. Ezt érdemes akkor is figyelembe venni, amikor a módszertant alkalmazzuk.

A különböző auditálások adatait érdemes tehát felhasználni arra a célra, hogy az értékelési eljárást pontosítsuk. A 2. hipotézis szerint az auditálási terv

[1] Ez igaz nem csak a kutatás alapjaként felhasznált COBIT módszertanra, hanem többek között pl. az Egyesült Államok Központi Számviteli Irodájának ajánlásaira is (GAO, 1999).

pontosítását végre lehet hajtani, amennyiben a korábbi auditálások eredményeit megfelelő módon felhasználjuk.

Hipotézis 3.: A kockázati tényezők együttes hatásainak figyelembevételével lehetővé válik olyan, az informatika funkcióival összefüggő stratégiai fontosságú területek azonosítása is, amelyek a hagyományos módszerekkel nem határozhatók meg.

A jelenleg alkalmazott kockázatértékelési módszertanok nem, vagy csak implicit módon veszik figyelembe a kockázati tényezők közötti kölcsönhatásokat. A kutatás során használt feltételezés szerint azonban, a megfelelő módon kialakított és a kockázatok együttes hatását is feldolgozó mutató esetében olyan kockázati területek is felismerhetők, amelyek más módon nem azonosíthatók.

Amíg ugyanis egy-egy terület lehet aránylag alacsony kockázatú, ugyanezt nagyon kockázatosnak értékelhetjük más kockázati tényezők együttes fennállása esetén.

Az első hipotézis igazolása közvetlen módon, a megfelelő metrika előállításával végezhető el. A második és harmadik hipotézis elfogadhatóságáról a szimulációs kísérlet során összegyűjtött adatok elemzése után dönthetünk.

III. FEJEZET
Az auditálás fogalma

III.1. Az auditálás általában

Az auditálás és az ehhez kapcsolódó fogalmak, a dolgozat céljának megvalósítása érdekében, tisztázásra szorulnak. A különböző meghatározások gyakran pontatlanok, és nem fedik le teljesen a kérdéses témakört. Ez részben az angol nyelvű szakirodalom meghatározásainak átvételéből adódik (Nyikos-Kresalek, 2003). Így gyakran összekeveredik az auditálás, ellenőrzés, könyvvizsgálat, belső ellenőrzés fogalma. Tovább bonyolítja az értelmezést, hogy az információrendszerek auditálásában is megkülönböztethetők olyan területek, amelyek elnevezésüket tekintve átfedésben vannak az ellenőrzés más területeivel. Ráadásul gyakran nagyon általánosan használják az informatikai rendszerek biztonsági ellenőrzésére vonatkozó elnevezéseket. Ezért feltétlenül szükséges a kérdéses fogalmak pontos definiálása ahhoz, hogy a kutatást ne nehezítsék átfedések és pontatlanságok.

Az auditálás igen nagy múltra tekint vissza. A III.6. alfejezetben található történelmi áttekintésből kitűnik, hogy a fogalom szinte egyidős az emberiséggel, még ha az elnevezés természetesen nem is létezett. A mai modern auditálási gyakorlat egyik első példájaként említhető a német Krupp vállalat, ahol már a 19. század második felében létezett auditálási kézikönyv. Ebben meghatározzák az auditorok felelősségét: „*Az auditorok feladata annak eldöntése, hogy a törvényeket, szerződéseket, előírásokat és eljárásokat megfelelő módon figyelembe veszik-e, illetve, hogy minden üzleti tranzakciót a rögzített előírásoknak megfelelően és sikeresen hajtanak-e végre. Ezzel kapcsolatban az auditoroknak javaslatokat kell tenniük a meglévő létesítmények és folyamatok javítására, építő kritikát kell megfogalmazniuk a szerződésekkel kapcsolatban stb.*” (Cangemi-Singleton, 2003, p. 10.). Bár ez a megfogalmazás inkább az auditálást végzők munkájának leírásán keresztül közelíti meg a kérdést, ebből is kitűnik az auditálás mai feladata: a vállalat

működésének valamilyen előre rögzített szabályokkal való összevetése és értékelése.

Az auditálás már a magyar hivatalos köznyelvben is elterjedt kifejezés, jelentése a Magyar értelmező kéziszótár szerint: „*A vállalkozók éves beszámolójának, ill. vagyoni, pénzügyi helyzetének felülvizsgálata és hitelesítése.*" illetve: „*Valamely vállalat, vállalkozás működésének, számviteli, ügyviteli, információs stb. szakszerűségének vizsgálata, ellenőrzése.*" (MÉK, 2003, p. 74.). Ebből a meghatározásból is kiderül, hogy az auditálás a közfelfogás szerint elsősorban a pénzügyi-számviteli ellenőrzést jelenti, és a vállalatok gazdasági működésére helyezi a hangsúlyt. Ugyanakkor a definícióban már megjelenik a szakszerűség vizsgálata, és ilyen környezetben az információs rendszerek ellenőrzése is említésre kerül.

Maga a kifejezés a latin *audire* (hallani, hallgatni) igéből származik, és eredetileg meghallgatást jelentett. Ennek során a tulajdonos a vagyon kezelésével megbízott személy beszámolóját hallgatta meg a kezeléssel kapcsolatos kérdésekkel kapcsolatban.

Az angol *audit* kifejezés meghatározása a Longman szótár szerint: „*Egy vállalat pénzügyi nyilvántartásának vizsgálata a helyesség ellenőrzése céljából.*" (Longman, 1995, p. 72.)

Ezekből a definíciókból világosan kitűnik, hogy az audit és auditálás fogalma elsősorban továbbra is a számviteli ellenőrzésre vonatkozik. Ez természetes is, hiszen a számviteli ellenőrzés, auditálás igen hosszú múltra, komoly történelmi előzményekre tekinthet vissza. Az informatika térhódításával azonban a számvitel és a vállalatok gazdálkodása egyre inkább elválaszthatatlan az információrendszerektől. Mivel a könyvelési adatok nagyrészt számítógépes információrendszerekben találhatók, a számviteli ellenőrzés sem térhet ki ezen rendszerek auditálása elől. Az informatikai auditálás valójában a számviteli ellenőrzés kiterjesztéseként értelmezhető (Gallegos – Allen-Senft – Manson, 1999), és elterjedésében szerepe van annak

is, hogy a vállalatvezetők felismerték, hogy a pontos ellenőrzéshez a fent említett terület auditálása is szükséges (Kő, 2003).

Az Amerikai Számviteli Társaság[2]definíciója szerint az auditálás olyan rendszeresen ismétlődő folyamat, amely tárgyszerű bizonyítékok szerzésére és azok objektív értékelésére irányul. Ezeknek köszönhetően megfelelő bizonyítékokhoz lehet jutni annak megállapításához, hogy az ellenőrzött szervezet gazdasági eseményeiről szóló állítások milyen mértékben felelnek meg az előre rögzített szabályoknak. Az összehasonlítás eredményét pedig vélemény formájában közlik az érdekeltekkel. Ez az audit beszámoló (Robertson – Davis, 1998).

A meghatározás alapján is állíthatjuk, hogy az auditálás egy folyamatos vagy periodikusan ismétlődő folyamat (Dull – Tegarden, 2004), amely során valamilyen előírásoknak való megfelelést vizsgálnak. Mivel itt egy számviteli szervezet definíciója szerepel, szinte szükségszerű, hogy a hangsúly a gazdasági események értékelésén van, ugyanakkor a korábban említettek az auditálás teljességéről továbbra is helytállónak tekinthetők.

A legtöbb forrás nem említi, hogy az auditálás a vállalati működés egyéb területeit is érintheti, így – a későbbiekben kifejtett IT auditon túl – létezik például környezetvédelmi és minőségbiztosítási auditálás is. A fogalom használata általában olyan területeken fordul elő, ahol a vállalatnak a külső érintettek felé bizonyítaniuk kell a folyamatok megfelelő működését. Hiszen az auditálás célja nem csupán a vállalati működés hatékonyságának javítása, hanem a meglévő folyamatok megfelelőségének tanúsítása is az üzleti partnerek, vevők, egyéb külső érintettek felé.

III.2. Ellenőrzés

A magyar szóhasználatban az *auditálással* gyakran szinonim fogalomként említik az *ellenőrzést*. Az ellenőrzés valakinek vagy valamely tevékenységnek, munkának vagy állapotnak, helyzetnek az (elbírálás végett)

[2] *American Accounting Association*

történő megvizsgálását vagy figyelemmel kísérése, illetve adatok vagy méretek helyességük szempontjából történő felülvizsgálata (MÉK, 2003, p. 279.).

Az ellenőrzés tehát egy átfogó fogalom, és gyakran adódik félreértés abból, hogy *audit* alatt a könyvvizsgálatot értik, amely viszont csak egy részét jelenti a teljes ellenőrzésnek. Érdemes megemlíteni továbbá, hogy az ellenőrzés nem feltétlenül csak egyszeri tevékenységet jelent, hiszen a „figyelemmel kísérés" folyamatos, illetve ismétlődő ellenőrzéseket takar. Ennek a pénzügyi és az információtechnológiai ellenőrzések esetében is nagy jelentősége van. Az auditálás és az információrendszerek ellenőrzése ugyanis csak akkor lehet hatékony, ha az folyamatosan történik. Ehhez a kontrollok be kell hogy épüljenek a vállalati folyamatokba, és az egész szervezeti működésnek az auditálhatóság szempontját figyelembe véve kell kiépülnie. Ez pedig nem más, mint az utóbbi években széleskörűen elterjedő IT irányítás[3].

III.3. Pénzügyi ellenőrzés

Bár Magyarországon nincs hivatalos meghatározása a fogalomnak, gyakran használják a *pénzügyi ellenőrzés* kifejezést is. Ez az angol *financial audit* fordításaként került be a szakszavak közé (Nyikos, 2000). A gyakorlatban sokszor ez az a terület, amelyet a gazdasági élet szereplői audit alatt értenek. Magyarországon ugyanis elsősorban a számviteli vagy pénzügyi ellenőrzés az, amelyre széleskörűen elterjedt az audit kifejezés. Maga az audit azonban jóval szélesebb területet fed le, nem feltétlenül csak a gazdálkodáshoz közvetlenül kapcsolódó ellenőrzések képezik a részét. A jelen kutatásban is egy olyan terület auditálásáról esik szó, amely csak részben kapcsolódik a pénzügy és számvitel fogalomköréhez. Bár ezek a kapcsolódások rendkívül fontosak, az információtechnológiai auditálásnak ezeken túlmenően részét képezik a rendszerek fejlesztésével, üzemeltetésével kapcsolatos elemzések is.

[3] Magyarul leggyakrabban így fordítják az *IT governance* fogalmát.

III.4. Audit és könyvvizsgálat

A könyvvizsgálat és az auditálás a magyar szóhasználatban gyakran azonos tartalommal bírnak, ugyanakkor más felfogások szerint az auditálás a könyvvizsgálatnál tágabb fogalomkört jelöl. Ebbe beletartozik a számviteli bizonylatok és eljárások vizsgálatán túl a vállalat szervezeti-hatékonysági kérdéseinek elemzése is, illetve általános értelemben a teljes vállalati működés felügyelete. Ilyen felfogás szerint a hatékonyság és a vállalati működés értékelése során természetesen érinteni kell az információrendszerek hatékonyságát is.

Az 1991-ben, majd 2000-ben megalkotott Számviteli Törvény szerint a könyvvizsgálat célja annak megállapítása, hogy a vállalkozás által készített éves beszámoló „megbízható és valós" képet ad-e a vállalkozó vagyoni és pénzügyi helyzetéről. Ez tehát egy viszonylag szűkebb területet jelent, hiszen az éves beszámolóhoz kapcsolódó ellenőrzésről van szó. Ugyanakkor annak vizsgálata, hogy az éves beszámoló megfelelő módon tükrözi-e a valós tényeket, természetszerűleg mélyebb ellenőrzést tesz szükségessé, amely túlmegy az egyszerű dokumentumelemzésen.

Tovább bonyolítja a helyzetet, hogy a magyar nemzeti könnyvizsgálati standardok glosszáriumában könyvvizsgálatnak fordították a nemzetközileg elterjedt *audit* kifejezést (Nyikos – Kresalek, 2003).

Az eddigiekből is világosan látszik, hogy az elnevezések nem teljesen kiforrottak, és használatuk nem mindig következetes. Ez többek között arra is visszavezethető, hogy a vizsgált területen – és az információtechnológiai szférában különösen – a legtöbb szakkifejezés angolszász eredetű, amelyek magyar fordítása gyakran nem is létezik; máskor pedig egy-egy fogalom magyarítására a különböző szerzők más-más megfelelőt találnak. Ennek eredményeként előfordul, hogy ugyanaz a kifejezés más szerzőknél más fogalmat takar.

III.4.1. Belső ellenőrzés

Az auditálást végző személy lehet a vállalat belső alkalmazottja, vagy pedig valamilyen külső, megbízott személy. Ez alapján teszünk különbséget belső és külső ellenőrzés, illetve auditálás között. Természetesen a vállalat alkalmazottja nem lehet teljesen független a cégtől, így a teljes tárgyilagosság sem minden esetben feltételezhető róla. A belső auditálást könyvelők, illetve belső ellenőrök végzik. Feladatuk a három alapelv tiszteletben tartásának vizsgálata; azaz, hogy a vállalat működése során a teljesség, a megbízhatóság és a pontosság szempontjait figyelembe véve járnak-e el. Amennyiben eltérést észlelnek, azt fel kell jegyezniük

III.4.2. Külső ellenőrzés

A vállalattól független értékelés természetesen csak a külső ellenőrzésektől várható el. A külső ellenőrzést ennek megfelelően gyakran nevezik független auditálásnak is. A külső ellenőrök olyan személyek, akik a vállalattól függetlenül működnek, általában megbízás alapján dolgoznak. A külső pénzügyi ellenőrzés során megvizsgálják, hogy a vállalat beszámolóiban szereplő adatok megfelelnek-e a valóságnak, és kellő módon tükrözik-e a vállalat gazdálkodási folyamatait.

Noha a külső ellenőröknek definíciószerűen függetleneknek kell lenniük a vizsgált vállalattól, a külső ellenőrzések megbízhatóságával kapcsolatban számos kérdés merült fel az elmúlt évek könyvelési botrányai kapcsán. Ennek eredményeként a törvényi szabályozások is megváltoztak a független ellenőrzésekkel és külső auditálásokkal kapcsolatban. A kérdésről később részletesebben is esik szó.

III.5. IT audit

Az eddigiek elsősorban a számviteli típusú auditáláshoz kapcsolódó definíciók. Az auditálás azonban nem csupán a számviteli dokumentumok és eljárások elemzését jelenti. Mint azt már korábban láthattuk, az auditálás ennél bővebb fogalmat takar, és gyakorlatilag a vállalat egész működésének

figyelemmel kísérését magában foglalja. Ez alól nem lehet kivétel a számítógépes információrendszerek működése sem. Így tehát egy átfogó ellenőrzésnek természetszerűleg részét kell hogy képezze az információtechnológiai infrastruktúra és a számítógépes rendszerek megbízhatóságának, biztonságának és egyéb jellemzőinek vizsgálata (Vendrzyk – Bagranoff, 2003). A vállalati folyamatok ellenőrzésébe pedig beletartozik a számítógépes információrendszerek beszerzésének, előállításának, az ezekben rejlő lehetőségek értékelésének végrehajtása is (Weber, 1999).

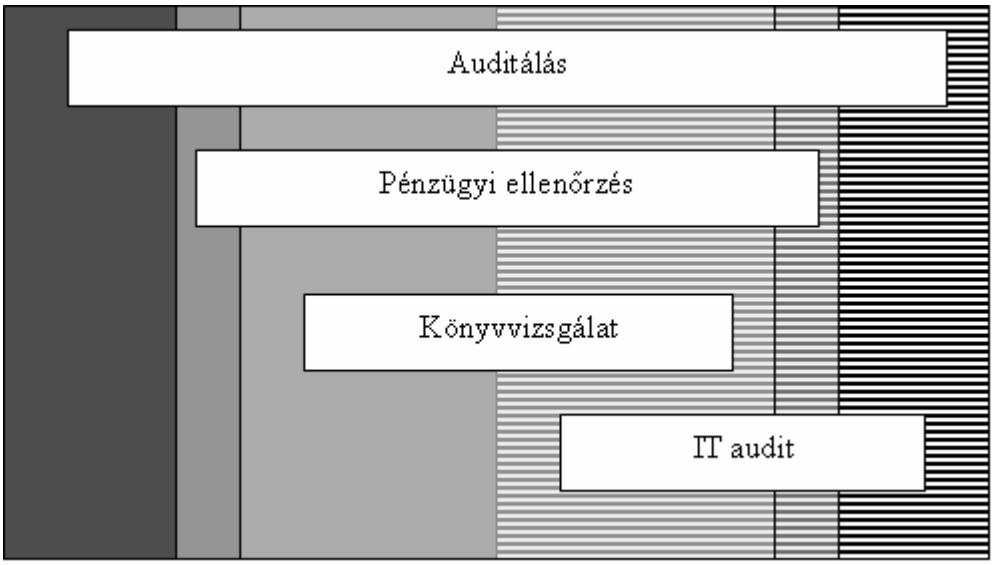
Az információtechnológiai (IT) audit, vagy más szóhasználattal az információrendszerek[4] auditálása tehát több ponton is kapcsolódik az eddigiekben vázolt auditálási fogalmakhoz. Egyrészt egy, a vállalat teljes működésére kiterjedő vizsgálat során az informatikához kapcsolódó területek beszerzései, folyamatai és működése is előtérbe kerül. Másrészt pedig a hagyományosabb értelemben vett pénzügyi ellenőrzés esetén sem lehet elkerülni, hogy az informatikai rendszerekre is kiterjedő vizsgálatot hajtsanak végre. A 21. század elején ugyanis szinte nem létezik komolyabb vállalat, amely könyvelését, számviteli bizonylatait, és szinte teljes működését ne számítógépes alkalmazások segítségével támogatná. Az informatika fejlődése és a vállalati struktúrák átalakulása korábban nem is létező ellenőrzési területeket is előtérbe hozott (Leem – Lee, 2004 és Murthy – Groomer, 2004). A vállalati működés szerves részét képezik az információtechnológiai megoldások, és így nem csak az átfogó ellenőrzéseknek, de szinte a vállalat bármely területét érintő auditálásnak ki kell terjednie az információrendszerek ellenőrzésére is. (Champlain, 2002).

Ezek alapján igazolva láthatjuk, amit ismét meg kell jegyezni, hogy az IT audit valóban a hagyományos auditálás – ebben az értelemben inkább könyvvizsgálat vagy pénzügyi ellenőrzés – kiterjesztéseként értelmezhető (Gallegos – Allen-Senft – Manson, 1999). Másrészt az információrendszerek működése felvet olyan auditálási kérdéseket is, amelyek az

[4] *Information Systems – IS*

információtechnológia létéből adódnak, így az IT auditnak vannak olyan területei is, amelyek nem a könyvvizsgálathoz, hanem a rendszerek meglétéhez vagy fejlesztéséhez kapcsolhatók. Ezt a viszonyt tekinthetjük át a következő ábrán. Fontos megjegyezni azonban, hogy az alábbi felosztás erősen szubjektív, és pusztán a kutatás során alkalmazott fogalmi keretet illusztrálására szolgál. Egyértelmű kategorizálásra ugyanis a fentiek miatt nincs lehetőség.

1. ábra



Az auditálás fő területeinek viszonya

Egy magyar szerzőtől származó definíció szerint: „*Az információrendszerek auditálása azt jelenti, hogy valamely IT terméket, illetve rendszert módszeres vizsgálatnak vetnek alá, amelynek során egy vizsgálati eljárás alkalmazásával megállapítják biztonsági tulajdonságait. Az auditálás tehát az informatikai biztonság szempontjából végzett értékelés.*” (Kő, 2003, p. 4. hivatkozza: Ködmön, 1999) Ez a megfogalmazás azonban szűken értelmezi az információrendszerek ellenőrzését, hiszen nem szerepel benne a menedzsmentre, a szoftverfejlesztésre stb. vonatkozó auditálás. Egy átfogóbb értelmezés szerint: „*Az információrendszerek auditálása gyűjtőfogalom, amely magában foglalja többek között a technikai szempontú ellenőrzést (infrastruktúra, kommunikáció), a menedzsment információtechnikai*

ellenőrzési eljárásainak auditálását, a szoftverfejlesztés és implementáció, valamint az alkalmazások ellenőrzését, és a nemzetközi és nemzeti szabványoknak való megfelelést." (Kő, 2003, pp. 3-4.). Ez a megfogalmazás közelebb áll a korábban említett általános elmélethez, ugyanakkor önmagában nem határozza meg pontosan, mit értünk IT audit alatt.

Az IT audit célja általánosságban nem különbözik a többi auditálási eljárás céljától: a vállalatnál észlelt bizonyos tényezők összehasonlítását jelenti valamilyen előre rögzített standarddal. A pontos értelmezéshez természetesen meg kell határozni, hogy milyen tényezőket vizsgálunk: ez ebben az esetben nyilván az információtechnológiához kapcsolódó jelenségeket jelenti, legyen az a vállalati döntéshozók viszonyulása a technológiai fejlesztésekhez, az informatikai fejlesztések során követett módszer, vagy éppen a már működő rendszerek biztonsága. Továbbá szükség van annak tisztázására, hogy mik azok a szabályok, amelynek való megfelelést vizsgálunk. Ez általában valamelyik szabványrendszerre történő hivatkozással oldható meg, erről részletesen a IV. fejezetben lesz szó.

Az információtechnológiai auditálás esetében is megkülönböztetünk belső és külső auditálást. A belső audit célja elsősorban a vállalatban meglévő szabályok alkalmazásának nyomon követése (Hermanson – Hill – Ivancevich, 2000). A külső audit pedig a belső audit független és elfogulatlan ellenőrzését, és a vizsgált rendszer(ek) biztonsági állapotának, jellemzőinek értékelését jelenti.

III.6. Audit történelem

III.6.1. Számvitel, auditálás, belső ellenőrzés

Az emberiség a civilizáció kezdete óta hajt végre gazdasági tranzakciókat, és az ezek rögzítésére irányuló törekvés végigkíséri történelmünket. A számvitel és a számviteli auditálás története bizonyos felfogások szerint egyidős az írással. A kutatók egy része úgy véli, hogy az írásjelek kialakulására részben az ellenőrzési feladatok ellátása miatt volt szükség. Léteznek bizonyítékok arra, hogy már az ókori Egyiptomban, majd Görögországban és a Római Birodalomban is voltak számvitellel foglalkozó szakemberek, és a számviteli ellenőrzés a mindennapi élet részét képezte (Brown, 1962). A mai értelemben vett számvitel a középkorban terjedt el.

A mai auditálási gyakorlatot nagymértékben meghatározó Amerikai Egyesült Államokban is bevett gyakorlattá vált a számviteli ellenőrzés, szinte az első telepesek megjelenésétől kezdődően (Flesher – Previts – Samson, 2005). Az első könyvelő által végrehajtott külső auditálást a 18. században végezték, amikor az egyik hatalmas angliai vállalat váratlanul csődbe jutott, részben a fiktív könyvelések következtében. Az auditálás középpontba kerülése, fejlődése, szabályozása azóta is általában valamilyen visszaélés, pénzügyi számviteli botrány kirobbanását követi.

A számviteli ellenőrzés a 19. században és még a 20. század elején is elsősorban a könyvelés pontos végrehajtásának ellenőrzését jelentette (Cangemi – Singleton, 2003). Az ellenőr feladata az volt, hogy megvizsgálja, az egyes könyvelések a számviteli szabályoknak megfelelően mentek-e végbe. A könyvelésben meg nem jelenő tételek tehát egyszerűen kimaradtak a vizsgálatból. Az ellenőri munka pedig inkább a mechanikus ellenőrzések végrehajtását jelentette, semmint kifinomult és mélyreható vizsgálódást.

A vállalati működés azonban jelentősen megváltozott a 20. század elején, a finanszírozás új formái jelentek meg, amelyek a számvitel és az auditálás változásait is magukkal hozták (Brown, 1962). Az ellenőrzés

hangsúlya egyre inkább eltolódott a mérlegben található eszközök értékelésére, a számtani helyesség ellenőrzése helyett.

A számvitellel és a számviteli ellenőrzéssel kapcsolatos felfogásbeli változások a 20. században is leggyakrabban valamilyen számviteli botránnyal, bizonyos ügyek elkendőzésének kísérletével, vagy valamilyen visszaéléssel kapcsolatosak. Az egyik legutóbbi ilyen esemény az ENRON-botrány volt, amelynek hatása erősen érződik az auditálás megítélésében (Hilary – Lennox, 2005). Az ilyen jelenségek hozzájárulnak a számviteli szabályok és az ellenőrzésre vonatkozó előírások kidolgozásához, folyamatos fejlődést és finomodást eredményezve (Friedland, 2002).

Mindazonáltal, egészen a második világháborúig az auditori és belső ellenőrzési tevékenység egy viszonylag elszigetelt területet jelentett a vállalati működésben. Nem volt önálló osztály vagy más szervezeti egység, amely az ellenőrzésekért felelt volna, hanem egyes személyeket bíztak meg a bizonylatok és a folyamatok kontrollálásával. Az auditor munkája egy nyomozóéhoz volt hasonlatos, aki a meglévő bizonylatok alapján dolgozott. Abban az időben nem voltak elfogadott és széleskörűen elterjedt szabványok az ellenőrzésekre vonatkozóan (Cangemi – Singleton, 2003). A belső ellenőrzés célja az volt, hogy a rendellenességeket még az éves ellenőrzések előtt feltárják és kiszűrjék. Ez a tevékenység csak később vált önálló vállalati funkcióvá. Az elmúlt században a belső ellenőrzés szerepe megváltozott. Ma már nem egyszerűen a visszaélések felderítése a célja, hanem olyan kockázatelemzések készítése, amelyek a vezetői döntéshozatalt támogatják (Dennis, 2004). A feladat bonyolultabb és minőségileg más: a vállalati működés szerves részét képezi.

III.6.2. Az IT audit története

A vállalatok gazdálkodásának tükre a főkönyv, és a kapcsolódó számviteli bizonylatok. Egy cég működésének ellenőrzése, a számviteli szabályok betartásának felügyelete tehát feltételezi ezeknek a gazdasági eseményeket rögzítő dokumentumoknak a vizsgálatát. A számviteli ellenőrzés

egészen az ötvenes évekig azt jelentette, hogy a vállalat működése során előálló rengeteg papíralapú dokumentumot át kellett tekinteni, és ez alapján lehetett a visszásságokat feltárni. Az 1950-es években azonban megjelent egy új eszköz, amely forradalmasította az adattárolást és az adatok kinyerését: az üzleti számítógép.

Ez a forradalom azonban nem egyik napról a másikra ment végbe, a könyvelés és a vállalati dokumentáció számítógépes alapokra helyezése egy hosszabb folyamat volt, amely még napjainkra sem fejeződött be teljesen. Ugyanakkor az új eszköz megjelenése alapvetően megváltoztatta azokat a módszereket, amelyekkel az ellenőrök, auditorok a kívánt adatokhoz hozzáférhettek. A számítógépek korában ugyanis a könyvelési tételek, a vállalat ügyeinek dokumentációja egyre kevésbe a megszokott formátumban – papíron – állt rendelkezésre, hanem a számítógépes vállalati információrendszerek adatbázisaiban lehetett hozzáférni. Ez természetesen magával hozta azt is, hogy az ellenőrzés nem különféle papírok valóságtartalmának megállapítását, és egymással való összehasonlítását jelenti, hanem egy átfogó kutatást, amely kiterjed a számítógépes információrendszerekben, adatbázisokban fellelhető adatok vizsgálatára is. Mivel azonban ezen információrendszerek és adatbázisok eredendően sokkal kevésbé átláthatóak, működésük egy nem kellőképpen felkészült ellenőr számára homályos lehet, ezért érthető, hogy az auditálás magában kell hogy foglalja az információrendszerek működésének, és használatának vizsgálatát is (Vroom – Solms, 2004). Ehhez az auditálásban megszokott és bevett módszerek alapvető átalakítására, és új eljárások kialakítására volt szükség.

A számítógépek megjelenésével az adatokat a már megismerteken kívül újabb veszélyek is fenyegették. Az auditoroknak meg kellett ismerkedniük az új technológiával, és a kockázatok értékelésekor a technológiai kérdéseket is figyelembe kellett venniük (Vendrzyk – Bagranoff, 2003.)

Az üzleti felhasználású számítógépek megjelenését követő első évtizedben a hozzáférési, manipulálási kérdésekkel kapcsolatban elegendő biztosítékot jelentett az is, hogy az adatokat számítógépes rendszerekben

tárolták. Ezek a számítógépek ugyanis nagygépes rendszereket[5] jelentettek. Ezekből viszonylag kevés volt, és programozásukhoz és kezelésükhöz rendkívül kevés ember értett. Egy esetleges visszaélésre viszonylag egyszerűen fényt deríthettek, és az elkövetők száma rendkívül korlátozott lehetett. (Cangemi – Singleton, 2003.)

Ezzel párhuzamosan a számítógépesítésnek egy másik következményével is számolni kellett. Az információrendszerekben található adatok elemzésére a számítógépek és a számítógépes programok lettek a legalkalmasabbak. A programok elkészítéséhez és futtatásához is – abban az időben, tehát az ötvenes évek végén, hatvanas évek elején – komoly szakértelemre volt szükség. Ez pedig jelentős korlátot jelentett az auditálások végrehajtásánál.

A hatvanas évek elején a számítógépes auditálás nagyrészt az adott feladatra készített programok lefuttatását jelentette. Az üzleti informatika terjedésével azonban az elkészítendő programok száma rendkívüli mértékben megnőtt, így hamar felmerült az igény egy általános audit szoftver[6] kifejlesztésére. (Cangemi – Singleton, 2003.) Az első ilyen programot az AUDITAPE megjelenése jelentette 1967-ben. Nem sokkal ezután szinte minden nagy könyvvizsgáló cég elkészítette saját audit szoftverét, amellyel a korábban körülményes IT auditálási feladatokat részben automatizálhatták.

Az *ad hoc* jellegű ellenőrzési módszerek helyett tehát kezdett kialakulni egy módszertan, amelynek segítségével az ellenőrök immár jóval felkészültebben indulhattak neki az elektronikus auditálási feladatoknak. Ezzel párhuzamosan felmerült az igény egy olyan szervezet kialakítására is, amely képes lehet összefogni a területen dolgozó ellenőröket. Ez a szervezet 1969-ben alakult meg, Elektronikus Adatfeldolgozási Ellenőrök Szövetsége[7] néven. A célja többek között, hogy egy egységes módszertan kidolgozásával segítse az auditori munkát, és mintegy kamaraként működve elősegítse az ellenőrök

[5] *Mainframe* számítógépes rendszereket
[6] Ezek elterjedt rövidítése a *GAS (Generalized Audit Software)*
[7] *EDPAA (Electronic Data Processing Auditors Association)*

működésének minőségbiztosítását. 1977-ben jelent meg a szervezethez tartozó alapítvány gondozásában a Kontroll Célkitűzések[8] első kiadása, amely egy normatív modell kialakításával segítette az auditorok munkáját. Ebből a vezérelvek, eljárás és esettanulmány gyűjteményből nőtt ki a COBIT[9].

1978-ban pedig az első hallgatók letehették a CISA[10] vizsgát, ezáltal egy olyan bizonyítvány birtokába jutva, amely az egységesített követelmények elsajátítását és alkalmazási képességét tanúsítja (Macartney, 2004).

A szervezet elnevezése 1994-ben ISACÁ-ra (Information Systems Control and Audit Association) változott, a célkitűzések és a megvalósítás módja azonban csak modernizálódott, alapvetően nem módosult. Jelenleg az ISACÁ-nak közel 30 ezer tagja van, ez a legjelentősebb IT audit szervezet (Lord, 2004), és a COBIT újabb kiadásaival komoly erőfeszítéseket tesz az auditori munka szabványosítására. Részben ezek a tények is magyarázzák, hogy a kutatás során a kockázati módszertan kialakításához is a COBIT lehet a leginkább megfelelő alap.

[8] A COBIT-ban is használt eredeti angol elnevezéssel: *Control Objectives*
[9] A COBIT módszertanról részletesen a következő fejezetben lesz szó.
[10] *Certified Information Systems Auditor*: Széleskörűen elfogadott képesítési tanúsítvány IT auditorok számára.

IV. FEJEZET
Audit szabványok és összefüggéseik

IV.1. A szabványosítás szükségessége

A kockázatértékelés az IT audit esetében azt jelenti, hogy a vállalati számítógépes információrendszerek tervezésével, implementálásával, működtetésével és felügyeletével kapcsolatos veszélyeket – legyenek azok technikai, személyi, szervezési vagy működési jellegűek –, valamilyen szempontrendszer szerint megvizsgáljuk, és megbecsüljük azok mértékét. A megfelelő értékeléshez azonban elengedhetetlen a megfelelő szabályrendszer alkalmazása. A kockázatértékelési rendszer kidolgozásakor ki kell alakítani, vagy át kell venni azt a szempontrendszert, amely alapján a különböző kockázatokat figyelembe vesszük. Ezért szükséges a különböző IT audit szabályok és szabványok áttekintése, és az alkalmazni kívánt rendszer kiválasztásának indoklása. Noha a kutatás alapjaként kezelt COBIT módszertan kialakulásának körülményeit láthattuk a III. fejezetben, érdemes az összefüggéseket is áttekinteni.

Az auditálás folyamata feltételezi, hogy a valós helyzetet valamely előírással, követelménnyel, illetve szabványosított követelményrendszerrel hasonlítsák össze. Az auditálás nem lehet igazán sikeres, amennyiben a szabályokat a folyamat során változtatják, vagy azok eseti módon kerülnek kidolgozásra. Ebben az esetben ugyanis az elfogulatlanság erősen megkérdőjelezhető, és az auditálás megbízhatósága és hatékonysága is jelentős csorbát szenved.

Természetesen nem várható el, hogy egészen eltérő profilú vállalatok esetén, amelyek akár eltérő platformokon működő, különböző számítógépes infrastruktúrával, más operációs és alkalmazási rendszerekkel stb. rendelkeznek, ugyanazokat a kérdéseket tegyék fel az auditálás során; sem pedig az, hogy az auditálás folyamata a különböző helyeken teljes mértékben megegyezzen. Egy jó auditálás minden esetben testre szabott. Ez azonban nem

azt jelenti, hogy az audit programot minden alkalommal teljesen az alapoktól kellene felépíteni. Az audit program – tehát annak eldöntése, hogy milyen területek milyen mértékben legyenek érintve az auditálás során, illetve, hogy az audit milyen kérdésekre terjedjen ki – valójában egy válogatást jelent a már meglévő szabványosított eljárások között. A vizsgált vállalat jellemzői, valamint a vizsgálandó terület alapján a szabályrendszerből ki kell emelni az érintett területekre vonatkozó tudnivalókat, és az adott problémára alkalmazni.

IV.2. Szabványosítási törekvések

A szabványosítási törekvések az információtechnológiai audit elterjedésével párhuzamosan erősödtek. Az üzleti felhasználású számítógépek széleskörű alkalmazásával egyre nyilvánvalóbb igény merült fel az információrendszerek auditálására. Jogos elvárás volt valamilyen egységesített keretrendszer létrehozása, amely alapján a különböző értékelések elvégezhetőek, és a különböző vállalatoknál, vagy ugyanazon vállalatnál különböző időben végrehajtott ellenőrzések eredményei összehasonlíthatók. Ez az elvárás az összehasonlíthatóságra, a mutatók összevetésére[11] fontos tényező a szabványosítás kialakulásában. Ahhoz ugyanis, hogy a különböző értékelések eredményei összehasonlíthatók legyenek, feltétlenül biztosítani kell, hogy a követelményrendszer azonos legyen. Mivel ez a szempont a jelen kutatás szempontjából is nagy jelentőséggel bír, a későbbiekben részletesebben is említésre kerül.

Az információrendszerek auditálásának elterjedése idején a hagyományos auditálás – könyvvizsgálat, pénzügyi ellenőrzés – már rendelkezett jól bejáratott szabványokkal. Így érthető, hogy a rokon-területnek számító IT audit nagyban támaszkodik a hagyományos auditálásban már bevált egységesítési módszertanokra.

Mintegy húszévnyi fejlődés után, amelynek során az új területen alkalmazott eljárások kikristályosodtak (ld. a történeti áttekintést a III.6.2. alfejezetben), az első teljes értékelési módszertanként értékelhető COBIT

[11] A magyarban is – jobb híján – átvett angolszász kifejezéssel: *benchmarking*.

előfutára 1977-ben jelent meg Kontroll Célkitűzések címen. Bár ez valójában nem tekinthető szabványnak, hiszen nem állami hatóság vagy kormányzati szerv teszi kötelezővé a használatát, a gyakorlatban a legelterjedtebb módszertan, amelyet a világ számos országában használnak az információtechnológiai audit folyamatok tervezésére és levezénylésére. Az alábbiakban az információtechnológiai auditálásra vonatkozó legfontosabb szabványokat tekintjük át.

IV.3. Szabványok és kvázi-szabványok

IV.3.1. COBIT

Valószínűleg a legelterjedtebb szabályrendszer, amely valójában nem tekinthető szabványnak, hiszen nincs is szabványként bejegyezve, a gyakorlatban azonban sokszor szabványszerűen alkalmazzák. Az ISACF[12] (Információrendszer Audit és Kontroll Alapítvány) 1996-ban jelentette meg a COBIT[13] (Kontroll célkitűzések az információtechnológia és kapcsolódó technológiák számára) első kiadását. Ez valójában olyan dokumentumok gyűjteményeként értelmezhető, amelyek az információtechnológiai kormányzás, kontroll és biztosítás általánosan elfogadott követendő gyakorlatait (*best practices*) tartalmazzák (ITGI, 2004). A gyűjtemény elsősorban az információtechnológiai auditálás céljait szolgálja. Az első kezdeménynek tekinthető Kontroll Célkitűzések 1977-es kiadása óta folyamatos fejlődések és frissítések segítségével az auditori munka irányítására és segítésére használják. 1998-ban a COBIT részévé tett Menedzsment irányelvekkel (ld. ITGI megalakulásának éve a történelmi áttekintésben) szélesebb körű célt tűzött ki maga elé, és egyre inkább az IT irányítás eszközévé válik. Az IT irányításban történő felhasználás elősegítésére mérési módszereket és érettségi modelleket is kínál. Ezeknek köszönhetően

[12] *Information Systems Audit and Control Foundation*

[13] A rövidítés az angol megfelelőből – *Control Objectives for Information and related Technology* – származik.

viszonylag könnyen felhasználható kockázatértékelési módszertanok alapjaként is (Lainhart, 2000).

A COBIT célja: „*Olyan hatályos, naprakész, nemzetközileg általánosan elfogadott kontroll célkitűzések kutatása, fejlesztése, közzététele és népszerűsítése, amelyek menedzserek, IT-szakértők és biztonsági szakértők a mindennapokban használhatnak.*" (COBIT, 2000c, p. 1.).

A COBIT elsősorban felsőszintű irányelveket tartalmaz. Bár ezekből a mindennapi használat során túlnyomórészt kikövetkeztethetők az adott területre vonatkozó tennivalók, a COBIT nem tartalmaz technikai részleteket. A célkitűzés szerint teljesen átfogó, de nem minden esetben specifikus megoldást kínál.

A teljesség elérése érdekében a COBIT kétféle szempont szerint közelít az informatikai rendszerekhez: egyrészt az üzleti célok támogatása felől, másrészt az informatikai erőforrások kezelése és az informatikai folyamatok menedzselése felől. Az üzleti célok elérése érdekében az információkkal kapcsolatban hét alapelv teljesülését követeli meg, amelyek három fő csoportba sorolhatók:

- Minőségi követelmények:
    - eredményesség - feleljen meg az üzleti igényeknek
    - hatékonyság - előállítása optimálisan történjen
- Biztonsági követelmények:
    - bizalmasság - csak az illetékesek férhessenek hozzá
    - integritás – legyen teljes
    - rendelkezésre állás – álljon mindig rendelkezésre
- Bizalmi követelmények:
    - megfelelőség – feleljen meg más vállalkozások, hatóságok elvárásainak
    - megbízhatóság– álljon összhangban a valósággal

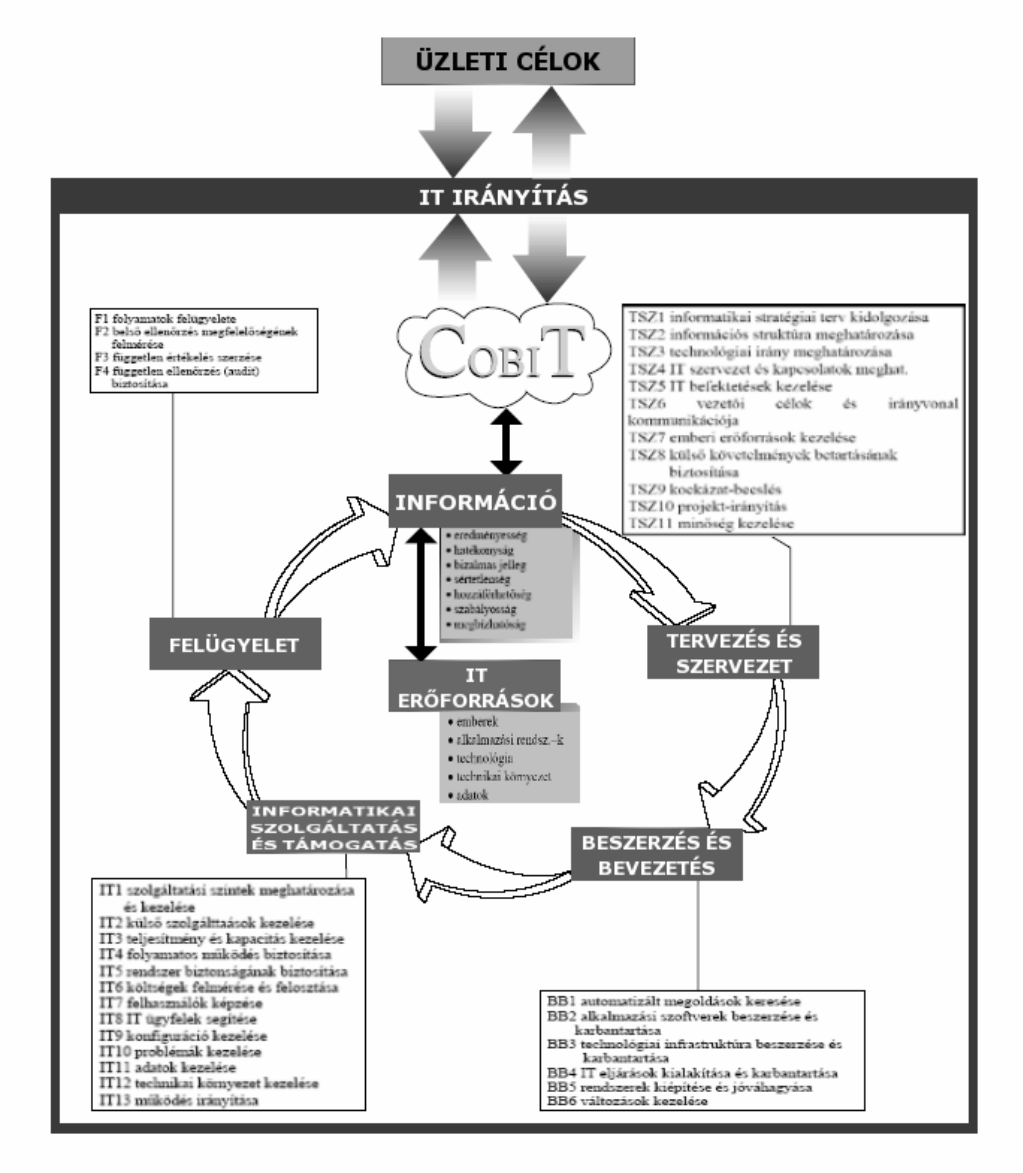
Az információtechnológiai erőforrások pedig öt csoportot alkotnak (ITGI, 2004):

- adatok
- alkalmazási rendszerek
- technológia
- támogató eszközök
- emberek

A COBIT megkülönböztet négy nagy területet az ellenőrizendő informatikai tevékenységekben, ezek az úgynevezett domének:

- Tervezés és Szervezet (PO) – az informatikai stratégia megalkotása és annak körülményei, valamint a szervezési kérdések
- Beszerzés és Megvalósítás (AI) – az eszközök beszerzéséhez és a rendszerbevezetéshez kapcsolódó kérdések, változáskezelés
- Szolgáltatás és Támogatás (DS) – a szolgáltatások nyújtásával és a felhasználás támogatásával kapcsolatos kérdések
- Felügyelet (M) – az informatikai folyamatok felügyelete, ismétlődő vizsgálata, értékelése

2. ábra

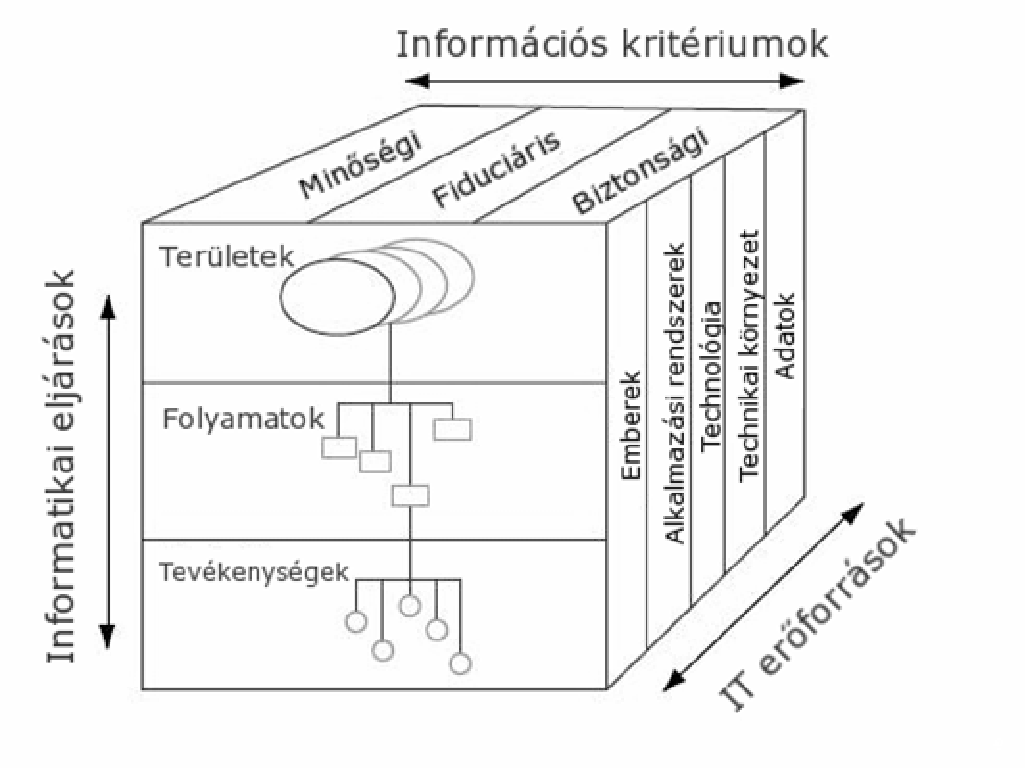


A COBIT értékelési területeinek rendszere (COBIT, 2000a)

A COBIT kialakítása és fejlesztése során igyekeznek a vizsgálandó problémákat a lehető legkevesebb eredendő elvre visszavezetni. Ezért a COBIT felépítése a korábbi kiadásokkal szemben az egyszerűsödés irányába mutat. A jelenleg megkülönböztetett négy terület is a korábbi területek összevonásaként állt elő. A kutatáshoz felhasznált harmadik kiadásban a négy fő terület összesen 34 magas szintű Kontroll Célkitűzést tartalmaz.

A fentiek alapján a COBIT felépítése egy háromdimenziós egységet képez, amelyben az egyik dimenziót az információs kritériumok – minőségi, bizalmi és biztonsági, a másikat az informatikai erőforrások – a hét korábban említett, a harmadikat pedig az informatikai folyamatok – területek, folyamatok és funkciók jelentik.

3. ábra



A COBIT "kocka" (COBIT, 2000c és COBIT, 2000d)

A COBIT a magas szintű áttekintésből kiindulva a gyakorlatban is jól használható útmutatóként szolgál az auditálások végrehajtásához. Az audit programok elkészítésétől kezdve az érettségi modellekig, az audit beszámolók készítéséig, és a *benchmarking* funkciókig számos segédeszközt kínál a gyakorlati alkalmazáshoz (Borda, 2001). Bár nem képezi szerves részét a technikai jellegű funkcióellenőrzések leírása, a COBIT-ra támaszkodva

számtalan ilyen jellegű útmutató készült (pl. integrált vállalatirányítási rendszerek ellenőrzésére)[14].

A COBIT tehát egy, a mindennapi ellenőrzésben és az audit munkálatok támogatásában kipróbált, jól bejáratott módszertan. Jelen kutatásban is jól alkalmazható, mint a kockázatértékelő rendszer kiindulópontja, hiszen a kockázatok felméréséhez rendkívül jó alapot biztosít. Ugyanakkor a COBIT nem tartalmaz számszerűsíthető eljárásokat a kockázatok értékelésére. Az érettségi modellek ugyan alkalmazhatók egy-egy terület készültségi fokának, a fennmaradó kockázatoknak az ellenőrzésére, ez azonban csak a kiindulópont lehet a metrika megalkotásához. Ezek ugyanis olyan kvalitatív értékelést tesznek csak lehetővé, amelyek közvetlenül nem alkalmasak számszerű kimutatások készítésére.

IV.3.2. ITIL

Az ITIL jelentése IT Infrastruktúra Könyvtár[15]. Valójában ez egy hét kötetből álló sorozat, amelyet brit kormányzati szervek adnak ki. Az ITIL az IT szolgáltatásmenedzsmentre vonatkozó „legjobb gyakorlatok" (*best practice*), követendő példák tárházát jelenti (ITIL, 1989). Bár a sorozatot egy kormányzati szerv adja ki, mégsem tekinthető *de jure* szabványnak. Az ITIL az információtechnológiát mint szolgáltatást értelmezi, központjában a felhasználó áll.

Az ITIL nem kifejezetten auditálási célokat szolgál, ugyanakkor teljességre törekvő szemlélete miatt az auditálással kapcsolatos kérdések jelentős részét felöleli. Jellegéből adódóan azonban nem foglalkozik számos olyan kérdéssel, amely a szervezeti illetve a monitorozási, felügyeleti területhez kapcsolódik. Az ITIL elsősorban a szolgáltatások nyújtására koncentrál, célközönségét pedig a szolgáltatásmenedzsmentért felelős személyek jelentik.

[14] Az SAP rendszerre vonatkoztatva ilyen az ISACA *Security, Control and Audit Features: SAP R/3* című kiadványa
[15] *IT Infrastructure Library*

Az ITIL, mint szolgáltatásközpontú szabályrendszer arra fókuszál, hogy milyen személyek, milyen felelősségekkel és hogyan nyújtják ezeket a szolgáltatásokat. Az ITIL egy felhasználó-központú, átfogó szolgáltatásmenedzsment rendszer. Az érintett fő témakörök (ITGI, 2004):

- Szolgáltatások támogatása:
  - eseménykezelés
  - problémakezelés
  - konfigurációkezelés
  - változásmenedzsment
  - verziókezelés
- Szolgáltatások végzése:
  - szolgáltatásiszint-kezelés
  - IT-szolgáltatások pénzügyi menedzsmentje
  - kapacitásmenedzsment
  - IT-szolgáltatatások folytonosságának biztosítása
  - rendelkezésre-állás biztosítása

Az ITIL tehát egy átfogó szolgáltatásmenedzsment értékelő segédeszköz, amely az infrastruktúra kezelés minden lényeges elemére kitér (Yoke, 2005). Ezért a vállalatok informatikai folyamatainak elemzésére és felügyeletére rendkívül jól használható, sok gyakorlati tapasztalatot tartalmaz. Ez a tudás beépül a vállalatok auditálási gyakorlatába is, de az auditálás céljait csak részben meríti ki (Morency, 2005).

IV.3.3. ISO/IEC 17799:2000

Az ISO 17799 valódi szabvány, amely a brit BS 7799-es szabvány első részének felhasználásával készült. Az eredeti, 1999-ben kiadott brit szabvány ugyanis két részből áll: az első az „Információtechnológia – Információ-biztonsági menedzsment gyakorlati eljárásrend”[16], a második pedig az

[16] *Information Technology—Code of Practice for Information Security Management*

„Információ-biztonság menedzsment rendszerek – specifikáció gyakorlati útmutatóval”[17] címet kapta.

Az ISO 17799-es szabvány az informatikai biztonság kidolgozásáért felelős alkalmazottak számára nyújt segítséget. Egy olyan alapot jelent, amelyre támaszkodva kidolgozhatók a vállalat biztonságra vonatkozó szabályzatai, és azok az eljárásrendek, amelyeknek köszönhetően a vállalat külső érintettjei is megbízhatnak az adott vállalat információbiztonságában (ISO/IEC 17799, 2000).

4. ábra

Az ISO 17799 által lefedett területek (BS7799, 2004)

Az információbiztonsággal kapcsolatos iránymutatás tíz részből áll, amelyek összesen 36 célkitűzést és 127 kontrollt tartalmaznak. A tíz terület, amelyet számba kell venni az információbiztonság kapcsán (lásd a 4. ábrát):

- Biztonsági politika
- Szervezeti biztonság

[17] *Information Security Management Systems—Specification with Guidance for Use*

- Eszközök osztályozása és ellenőrzése
- Személyzeti biztonság
- Fizikai és környezeti biztonság
- Kommunikációs és működési menedzsment
- Hozzáférések ellenőrzése
- Rendszerfejlesztés és karbantartás
- Folyamatos üzletmenet fenntartása
- Megfelelőség

A szabvány az információbiztonságra koncentrál, ezért számos, a menedzsmentre vonatkozó kérdés nem szerepel a vizsgálandó területek között. A szabvány az információbiztonság technikai-technológiai kérdéseit helyezi előtérbe, és bár számos auditálás során hivatkoznak rá, mint összehasonlítási alapra, jellegéből adódóan nem lehet teljes. Ugyanakkor az ISO 17799-es szabvány nagy hatással van szinte minden audittal foglalkozó szakértőre, és az ebből leszűrhető tudást széleskörűen alkalmazzák, olykor más szabályrendszerek kiegészítéseként. Számos olyan auditálási segédszoftver is elérhető, amely ezt a szabványt alkalmazza értékelései során.

IV.3.4. ISO/IEC TR 13334

Az ISO 13334-es szabvány egy öt részből álló beszámoló-struktúra, amely az „Információtechnológia – IT biztonsági menedzsment útmutató” címet kapta. Kifejezetten a menedzsment kérdésekkel foglalkozik. Az öt rész:

- IT-biztonsági koncepciók és modellek
- IT-biztonság menedzsment és tervezés
- IT-biztonság menedzsment technikák
- Biztosítékok kiválasztása
- Hálózati biztonság menedzsment útmutató

A gyűjtemény első része kifejezetten a vállalati döntéshozók számára készült, a többi terület pedig az informatikai biztonságért felelős szakembereket – IT-menedzsereket, IT biztonsági személyzetet célozza meg.

Az ISO 13334-es szabvány jól alkalmazható az informatikai biztonsággal kapcsolatos menedzsment kérdések vizsgálatakor.

IV.3.5. Common Criteria

A Common Criteria (CC) – magyarra Közös követelményekként fordítható – az Európai Bizottság által 1991-ben kiadott ITSEC[18] (Információtechnológiai biztonság-értékelési követelmények) utóda. A hivatalos címe: Közös követelmények az információtechnológiai biztonság értékeléséhez[19]. A CC-ra alapozva nemzetközi szabvány is készült ISO/IEC 15408:1999 címen, amely tartalmában gyakorlatilag megegyezik az eredetivel (ISO/IEC 15408, 1999).

A szabvány széles nemzetközi együttműködés eredményeként jött létre. Célja egy olyan követelményrendszer kialakítása, amely lehetővé teszi az információtechnológiai biztonság egységes és összehasonlítható értékelését. A célközönség nagyon széles tömegeket ölel fel, talán ennek is köszönhető, hogy az egyik legismertebb követelményrendszer. Egyaránt szól a vevőkhöz, felhasználókhoz, fejlesztőkhöz, értékelőkhöz, illetve a biztonsági szakemberekhez. A CC rendkívül részletes, ráadásul ingyenesen hozzáférhető, így nagy népszerűségre tett szert. Ugyanakkor nem foglalkozik tervezési, szervezeti és menedzsment kérdésekkel, hanem az IT termékekre és szolgáltatásokra koncentrál. Így, bár ezeken a részterületeken rendkívül hasznos és időtálló gyűjteménynek bizonyult, nem tekinthető teljesnek.

Három részből áll (CC, 1999):

1. Bevezetés és általános modell: az információtechnológiai biztonság értékelésének általános modelljét adja.
2. Funkcionális biztonsági követelmények: olyan funkcionális összetevőket tartalmaz, amelyek értékelési célpontként értelmezhetők a biztonsági követelmények megfogalmazása során.

[18] *Information Technology Security Evaluation Criteria*

[19] *Common Criteria for Information Technology Security Evaluation*

3. Biztonsági garancia követelmények: olyan követelmények gyűjteménye, amelyek alapot jelentenek az informatikai termékek és szolgáltatások biztonsági garanciáinak meghatározásához.

A Common Criteria használható kockázatértékelési rendszer alapjaként is, különösen a második rész, amelyben olyan entitások kerülnek meghatározásra, amelyek mint kockázatviselő tényezők kerülhetnek előtérbe. Ugyanakkor egy kizárólag a CC-ra támaszkodó értékelési eljárás nem lehet teljes, hiszen maga a követelményrendszer sem terjed ki olyan fontos tényezőkre, mint a menedzsmenttel kapcsolatos vagy szervezeti kérdések.

IV.3.6. TickIT

A 2001-ben publikált TickIt a BSI (Brit Szabványügyi Hivatal) kezdeményezése, amely a vállalati szoftver minőségbiztosítási rendszerek értékelésére szolgál (TickIT, 1994). Ennek megfelelően elsősorban szoftverfejlesztéssel foglalkozó cégek számára nyújt útmutatást. A követelményeknek eleget tevő vállalatok számára tanúsítványokat állítanak ki, amelyben a megfelelő minőségbiztosítási tevékenység meglétét garantálják.

A TickIT célja kifejezetten csak a szoftverfejlesztéssel kapcsolatos funkciók felmérése, így a stratégiaalkotási és működtetési kérdésekkel egyáltalán nem foglalkozik. Az érintett területeken is inkább általános megfogalmazásokat tartalmaz, így gyakorlati használhatósága korlátozott. Fő célja az ISO 9000-es szabványcsalád keretein belül egy olyan tanúsítvány kiadása, amely a szoftverfejlesztési minőségbiztosítás kérdéseit érinti.

IV.3.7. NIST 800-14

Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST[20]) kiadványa az „Általánosan elfogadott elvek és gyakorlatok az információtechnológiai rendszerek biztosítására” egy viszonylag átfogó, ugyanakkor magas szintű, elvi megközelítést alkalmaz a biztonsági

[20] *National Institute of Standards and Technology*

követelmények megfogalmazásában (NIST, 1996). Elsősorban az Amerikai Egyesült Államokban meglévő viszonyokra, a helyi kormányzati erőkre koncentrál, így nemzetközi, vagy magyarországi felhasználhatósága erősen korlátozott. Főleg olyan általános elveket tartalmaz, amelyek közérthetően fogalmazzák meg, hogy milyen biztonsági szempontokat kell figyelembe venni a kormányzati működés során.

IV.3.8. COSO

A COSO a belső ellenőrzésre vonatkozó szabványosítási törekvések eredménye. Valójában az ezen a néven ismertté vált előírásrendszer címe: „COSO Belső kontroll – integrált keretrendszer[21]", amelyet a COSO[22] nevű, a számviteli visszaélések kiküszöbölésére alakult önkéntes szervezet ad ki. Az első kiadás 1992-ben jelent meg.

A COSO a belső kontroll átfogó módszertana. Célja, hogy a felsővezetők számára meghatározza azon belső kontrollok felállításának módját, amelyek a vállalat céljainak elérését, és a kockázatok kezelését lehetővé teszik (COSO, 1992).

Jellegéből adódóan a COSO, amely inkább pénzügyi-számviteli előírásrendszerként ismert, nem foglalkozik részletesen az információtechnológia speciális problémáival. Ezen a területen rendkívül magas szintű követelményeket fogalmaz meg, amelyek a különböző politikaalkotások alapjaként, vagy a vállalati koncepcióalkotás szintjén hasznosíthatók. Ugyanakkor az IT audit részletes sorvezetőjeként nem alkalmazható közvetlenül. A COSO logikus felépítése, áttekinthető szerkezete ellenben inspirációt jelentett az információtechnológiai szabványok, elsősorban a COBIT megalkotásában. A COBIT felépítése és működése számos helyen támaszkodik a COSO által kialakított koncepcióra.

[21] *COSO Internal Control—Integrated Framework*

[22] *Committee of Sponsoring Organizations of the Treadway Commission*

A COSO 2001-ben, a PriceWaterhouseCoopers együttműködésével kezdett dolgozni egy olyan útmutatón, amely alkalmas lehet a vállalati kockázatkezelési módszerek értékelésére. A fejlesztés időben éppen egybeesett számos vállalati könyvelési botránnyal, amely nyilvánvalóan befolyásolta a készítőket. A 2004-ben publikált COSO ERM[23] egy olyan átfogó rendszer, amely a vállalati kockázatok kezelésének teljes spektrumát kívánja lefedni. Célkitűzése szerint egy olyan keretrendszert kíván nyújtani, amely a vállalati menedzsment részére lehetővé teszi a felmerülő kockázatok szisztematikus felmérését, és a kockázatok hatékony és gyors kezelését (COSO, 2004). Így a kitűzött cél nagyon közel áll a jelen kutatás témájához, ugyanakkor túlságosan is széles ahhoz, hogy a konkrét kockázatértékelési metrika megalkotásában fel tudjuk használni közvetlenül.

IV.3.9. CRAMM

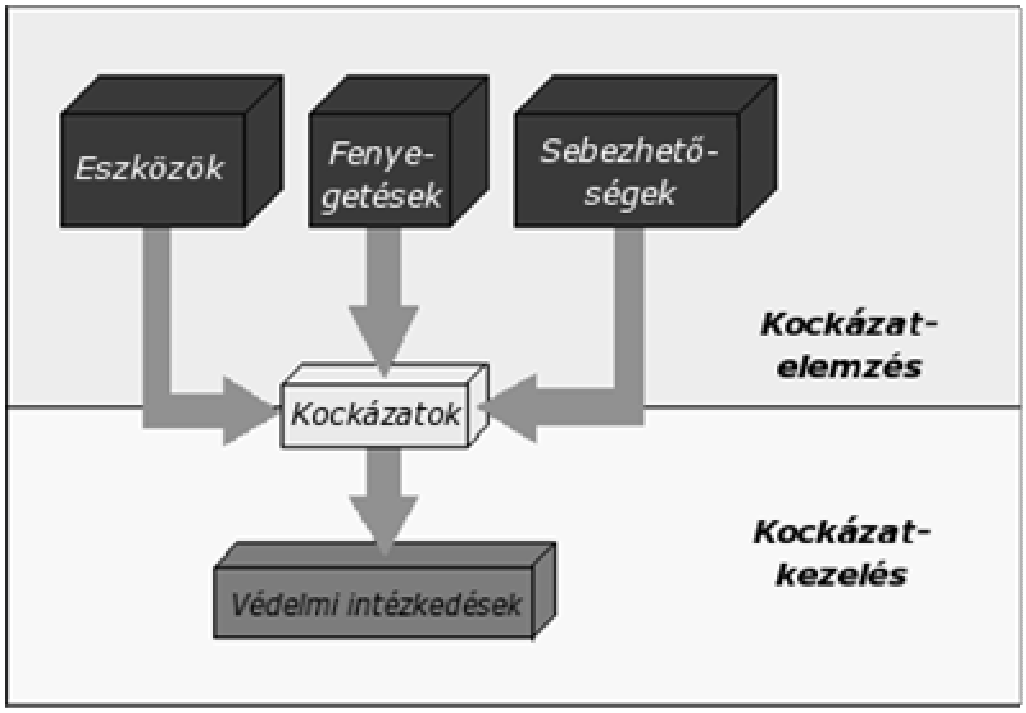
A CRAMM[24] a brit kormányzat által 1985-ben publikált (és azóta több frissített kiadást megért) kvalitatív kockázatértékelési és kockázatkezelési módszere. Megalkotásának célja az volt, hogy a brit kormányzati szervek számára útmutatást nyújtson az informatikai biztonsági ellenőrzésekhez.

A CRAMM a kockázatokat három tényező: az informatikai eszközök, a fenyegetések és a sebezhetőségek eredőjeként határozza meg (lásd az 5. ábrát).

[23] *COSO Enterprise Risk Management*

[24] *CRAMM – CCTA Risk Analysis and Management Method* (CCTA Kockázatelemzési és –menedzsment módszer). A CCTA a brit kormányzat központi számítógépes és telekommunikációs ügynöksége. Az ügynökség szerepét az OGC nevű szervezet (az ITIL megalkotója) vette át 2001-ben.

5. ábra



Kockázati összetevők a CRAMM szerint (CRAMM, 2004)

A kockázatok csökkentését a három összetevő minél alacsonyabb szinten tartásával lehet megvalósítani. Ezen az elven több gyakorlati megoldás is nyugszik, például banki alkalmazások biztonsági értékelésére (Laliberte, 2004).

A CRAMM alapján készült kereskedelmi szoftver is, amely felhasználható a vállalati informatikai kockázatok értékelésére. Ezt a módszert a magyarországi ajánlások megalkotásakor is figyelembe vették.

A módszerben felhasznált metrizálás meglehetősen egyszerű, ezért a kutatáshoz közvetlenül nem használható, ugyanakkor a megközelítés módja hasznos lehet az egyes kockázati tényezők azonosítása során.

IV.4. Következtetések

Az eddigiekben a legfontosabb szabványokat, illetve szabványszerű kezdeményezéseket tekinthettük át, amelyek az információtechnológiai auditálás és az információbiztonság vizsgálata során szóba jöhetnek. Ezek egy

része kifejezetten az információtechnológiai biztonsággal foglalkoznak, mások (pl. COSO) pedig azt csak, mint a vállalat működésének egyik egységét elemzik. Előbbiek általában részletesebben foglalkoznak az IT kérdéseivel, ugyanakkor kevéssé térnek ki az információtechnológiához kapcsolódó területek értékelésére.

Ezért, bár a kockázatértékelés alapjaként részben használhatók – azokon a területeken, amelyek részletesen kidolgozottak, az IT szervezeti, szervezési kérdéseivel, és általában a kevésbé technológiai jellegű kockázatok értékelésénél nem nyújtanak kellő támpontot. Az általános útmutatások pedig, átfogó jellegükből adódóan, nem elég részletezettek az információrendszerek kérdéseit illetően. Bár komoly segítséget jelenthetnek az információtechnológia megfelelő környezetben történő értékeléséhez, a konkrét kockázatok területén, amelyeket az adott rendszert elemezve kell megállapítani, csak nagyon korlátozottan használhatók.

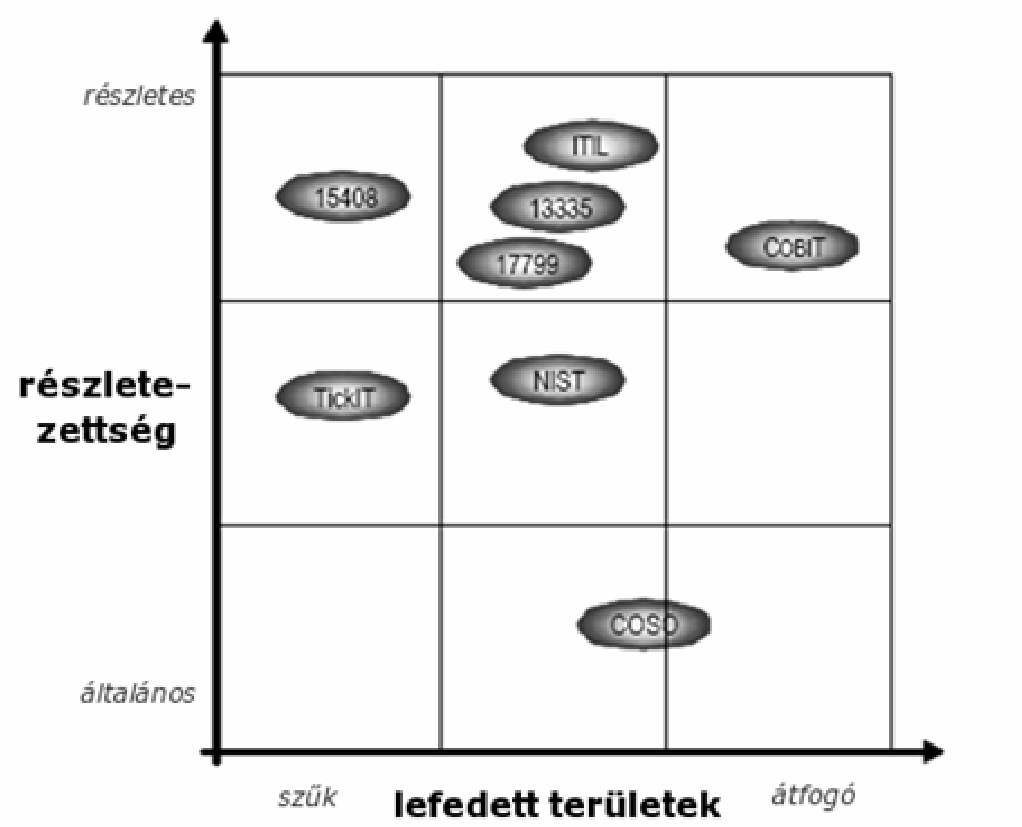
Megjegyzendő, hogy az informatikai termékekre, informatikai folyamatokra, informatikai projektekre, és ezek kockázataira vonatkozóan még számos előírás vonatkozik, amelyek egy-egy terület pontosításában segítséget nyújthatnak (Crockett – Foster, 2004), ugyanakkor nem eléggé átfogóak ahhoz, hogy a jelen kutatásban könnyen felhasználhatóak legyenek. Legalább hivatkozás szintjén azonban feltétlenül említést érdemelnek a következők:

- Informatikai rendszertermékek fejlesztésének specifikációi (BS 7738-1, 1994).
- Számítógépes alkalmazási rendszerek dokumentálása (ISO 6592, 2000).
- Az ISO 9001 követelmények alkalmazása a szoftverfejlesztésben és üzemeltetésben (ISO 9000-3, 1991).
- Szoftver életciklus kezelés (ISO/IEC 12207, 1995).
- Szoftverfolyamatok értékelése (ISO/IEC TR 15504-5:1999, 1999).
- Szoftvertermékek értékelése (MSZ ISO/IEC 9126:2000, 2000)

Meg kell továbbá említeni, hogy Magyarországon is történtek erőfeszítések az átfogó biztonsági követelményrendszer kidolgozására, amelynek legjobb példái az Informatikai Tárcaközi Bizottságnak – részben a fent említett követelmények felhasználásával – elkészített 8. és 12. számú ajánlásai (ITB, 1994a és ITB 1994b).

Az eddigiek alapján megállapítható, hogy a legfigyelemreméltóbb keretrendszerek, amelyek szóba jöhetnek a kockázatértékelési rendszer kidolgozásának alapjaként az ISO 17799, a COSO illetve a COBIT. Az ISO 17799 meglehetősen részletes útmutatással szolgál a technikai elemeket illetően (Solms, 2005), és ezért felhasználható a konkrét rendszerek értékeléséhez, azonban a menedzsment és szervezeti kérdésekkel nem foglalkozik részletesen, az ezekből adódó kockázatok elemzéséhez nem használható. A COSO pedig igen nagy területet fed le, ugyanakkor nem annyira részletes, hogy közvetlenül lehessen erre a célra használni. A COBIT mind széles látókörével, mind aránylag mély részletezettségével nagy segítséget nyújthat egy kockázatértékelő rendszer elkészítéséhez (6. ábra).

6. ábra



A COBIT és más előírásrendszerek áttekintése a lefedett területek szerint (ITGI, 2004)

A COBIT célja szerint teljes, tehát valamennyi területre kiterjed, amely az információtechnológiai kérdések vizsgálatakor felmerülhet. Ráadásul a COBIT gyakorlatilag az egyetlen olyan szabályrendszer az említettek közül, amelyet kifejezetten auditálási célra hoztak létre, így felépítésében és működésében is követi az auditálási eljárás során alkalmazott technikát. Bár a COBIT valójában nem szabvány, mint az ISO 17799, és ez némileg ellene szól, hiszen nem egy hivatalos hatóság állítja elő, ennek ellenére az IT audit területén szinte szabványként alkalmazzák. Elmondható, hogy a kutatás szempontjából a COBIT a megfelelő középutat jelenti, hiszen mind a felölelt terület, mind részletezettsége a kívánt mértékű.

A COBIT mellett szól az a nem elhanyagolható tény is, hogy míg az ISO 17799-es szabvány megvásárolandó termék, amely fizetés ellenében érhető el a szabványügyi hivataltól, addig a COBIT szabadon hozzáférhető. Ez

nem csak a megvalósítás, hanem az esetleges utóhasznosítás szempontjából sem mellékes. A fenti tényezők együttes értékelése után lehetett úgy dönteni, hogy a kialakítandó kockázatértékelési rendszer alapjaként a COBIT alkalmazható.

A COBIT használata azonban felvet komoly nehézségeket is. A legnagyobb probléma, hogy a COBIT nem nevez meg kockázatokat az információrendszerek auditálásában, ilyen mértékű részletezettséget nem ér el. Ugyanakkor kézenfekvő, hogy a részletes kontroll célkitűzéseket, amelyek csupán egy szinttel vannak feljebb a kockázatoknál, viszonylag kevés munkával átalakíthatjuk, és az adott problémára értelmezve, a kívánt kockázati tényezők meghatározásai előállíthatók. A kockázatértékelési rendszer kialakításakor ezt figyelembe kell venni, és számolni kell a kockázati tényezők előállításának kérdésével.

V. FEJEZET
Kockázatok értékelése az informatikai auditálásban

V.1. A kockázatértékelés szerepe az IT auditban

Az információtechnológiai auditálás célja, hogy feltárja a vállalatban az információtechnológiához kapcsolódó termékek, szolgáltatások, szervezeti egységek, személyek, eljárások tulajdonságait, és ezeket egy előre meghatározott szempontrendszer szerint értékelje. Gazdasági szempontból az IT auditálás célja, hogy a vállalat meg tudjon felelni a kitűzött céloknak, megfelelően hatékonyan és eredményesen működjön. Ennek érdekében az auditor megvizsgálja, hogy a vállalatnál követett eljárások megfelelnek-e a rögzített szabályoknak. Az ellenőrzés végeztével az auditor beszámolót készít, amelyben részletezi a feltárt hiányosságokat, és észrevételeket tesz a teendőkkel kapcsolatban.

Közismert vélekedés, hogy tökéletes biztonság nem létezik. Nem csak az üzleti teendőkkel kapcsolatban, hanem az információs infrastruktúrával összefüggésben is mindig lesznek kockázatok (Stewart, 2004). Ezért amikor a beszámoló megrendelője értékeli az eredményeket, a legtöbb esetben lesz valamilyen probléma, amelyre koncentrálnia kell. Sőt, a legtöbb esetben számos olyan kockázatra felhívják a figyelmet, amelyek a vállalat biztonságos és gazdaságos működését veszélyeztetik. Az auditálás célja, a vállalat biztonsági szintjének tanúsításán túlmenően, éppen ezeknek a hiányosságoknak a feltárása.

A vállalatvezetők, illetve az audit jelentés megrendelői hatáskörüktől függően dönthetnek arról, milyen módon hasznosítják az audit beszámolóban eléjük tárt eredményeket. A problémák rangsorolásánál és az erőforrások elosztásánál nagy jelentősége van a különböző kockázati tényezők érintettségének. Számos olyan probléma fordulhat elő, amely különösebb költség, ráfordítás nélkül is kiküszöbölhető. A legtöbb kockázati tényező

azonban költségekkel, esetleg más erőforrások bevonásával jár. Az erőforrások megfelelő allokációjához, a lehető leghatékonyabb kockázat-elhárításhoz pedig szükséges a kockázati tényezők rangsorolása. Ehhez azonban valamilyen kézzelfogható és összehasonlítható mérőszámot kell találni (Vijayan, 2003).

Egy másik feladat, hogy a vállalat biztonsági szintjét, és a felmerülő problémák nagyságát össze lehessen mérni a korábbi állapotokkal, illetve az iparágban működő egyéb vállalatok biztonsági szintjeivel (*benchmarking*). Ezen funkciók ellátásához rendkívül hasznos egy olyan mérési skála alkalmazása, amely lehetővé teszi a problémák nagyság szerinti sorba rendezését, a kockázatok veszélyessége és esetleges következményei alapján (Dilla – Stone, 1997), így lehetővé téve az összemérhetőséget és az erőforrások megfelelő allokációját a problémák kiküszöbölésére. Ehhez nyújt nagy segítséget a kockázatértékelési rendszer kialakítása.

Természetesen mindezek az eljárások csak úgy lehetnek sikeresek, ha a kockázatok kezelése a vállalati kultúra részévé is válik, és a menedzsment megfelelően közelít a kérdésekhez (Ashenden, 2005; Dodds – Hague, 2004; Nolan – McFarlan, 2005). Ez a globális szemlélet megjelenik a követelmények között is, például a COBIT és a COSO ERM esetében (COBIT, 2000b és COSO, 2004) (lásd a IV.3. alfejezetet).

V.2. Az auditálási szabályok átalakulása

Az auditálás – legalább is, amit általánosan értenek e fogalom alatt –, mint azt a történelmi áttekintésben is láthattuk, nagyon hosszú múltra tekinthet vissza. A vállalatok gazdálkodásának ellenőrzése és a beszámolók valóságtartalmának jóváhagyása gyakorlatilag részévé lett a nagyvállalatokról kialakult képnek. A cégeknek szükségük van azokra a tanúsítványokra, amelyeket a könyvvizsgálók állítanak ki az előírásoknak való megfelelésről. A tanúsítvány azonban természetesen csak abban az esetben értékelhető, amennyiben annak kiállítója valóban függetlennek, elfogulatlannak és minden manipulációs gyanún felül állónak tekinthető. Nem véletlen, hogy a könyvvizsgálat területén a cégek nagyfokú koncentrációja a jellemző, hiszen

ezen tevékenység végzéséhez, ahhoz, hogy az eredmény hitelesnek tűnjön, szükséges egy olyan márkanév, amely világszerte a fent említett tulajdonságokkal rokon értelmű. Ehhez pedig olyan nagy cégek szükségesek, amelyek a világ minden táján jelen tudnak lenni, és el tudják végezni az ellenőrzéseket, valamint a tanúsítványok kiadását.

Az utóbbi néhány évben azonban számos olyan esemény történt, amely alapvetően megrengette a könyvvizsgálatba, az auditálásba, és az ezeket a tevékenységeket végző cégekbe vetett bizalmat. Az Egyesült Államokban az ENRON, a WorldCom és más cégek, illetve néhány európai nagyvállalat, például a Parmalat esetében is előfordult, hogy a vállalatok anyagi helyzete egészen nagymértékben eltért a könyvvizsgálatban szereplő értékektől. A legtöbb esetben az auditálást végző cégeket is felelőssé tették azért, hogy a befektetők és a vállalat egyéb érintettjei a valóságot nem tükröző információkat kaptak a cégek gazdálkodásáról (Rezaee, 2005). Ennek eredményeként a könyvvizsgáló cégekbe vetett bizalom megrendült. Sokan felismerték, hogy ezek a jelenségek nem fogadhatók el pusztán statisztikai hibaként, hanem az auditálási módszerek megújításának szükségességét jelzik (Alles – Kogan – Vasarhelyi, 2004).

A kormányzati szervek sem tétlenkedtek; új előírásokat léptettek életbe, annak érdekében, hogy a korábban tapasztalható bizalom legalább részben helyreálljon, egyúttal az auditálási munka és a könyvvizsgálási folyamat minél áttekinthetőbb legyen. Többek között az áttekinthetőség, átláthatóság biztosításával kívánják elejét venni, hogy a továbbiakban az eddig tapasztaltakhoz hasonló botrányos esetek forduljanak elő. Az Egyesült Államokban a Sarbanes-Oxley törvény elfogadásával, az Európai Unión belül pedig a 8. direktíva továbbfejlesztésével, kiegészítésével és átdolgozásával próbálják elérni, hogy az auditálás visszanyerje megbecsülését, és a beszámolók megbízhatósága helyreálljon.

Az is világos, hogy az új szabályozás csak abban az esetben lehet sikeres, amennyiben a vállalati döntéshozók maguk is a kockázatok kezelését a vállalat működésének szerves részét képező tevékenységként fogják fel. (Asare

– Cohen – Trompeter, 2005). Mindehhez számos esetben új menedzsment módszerekre is szükség van.

V.2.1. A Sarbanes-Oxley törvény és az EU 8. direktíva

A 2002-ben elfogadott Sarbanes-Oxley törvény (SOX) fő célja a könyvelési botrányok miatt megrendült befektetői bizalom visszaállítása az amerikai nagyvállalatokkal szemben. Ennek érdekében szigorú előírásokat tartalmaz a beszámolókra vonatkozó felelősségek, a vállalat döntéshozóinak személyes érintettsége, az auditálás teljes függetlenségének biztosítása és más érzékeny pontok vonatkozásában. A törvény eredményeként számos vállalati folyamatot felül kell vizsgálni, és a hatáskörök, valamint az audit folyamat és az auditálással kapcsolatos felelősségek is jobban rögzítve vannak (Vranceanu, 2005).

Az EU 8. direktíváját eredetileg 1984-ben iktatták törvénybe (84/253/EEC, 1984). A direktíva a könyvelési auditálást végző személyekkel kapcsolatos követelményeket és a megfelelési feltételeket tartalmazza. A nemrégiben történt könyvelési botrányok következtében, a Sarbanes-Oxley törvényhez nagyon hasonló módon, a befektetői bizalom visszaállítása érdekében átalakították a direktívát. A 2005-ben elfogadott, továbbfejlesztett dokumentum az amerikai mintához hasonlóan szigorú szabályokat tartalmaz az auditálásokat végző személyek és a vállalatvezetők felelősségéről, valamint az auditálásokat végző testületek függetlenségéről (Turley, 2004).

Ezek az előírások az auditálás egészére vonatkoznak, és kimondva vagy kimondatlanul a pénzügyi ellenőrzés, elsősorban pedig a vállalati beszámolók értékelése áll a legfontosabb helyen. Ilyen módon az információtechnológiai auditálást csak közvetve érintik, ugyanakkor az informatikai auditálást végző szervezetekre is kötelező érvényűek.

A közvetett hatások azonban várhatóan igen erőteljesek lesznek (Damianides, 2004). A következő években a vállalatok audit tevékenysége előreláthatólag egyre fontosabbá válik, és a beszámolók elemzésén és a biztonsági hiányosságok felfedésén túlmenő, a vállalat egész működését

befolyásoló, globális tényezővé válik (Brown – Nasuti, 2005). Az audit kontrollok mintegy beépülnek a vállalati szervezetbe, és a teljes működésben, felépítésben szerepet kap az auditálhatóság szempontja. Így az előírások közvetett hatásai várhatóan jóval jelentősebbek lesznek a közvetlen hatásoknál. Az átalakulás, amely a vállalatvezetők gondolkodását egyre inkább az átfogó vállalatirányítás, az információtechnológiában érintett ellenőröket pedig az IT irányítás irányába vezérli, már elkezdődött. Ezért a kockázatok értékelése mindinkább szerves részét képezi a vállalati működésnek, és a kockázatkezelést az üzleti folyamatokban is figyelembe kell venni.

V.2.2. Kockázatértékelési egységesítés: Bázel II.

A fent említett változások hatására több területen is felmerült az egységesítés, szabványosítás és az átláthatóság biztosításának igénye. Az egyik leginkább érintett terület, ahol a szabványos értékelések hiánya a felügyeleti jogok gyakorlását gátolta, a banki-pénzügyi szektor. Ezen a területen felismerték, hogy a megfelelő tőkekövetelmények egységes meghatározásához szükség van arra, hogy a bankok pénzügyi tranzakcióiból és működéséből eredő kockázatokat egységesen ítéljék meg. Ezért olyan szervezetet hoztak létre, amely alapos kutatómunkával kidolgozta a különböző, pénzintézeteket érintő kockázatok egységes értékelésének módszertanát. Ez a Bázel Bizottság, amely a felügyeleti szervek tőke-megfelelőségi kritériumai konvergenciájának biztosítását kívánja elérni (Basel, 2004). Ezen cél érdekében pedig elsősorban azt kívánják biztosítani, hogy a különböző kockázatok megítélése szabványos módon történjen. A több évig tartó, számos szervezetet felölelő együttműködés eredménye egy olyan beszámoló, amely a kockázatok értékelésére vonatkozó egységesítési eljárásokat is tartalmaz.

Bár a Bázel II. néven ismertté vált együttműködés nem foglalkozik az informatikai kockázatok részletes elemzésével, az együttműködés és az értékelések szabványosítására való törekvés példaértékű lehet az IT audit számára is.

V.3. A kockázatmenedzsment alapfogalmai

Az információrendszerek kockázataival kapcsolatban az alapvető fogalmak tisztázásra szorulnak. *Kockázatelemzésen* azt a folyamatot értjük, amely során az információrendszerekkel kapcsolatos eszközöket, és az ezekhez kapcsolódó veszélyeztetettség mértékét felmérjük (Micksch, 2000). A *kockázatértékelés* során megállapítjuk, hogy a feltárt kockázatok mennyire kritikusak, és így az egyes problémák mennyire tekintendők súlyosnak. A *kockázatkezelés* pedig a kockázatértékelés eredményeinek felhasználásával az erőforrások megfelelő allokációját, és megfelelő politikák alkalmazásával, a lehető leginkább költséghatékony módon történő felhasználását jelenti a kockázatok minimalizálására.

Az ISO/IEC 73 és az ennek felhasználásával készült AS/NZS 4360 ausztrál/ új-zélandi szabvány megkülönbözteti a *kockázatok azonosítását*, a *kockázatok értékelését* és a *kockázatok kezelését*. Ebben a felfogásban a kockázatértékelés is két részből áll: a kockázatok elemzéséből és a kockázatok kiértékeléséből[25]. (AS/NZS 4360:2004, 2004)

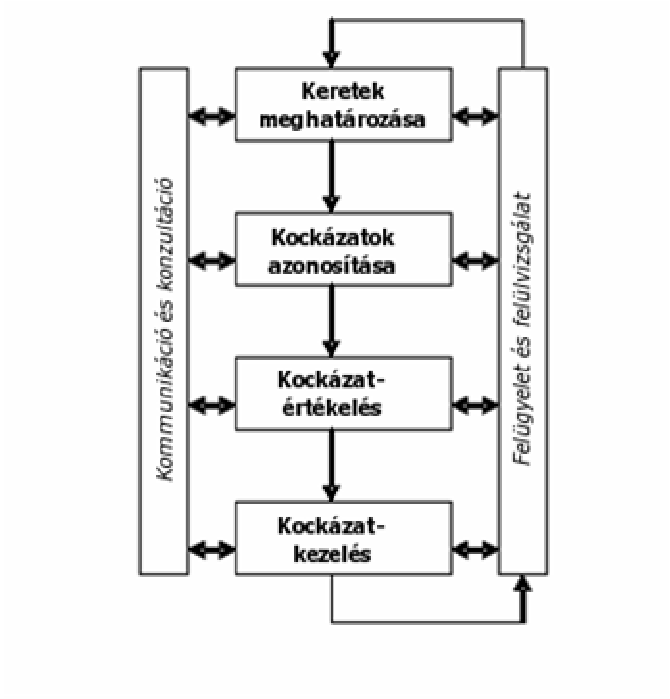
A jelen kutatás felfogásában, és a kockázatmenedzsment folyamatának értelmezésében ennek az utóbbi modellnek a módosított változatára támaszkodik. Az itt alkalmazott megközelítés szerint a kockázatmenedzsment folyamata 4 fő lépésből áll:

- A keretek meghatározása
- A kockázatok azonosítása
- Kockázatértékelés
- Kockázatok kezelése

A kockázatmenedzsment folyamatában azonban fontos szerepe van a folyamatos kommunikációnak és a felügyeletnek is, amely számos ponton kapcsolódik visszacsatolásokkal (lásd a 7. ábrát).

[25] *Risk evaluation*

7. ábra



A kockázatmenedzsment folyamata (AS/NZS 4360:2004, 2004 alapján)

Az auditálási folyamatban a kockázatok azonosítása és a kockázatelemzés megtörténik. Egy átfogó információtechnológiai auditálás ráadásul nem csupán a technológiával közvetlenül kapcsolatban lévő területeket, hanem a szervezeti és tervezési kérdéseket is érinti. A veszélyeztetett területeket és a veszélyeztetettség mértékét az audit beszámolók többnyire tartalmazzák. Ezen problémák felmérése az auditálás elsődleges célja, ezért ehhez számos segítséget kínálnak a különböző segédeszközök.

A kockázatkezelés közvetlenül nem képezi részét az auditálási folyamatnak, azonban a végső megállapítások felhasználhatók a vállalat felelős alkalmazottai számára, hogy a különböző kockázati tényezők kiküszöbölhetőek vagy mérsékelhetőek legyenek. Nem szabad azonban arról sem megfeledkezni, hogy az auditálás nem egyszeri feladat, hanem egy folyamatos, és a vállalati működésbe beépülő koncepciót kell, hogy jelentsen (Flowerday – Solms, 2005). Ilyen felfogásban a kockázatkezelés tehát kölcsönhatásban van az auditálással, hiszen a megfelelően végzett kockázatkezelés eredményét az auditálás is visszaigazolja, amennyiben pedig a kockázatok kezelésének

módszerei nem épülnek be kellően a vállalat működésébe, arról megfelelő módon tájékoztat.

A folyamat középső szakasza a kockázatok értékelése (Haimes, 1998). Ebben a szakaszban a feltárt kockázati tényezők súlyosságának megállapítása történik. A megfelelő lépések megtételének előkészítése érdekében ugyanis el kell dönteni, hogy egy-egy probléma mennyire kritikus, illetve a vállalat működése szempontjából mekkora veszélyt jelent. Ez pedig talán a legnehezebb kérdése az auditori munkának és a kockázatokkal kapcsolatos kérdéskörnek (Tregear, 2001). Az értékelést ugyanis jelentősen befolyásolják egyéb tényezők, egy-egy kockázat értékelésénél az azzal kapcsolatban álló összes többit is figyelembe kell venni.

Ezért a gyakorlatban sokszor igen szubjektív módon, esetleg sehogyan sem történik meg a kockázatok értékelése, és így a fent említett folyamat középső szakasza egyszerűen kimarad. Ez azzal a veszéllyel jár, hogy a meghozott kockázatkezelési intézkedések nem a megfelelő módon, nem a legfontosabb területeket érintve, és nem az erőforrások ideális felhasználásával történik (Charette, 1996 és Ciechanowicz, 1997). A kockázatértékelés tehát ezen a problémán segíthet. A megfelelő kockázatértékeléshez azonban valamilyen megalapozott módszert kell használni, amennyiben az értékelés eredményeit hasznosítani kívánják.

Az információtechnológiai kockázatértékelésre nagyon sokféle megoldás létezik (Karabacaka – Sogukpinar, 2005). A kockázatok nagyságának, veszélyességének meghatározása azonban a legtöbb esetben valamilyen szubjektív szempontrendszer alkalmazásával történik (Dickie, 1997), hiszen nincsen olyan egységesen elfogadott, kalibrált mérési rendszer, amely a kockázatok értékelését pontosan lehetővé tenné. Ennek következtében az egyes mérési eredmények önmagukkal ugyan konzisztensek, az ellenőrzések közti összehasonlítás lehetősége – legyen az ugyanannál a vállalatnál, de más időben, vagy vállalatok között – azonban erősen kétséges. A mérés szubjektív volta miatt ugyanis nem lehetünk biztosak abban, hogy akár ugyanaz a mérés,

ugyanazon a területen ugyanazt az eredményt adja, amennyiben más a végrehajtó.

Ezért van szükség olyan tudományosan megalapozott módszerre, amellyel összehasonlítható eredmények állíthatók elő az IT audithoz kapcsolódó kockázatértékelések során. A kutatás célja egy ilyen módszer megalkotása, gyakorlati megvalósítása.

V.4. A kockázatértékelés módszerei

A kockázatértékelés nagy múltra visszatekintő és igen gazdag irodalommal rendelkező szakterület. A kockázatok felmérése, értékelése és kezelése az élet számos területén felmerülő mindennapos probléma. A kockázatok étékelése alighanem a folyamat leginkább problematikus területe. Vannak azonban területek, amelyeken jól bejáratott módszereket alkalmaznak a kockázatok értékelésére. Ilyen például a biztosítási iparág, amelyben az egyes káresemények súlyosságát és bekövetkezésük valószínűségét a biztosítók már a kezdetektől fogva beépítik termékeik árazásába. Az aktuárius szakma nagyrészt ezen kockázatok értékelésével foglalkozik.

Az információrendszerekkel kapcsolatos kockázatok értékelésére, mint korábban láthattuk, szintén számos eljárás létezik. Ezekben a kockázatokat elsősorban mint az információbiztonságot, illetve a számítógépes rendszerek működési biztonságát befolyásoló tényezőket kezelik.

Az információtechnológiai biztonsággal kapcsolatos kockázatelemző eljárások, módszerek és az ezekre támaszkodó alkalmazások javarésze az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézetének[26]először az 1970-es években publikált Szövetségi Információfeldolgozási Szabványok[27]31. és 65. részéből fejlődött ki (Ozier, 2003a). Azóta nagyon sokféle kockázatértékelési segédeszközt fejlesztettek ki. Ezek egy része, viszonylag egyszerű módon, ahhoz nyújt segítséget, hogy a felhasználó azonosítsa az eszközöket, és megítélje, hogy ezek milyen mértékben vannak

[26] Ez azonos a szabványokkal kapcsolatban már említett *NIST*-vel.
[27] *Federal Information Processing Standards Publications*

kitéve a különböző kockázati tényezők hatásának. Ezek a kockázati tényezők lehetnek természeti, illetve szándékos vagy véletlen humán eredetű kockázatok. Az összetettebb kockázatértékelő eszközök gyakorlatilag szakértő rendszernek tekinthetők, amelyek a kvalitatív jellemzőket kvantitatív tényezők formájában képezik le. Így például az eszközök, kockázatok vagy fenyegetettségek helyett azok pénzbeli értékével, illetve kockázati együtthatókkal dolgoznak.

Az így elkészített értékelések azonban rendkívül munkaigényesek, és ennek ellenére gyakran meglehetősen pontatlanok. A legkorábbi elemző eszközök például legtöbbször csak ±1 helyiérték pontosságúak voltak, és ezért gyakorlatilag használhatatlannak bizonyultak.[28]

V.5. Nehézségek a kockázatértékelési metrika megalkotásában

Az elméletek és a technológia fejlődésével a rendszerek finomodtak ugyan, számos probléma azonban továbbra is fennáll. Először is, a kvantitatív módszerek szinte mindegyike rendkívül munkaigényes, és alapvetően szakértői becsléseken alapul. Ez azt jelenti, hogy az auditor, vagy kockázatelemző személyes véleménye alapvetően befolyásolja, hogy egy-egy kockázati tényező milyen súlyosságúnak számít. Az erre épülő metrika pedig természetesen nem lehet objektív.

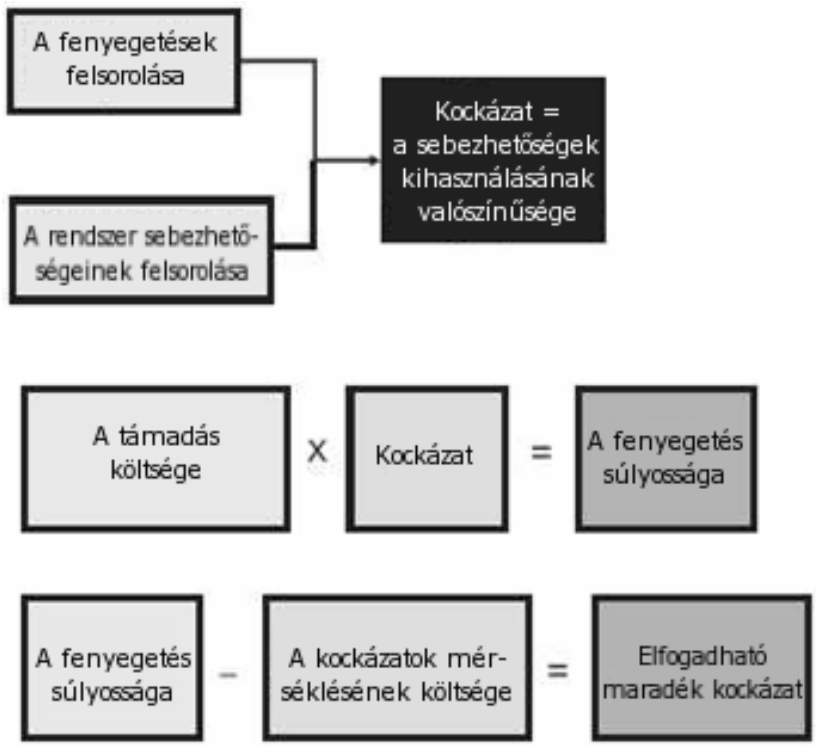
A másik hiányosság, hogy a kvantitatív módszerek nem is próbálkoznak azzal, hogy a nem szigorúan technikai jellegű kockázatokat értékeljék. Az eddig említett több tucatnyi kockázatértékelő rendszer mindegyikére jellemző ugyanis, hogy az információrendszerek veszélyeztetettsége felől közelít a kockázat kérdéséhez, és nem foglalkozik a szervezeti és menedzsment kérdésekkel, sőt általában a szoftverfejlesztési kockázatokra sem térnek ki (Wilson, 2005). Ez részben annak is tulajdonítható,

[28] Például egy kockázati esemény bekövetkezése utáni helyreállítás pénzben kifejezett értékét 100 eFt-ban határozza meg a rendszer, akkor csak abban lehettünk biztosak, hogy az valahol 10 eFt és 1MFt között lesz. Ez pedig nem igazán nagy segítség.

hogy, mint a szabványok áttekintéséből is kiderül, a legtöbb szabvány vagy követelményrendszer szintén nem foglalkozik ezekkel a kérdésekkel.

Komoly problémát jelent az is, hogy az értékelő rendszerek szinte mindegyike azt a megközelítést alkalmazza, amely szerint a kockázat nagysága két tényező: a bekövetkezés valószínűségének és a bekövetkezés hatásaként előálló kár mértékének valamilyen közös eredőjeként áll elő (8. ábra). Ez a megközelítés általában viszonylag egyszerű alkalmazásokat eredményez, hiszen egy egyszerű szorzással kaphatunk valamilyen értéket, amelyet egy-egy tényezőhöz rendelhetünk. A gyakorlatban azonban nagyon nehéz eldönteni, hogy melyik a nagyobb kockázat: egy kis valószínűséggel bekövetkező, de potenciálisan hatalmas kárt okozó, vagy egy nagy valószínűségű, de nem különösebben súlyos következményekkel járó tényező. Az ilyen típusú problémák esetében az erőforrások megfelelő allokációjában és a végrehajtandó lépések ütemezésében ezek a rendszerek nem sokat segítenek.

8. ábra



A hagyományos kockázatértékelés módja (Henning, 2005)

Szintén nehézséget jelent, hogy a kockázatértékelések jellemzően a kockázatokat egyenként értékelik, azaz a fent leírt módszerrel egyszerre csak egy tényezőt vizsgálnak, figyelmen kívül hagyva azt a tényt, hogy az egyes kockázati tényezők kölcsönös függőségben vannak egymással. Nyilvánvaló, hogy az információtechnológia világában gyakran előfordulhat olyan eset, hogy egy kockázat egészen eltérő mértéket mutat, amennyiben önmagában tekintjük, vagy ha más olyan összetevőkkel együtt, amelyek hatással lehetnek a vizsgált területre.[29] Az összetevők korrelációja azonban a legtöbb javasolt megoldás esetén nem megengedett (Lenstra – Voss, 2004).

A kutatás célja egy olyan metrika kialakítása, amely figyelembe veszi az információtechnológia szervezeti és vezetési kérdéseit is, és hosszútávon is alkalmazható, valamint alkalmas a különböző időpontok és különböző vállalatok közötti összehasonlítások megalapozására is. A fenti okok miatt ennek megvalósításához többtényezős döntési modellt kívánok felhasználni, amelynek segítségével a problémák jelentős része áthidalható.

V.6. Többtényezős döntési módszerek

Mint a fentiekben is láttuk, a kockázatértékelési metrika megalkotásával kapcsolatban számos probléma merül fel. Egyes szerzők ezek alapján arra a következtetésre jutnak, hogy bár nagyon hasznos lenne egyetlen metrika megalkotása, az a gyakorlatban kivitelezhetetlen, hiszen más dimenzióban mért értékek összehasonlítására lenne szükség, ami lehetetlen (Wikipedia, 2004). Ez a felfogás túlságosan ragaszkodik a kockázatértékelés hagyományos módszeréhez, azaz a bekövetkezési valószínűség és az esetlegesen okozott kár figyelembevételével kialakított kockázati együtthatókhoz. Valójában a helyzet még ennél is nehezebb, hiszen e szerint az elmélet szerint csak két változóval kell dolgozni, és nem számol a kockázati

[29] Például: a vállalati belső hálózaton lévő központi gép nincs megfelelően védve az illetéktelen használattól, ugyanakkor az alkalmazottaknak nincs meg a megfelelő tudásuk ennek kiaknázására. Ebben az esetben a betörés kockázata kicsi, ám ennek oka két olyan tényező együttes fennállása, amelyek önmagukban kockázatosnak ítélhetők: a védelem hiányossága és az alkalmazottak szakértelmének hiánya.

tényezők egymásra gyakorolt hatásával, amely számos – és feltehetőleg esetről esetre változó számú – kiegészítő változó figyelembevételét igényli.

Egy jól alkalmazható kockázati metrika megalkotásához tehát sok tényező együttes hatását kell figyelembe venni. A tényezők pedig nehezen összemérhető skálákon mértek. Az ilyen típusú problémák megoldásához nagy segítséget jelent az az eszközrendszer, amelyet a többtényezős döntési modellek jelentenek (Albrecht, 1987).

Ezen módszerek célja – mint az elnevezésből is kiderül – hogy több, nem összemérhető tényező együttes figyelembevételével segítsenek az összetett döntési feladatok megoldásában (Zeleny, 1982). Az eljárásokat, amelyekből közel tucatnyi ismeretes, elsősorban olyan jellegű döntési problémák megoldására hozták létre, amelyekben közszolgálati szervezetek döntéseit kellett megalapozni. Az 1970-es évektől kezdődően széles körben alkalmazzák őket, környezetvédelmi, gazdasági, beruházási és egyéb döntések alátámasztására.

V.6.1. A többtényezős döntési módszerek fajtái

A többtényezős módszereket több szempont szerint lehet csoportosítani, az egyik legismertebb osztályozást azonban Hwang és Yoon adja (Hwang – Yoon, 1995). E szerint az eljárások két nagy csoportra oszthatók. A többszempontú módszerek (MADM)[30] esetében több, előre meghatározott, általában korlátozott számú döntési lehetőséget ismerünk, amelyek értékelésében számos átváltásra van szükség az egyes jellemzőkön, attribútumokon belül és azok között. A többcélú módszerek (MODM)[31] esetében pedig folyamatos vagy egész skálán mért döntési változókkal meghatározott nagy- vagy végtelen számú lehetőség közül kell kiválasztani a döntéshozó célfüggvényének vagy preferenciáinak leginkább megfelelőt. A MADM módszerek azután használhatók arra is, hogy a többféle MODM módszerrel előállított lehetőség közötti választást alátámasszuk.

[30] *MADM – Multiple Attribute Decision Making*
[31] *MODM – Multiple Objective Decision Making*

Az első csoportba tartoznak a legismertebb módszerek. Ilyenek az elemi módszerek, mint a *lexikografikus* és a *maximin* módszer, a kritériumok szintézisén alapuló módszerek, mint a *TOPSIS*, az *UTA*, a *MAVT* és a két legelterjedtebb a *MAUT*[32], és az *AHP*. Szintén ide sorolhatóak a rangsoroláson alapuló módszerek, mint az *ELECTRE* a *PROMETHE,* a *NAIADE* (Schreck, 2002) és az *EXPROM*, továbbá az olyan vegyes eljárások, mint a *fuzzy konjunktív-diszjunktív* módszer, és a *Martel és Zaras* módszer (Seyhan, 1999).

A második csoport, tehát a MADM módszerek családja még összetettebb problémák megoldását célozza, amelyekben egyszerre több, egymással versengő cél megvalósulását kell értékelni a választási lehetőségek összemérése során. Az egyes tényezők súlyozása további igen komoly nehézségeket vet fel (Fan – Ma, 1999). A probléma igen komplexszé válik, és megoldásához lineáris illetve nemlineáris programozási módszerek alkalmazhatók. A jelen kutatás keretében ezek alkalmazására nincsen szükség, hiszen a kockázatértékelés során megfogalmazott cél – a kockázatok költséghatékony minimalizálása – ennél egyszerűbb és könnyebben kezelhető eszközökkel is megoldható.

Természetesen lehetőség van a többféle módszer együttes alkalmazására is, olyan módon, hogy az értékelés különböző fázisaiban a legmegfelelőbb eljárást használjuk (Brugha, 2004).

Jelen dolgozatban a két legismertebb eljárás bemutatása kapott helyet, abból a célból, hogy a kockázatértékelési metrikához való felhasználhatóságukat mérlegelhessük.

V.6.2. MAUT

A MAUT, azaz a többszempontú hasznossági elmélet valószínűleg a legelterjedtebb, a leginkább széleskörűen alkalmazott többtényezős döntési eljárás. A MAUT olyan strukturált módszertan, amelynek segítségével a több tényező közötti átváltások kezelhetővé válnak. Egyik első alkalmazása során a Mexikóváros új repülőterének elhelyezésével kapcsolatos lehetőségek közötti

[32] *MAUT – Multiple Attribute Utility Theory*

választásra használták az 1970-es években. A figyelembe vett tényezők között szerepelt a megépítés költsége, a kapacitás, a repülőtérre való kijutás időigénye, a biztonságosság, a társadalmi ellenállás és a zajszennyezés mértéke (HSOR, 2004).

A MAUT egy olyan normatív módszer, amely különböző egységek egymással versengő jellemzők alapján történő értékelését teszi lehetővé. A jellemzők közötti átváltást relatív fontossági súlyok határozzák meg, a jellemzők egységenkénti hasznosságát (a megelégedettséghez történő hozzájárulását) pedig skálázó függvényekkel lehet számszerűsíteni (Edwards – Newman, 1982). Végső lépésként valamilyen aggregáló függvény, jellemzően valamiféle additív függvény használható a különböző jellemzők értékeinek kombinálására (Schmitt – Dengler – Bauer, 2002).

A módszer működése nagyon hasonló az általános közgazdaságtanból ismert várható haszon elméletéhez. A hasznosság az adott eseménynek a személyes elégedettséghez való hozzájárulását mutatja meg, és n lehetséges kimenetel ($X_1,\ldots,X_n$) esetén a várható hasznosság:

$$EU = \sum_{i=1}^{n} p(X_i) \times U_i(X_i)$$

ahol $p(X_1),\ldots,p(X_n)$ az egyes kimenetelek bekövetkezési valószínűsége, $U_1,\ldots,U_n$ pedig az ezekhez tartozó hasznossági függvények.

A MAUT azonban nem valószínűségeket, hanem egymással versengő jellemzőkhöz rendelt fontossági súlyokat alkalmaz. A cél ugyanis nem a bizonytalan lehetőségek összemérése, hanem a különböző részfeladatoknak az egyes elemek osztályozásával történő értékelése. Ugyanazzal a képlettel találkozhatunk, mint a várható hasznosság elméleténél, itt azonban a hasznossági függvények az egyes jellemzők kívánatosságát fejezik ki. Egy n jellemzőjű eset teljes hasznosságát egy összegző függvény határozza meg:

$$U(X) = \sum_{i=1}^{n} w_i * u_i(x_i)\text{, ahol } \sum_{i=1}^{n} w_i = 1$$

amelyben x_i az i-edik jellemző értéke, w_i az i-edik jellemző többi jellemzőhöz viszonyított fontosságának súlya, és u_i az i-edik jellemzőhöz tartozó

hasznossági függvény (Schmitt – Dengler – Bauer, 2002). Ez a függvény tehát egy olyan súlyozási módszer, amellyel értékelhetjük az egyes jellemzők által a teljes hasznossághoz hozzáadott mértéket. A MAUT átalakításával természetesen elképzelhetőek olyan megoldások is, amelyben nem ezen a módon történik a súlyozás (Fagin – Wimmers, 1997).

A MAUT tehát – akár a többi döntési módszer – a különböző lehetőségek közötti választást hivatott elősegíteni. Ennek megvalósításához hasznosságokkal dolgozik, és végső célként a döntéshozó haszonmaximalizáló magatartásának megvalósítását segíti elő. Ráadásul történtek kísérletek arra is, hogy a MAUT használatához szükséges, és némileg nehézkesen megalkotható súlyokat (Borcherding – Eppel – Winterfeldt, 1991) a tényezők fontossági sorrendje, az értékelő preferenciái alapján lehessen előállítani (Bedford – Cooke, 1999), így segítve a gyakorlati alkalmazhatóságot. A kockázatértékelési metrika létrehozásához némileg eltérő megközelítés szükséges, ugyanakkor kétségtelen, hogy a MAUT által támogatott döntési eljárás és a MAUT módszer – bár némileg átalakított formában – nagyon jól felhasználható a vizsgált probléma megoldásában.

A MAUT-hoz igen hasonló módszer a MAVT, amely nem hasznosságokkal, hanem az egyes lehetőségekhez rendelt értékekkel dolgozik. Így némileg talán közelebb áll az itt vizsgált problémához, ugyanakkor a MAUT jóval szélesebb körben alkalmazott eljárás (Dyer et al., 1992), ezért a kutatás során hasznosabb lehet ennek felhasználása.

Az alkalmazhatósághoz arra van szükség, hogy a kockázati tényezőket mint a MAUT-ban megismert jellemzőket tekintsük. Ezek száma nagy, de az auditálási felfogás szerint korlátozott. Továbbá igaz, hogy egymással „versengő” jellemzőkről van szó, hiszen az értékelési probléma éppen ebből indul ki. Amennyiben azonban létrehozzuk az egyes kockázati tényezők egymáshoz viszonyított súlyait, az adott területre vonatkozó összesített kockázat ezek eredőjeként megkapható a megismert képlet – illetve annak kissé átalakított változata – alapján. Ebben valójában nem a hasznosság maximalizálása, hanem a kockázatok minimalizálása a cél, ugyanakkor a

MAUT apparátusa szinte kivétel nélkül alkalmazható. Természetesen a súlyok kialakításánál az egyes tényezők közötti összefüggéseket, hatásokat, ellenhatásokat, pozitív és negatív visszacsatolásokat is figyelembe kell venni. Ez igen komoly munkát igényel, ám nem megoldhatatlan feladat, és az interakciók figyelembevétele megtörténik a módszer kidolgozásakor.

Ezzel kapcsolatban felmerülhet, hogy a súlyok megállapítása alapvetően szubjektív ítéletekből áll, hiszen az egymással gyakran nehezen összemérhető kockázati tényezők értékeinek és kölcsönhatásainak megállapítása szakértői feladat, amely nem általánosítható. A súlyok megállapítása a bemutatott kutatási értelmezésben az auditor feladata. Ő dönti el az egyes felmérések során, hogy a kockázati tényezők egymáshoz viszonyított fontosságát hogyan értékeli. A tényezők közötti kölcsönhatásokat azonban általánosan meg lehet határozni. Ezt az értékelést, amennyiben az a megfelelő kockázat-felmérési – illetve általánosabban auditálási – módszertanra épül, elegendő egyszer, a metrika kalibrálásakor végrehajtani. A későbbiekben az így előállított viszonyrendszerek kiválóan alkalmazhatók a megismétlődő auditálások során, és az összehasonlíthatóság és megismételhetőség kritériumai teljesülnek.

V.6.3. AHP

Egy másik igen elterjedt módszer az AHP[33], tehát az analitikus hierarchia eljárás (Saaty, 1980 és 1989). Ebben a módszerben páronkénti összehasonlításokat, hierarchikus struktúrákat és a hányadosok mérését alkalmazzák a súlyok jellemzőkhöz rendelésének megoldására. A technika alkalmazása során a problémát célok, jellemzők és megoldási lehetőségek hierarchiájává bontják le. A kompozíciós eljárás additív technikán alapul, akárcsak a MAUT esetében. Egyik erőssége, hogy az értékelések tranzitivitásának biztosítása érdekében konzisztencia-ellenőrzés is részét képezi a módszernek. Számos területen alkalmazzák a döntés-előkészítés, döntéstámogatás során (Golden – Harker – Wasil, 1989), és jó néhány

[33] *AHP – Analytic Hierarchy Process*

döntéstámogatást segítő szoftverben is felhasználják (pl. HIPRE) (Saunders, 1994).

Az eljáráshoz a döntéshozónak meg kell határoznia minden egyes kritériumnak a többihez viszonyított relatív fontosságát, majd minden döntési lehetőségnél meg kell határoznia a kritériumokra vonatkozó preferenciáit. Az értékítéletekre alapozva numerikus értékek rendelhetők a fontosságokhoz egy 1-től 9-ig terjedő skálán, majd az értékítéletek szintéziséből előállítható az egyes döntési lehetőségek prioritási sorrendje.

Az AHP használatában nagy segítséget nyújt a grafikus ábrázolhatóság. A döntési problémához tartozó hierarchikus kapcsolatokat könnyen értelmezhető formában lehet elkészíteni (Forman, 1993). Az ábrák segítségével a célok, jellemzők és megoldási lehetőségek jól szemléltethetők, és jóval áttekinthetőbbé válnak a döntési folyamatok.

A vizsgált probléma, tehát az IT audit során szükséges kockázatértékelés támogatására, illetve megfelelő metrika előállítására az AHP módszer némileg nehezebben alkalmazható, mint a korábban ismertetett MAUT technika. A különböző lehetőségek közötti összehasonlítás, különösen a páronkénti összevetés meglehetősen nehezen kivitelezhető ebben az esetben. Az AHP a különböző döntési lehetőségek összehasonlítását teszi lehetővé, oly módon, amely a döntések meghozatalát segíti. Az auditálás, kockázatértékelés esetében azonban más típusú feladatról van szó, amelyben meglehetősen nehéz eldönteni, hogy egy-egy tényező, illetve egy-egy lehetőség közül melyik a kívánatosabb. Ennek során sok tényező együttes hatásainak vizsgálatáról van szó, és ebben a felhasználásban nem könnyű értelmezhető döntési lehetőségeket előállítani, amelyek páronkénti összehasonlításával el lehetne érni a kívánt célt. Ebből kifolyólag az AHP módszer meglátásunk szerint csak korlátozottan alkalmazható a kutatás céljának eléréséhez.

V.6.4. Egyéb módszerek

Természetesen az említetteken kívül sok más módszert is el lehet képzelni a kockázatértékelő rendszert megalapozó elméleti háttérként. A

sokváltozós környezetben történő elemzés, a sok egymással kölcsönös összefüggésben lévő változó összesítése, összehasonlításuk módja számos egyéb eljárás megszületését is indokolta[34]. Az egyik módszer, amely kifejezetten dinamikusan változó környezetben próbálja a különböző változók együttes és egyenkénti hatásait előállítani, valamint a rendszer egészére gyakorolt hatásokat felmérni, a rendszerdinamikai (SD[35]) megközelítés.

A Jay Forrester által már az 1960-as évek elején bemutatott SD felhasználása széles körben elterjedt, a gazdasági életben a nagyon nagy számú összefüggés ábrázolásához, és a lehetséges kimenetelek elemzéséhez számos területen alkalmazzák. Az információgazdálkodáshoz kapcsolódóan is történtek felhasználások, például az információs társadalom penetrációjának modellezésében (Sudár – Pető – Gábor, 2004). Sőt, a kockázatértékelés eszközeként is felmerült a használata (Saunders, 2002). Ez a megközelítés azonban elsősorban a technikai jellegű kockázatok egymásráhatásának feltérképezésére szolgál, és a jelen kutatás témáját képező átfogó auditálási munka esetében a vizsgált változók óriási száma feltehetőleg nagyon nehézkessé tenné annak használatát.

A lehetőségek áttekintése után a felhasználhatóságot szem előtt tartva történt a megfelelő módszer kiválasztása. A kutatásban az átalakított MAUT módszer használatára kerül sor, hiszen ennek segítségével a vizsgált kérdésekre választ kaphatunk, és a széles körben megalapozott módszer arra is biztosítékot nyújt, hogy az annak számos alkalmazása során nyert tapasztalatokat beépíthessük a készülő rendszerbe. A kutatás továbbvitele esetén, a későbbi fázisokban az értelmezésekhez és a további kalibráláshoz szükség lehet egyéb módszertanok bevonására is, ezt azonban a gondos előkészítés mellett is csak a későbbiekben lehet megállapítani, az itt bemutatott kutatási szakasz után.

[34] Vannak többek között olyan alkalmazások is, amelyekben a *Balanced Scorecard* technikát használják az auditálások osztályozási alapjaként (Schmidt, 2005), illetve *fuzzy logic* technnikákat (Smith – Eloff, 2002).
[35] *SD – System Dynamics*

VI. FEJEZET
A kutatási módszer

VI.1. Operacionalizálás

Az alábbiakban ismerhetjük meg, hogy a bemutatott hipotézisek milyen módon bonthatók le úgy, hogy azok ellenőrzése megtörténhessen, továbbá azt az eljárást, amelynek segítségével az igazolás elvégezhető. A jobb áttekinthetőség érdekében itt ismét szerepelnek a hipotézisek.

Hipotézis 1.: Létezik a vállalatok informatikai működésére vonatkozó olyan összesített kockázati mutatószám, amely az egyes kockázati területek közötti interakciókat is figyelembe veszi, és hitelesen orientál.

A hipotézis a kívánt mutatószám létrehozhatóságát, megalkothatóságát mondja ki. Az összesített mutatószám fogalma további magyarázatra nem szorul. Az egyes kockázati területek közötti interakciókat olyan módon lehet figyelembe venni, hogy megvizsgáljuk, több tényező együttes fennállása milyen módon befolyásolja a kockázati mutatószám értékét. Amint a későbbiekben bemutatjuk, egyelőre csak a tényezők közötti elsőrendű összefüggések vizsgálatára van mód. Bár ez kétségkívül fontos előrelépést jelent, világos, hogy – bár csökkenő mértékben – a többedrendű összefüggések is figyelmet érdemelnek. Ezek felmérését a kutatás továbbvitele esetén lehet kivitelezni.

A hiteles orientáció alatt azt értjük, hogy vizsgált területek kockázati szintje nem mond ellent sem a gyakorlati tapasztalatoknak, sem az ésszerűségnek. Tehát a mutató csak akkor jelez, ha valóban problémás egy terület. Ezért a vállalati menedzsment számára is használható, a döntések meghozatalához alkalmas segédeszköz áll elő. Ennek a feltevésnek az igazolása magának a mutatónak a konstrukciójával végezhető el. Amennyiben ugyanis a mutató matematikailag helyes, úgy világossá válik, hogy milyen módon reagál a kockázatokra. A későbbiekben a működés ellenőrzésére érzékenységvizsgálat is végezhető.

Az 1. hipotézis alátámasztását a mutató tényleges létrehozása, és a konstrukció áttekintése biztosíthatja.

Hipotézis 2.: Ha az informatikai auditálás végrehajtásának önreflexív jellegét explicit módon megfogalmazzuk, akkor az ebből származó eredményeket vissza lehet vezetni az audit terv javítására, pontosítására.

Önreflexivitáson az auditálás esetében azt értjük, hogy az auditálások módszertana nagyban függ az egyes területeken elvégzett ellenőrzések eredményétől. Valójában, mint azt korábban is említettük, a legelterjedtebb módszerek, útmutatások is a korábban összegyűjtött tapasztalatokon alapulnak. Ezért az auditálás területétől egyáltalán nem idegen ez a megközelítés. Amennyiben az így előálló eredményeket ténylegesen felhasználjuk, akkor pontosabb auditálási terveket lehet készíteni, azaz a vizsgálandó területek behatárolása precízebb lehet.

Ezen feltevés igazolása az auditálások eredményeinek beépítésével történhet. Az auditálások végrehajtását a kutatás során, a később részletezett okok miatt, szimulációs kísérlettel helyettesítjük. Így ellenőrizhetjük, hogy valóban hasznos-e az önreflexió felhasználása.

Hipotézis 3.: A kockázati tényezők együttes hatásainak figyelembevételével lehetővé válik olyan, az informatika funkcióival összefüggő stratégiai fontosságú területek azonosítása is, amelyek a hagyományos módszerekkel nem határozhatók meg.

Együttes hatások alatt az egyes kockázati tényezőknek a kölcsönhatások figyelembevételével meghatározott, a teljes kockázathoz való hozzájárulását értjük. A feltevés szerint, amennyiben így hozzuk létre a kockázati mutatószámot, akkor olyan területek is azonosíthatók, amelyek a vállalat informatikai stratégiája szempontjából fontosak, ugyanakkor az egyszerűbb módszerek nem alkalmasak a kimutatásukra. Ez elsősorban olyan területeken jelentkezhet, ahol az egyes kockázatok viszonylag alacsonyak, másokkal kombinálva azonban súlyosak lehetnek.

A feltevés igazolása szintén a szimulációk segítségével valósítható meg. Ezek alapján ugyanis megállapítható, hogy azokban az esetekben,

amelyekben más kockázati mutatószámok nem jeleznek, a kölcsönhatásokat is figyelembe vevő metrika – a körülményektől függően – magas kockázatra hívhatja fel a figyelmet.

A II.2. alfejezetben a hipotéziseken túlmutatóan bemutattunk néhány olyan elvárást is, amelyek a kockázatértékelési metrikához kapcsolódnak. Ezek elsősorban a kockázati mutatószám gyakorlati alkalmazhatóságára vonatkoznak. A kutatás során világossá vált, hogy a tényleges gyakorlati alkalmazáshoz még több feladatot is meg kell oldani. Ugyanakkor a már elkészült mutatószám felhasználása, illetve hasznosságának megítélése is fontos lehet. Így a későbbi kutatások irányát is meg lehet határozni, hiszen a vállalati informatikai felelősök elvárásait is be lehetne építeni a modellbe.

Az elvárások ellenőrzéséhez kiterjedt empirikus vizsgálatra lenne szükség. Az elvárások mindegyikének ellenőrzése a jelenlegi kutatásnak nem képezi részét, de a későbbi munkához, a kutatás folytatása esetén, hasznos információkat nyújthat.

A vizsgálatot az auditálást végző szakértőkkel, illetve vállalati IT-felelősökkel végrehajtott mélyinterjúk formájában lehet végrehajtani, annak tisztázásra, hogy hogyan látják a kockázatértékelési metrika használhatóságát munkájukban.

Amennyiben a meghozott döntések könnyebb számszerűsíthetőségére vonatkozó elvárás teljesül, a menedzsment döntései számonkérhetők lesznek, és egy-egy döntés meghozatalát alá lehet támasztani a döntés meghozatala előtti és utáni kockázati felmérés adatainak összevetésével.

Fontos elvárás a vállalati erőforrások elosztásának hatékonyságnövekedése is. A feltevést szintén a vállalati döntéshozók megkérdezésével lehet ellenőrizni. Így felmérhető hogy egy megfelelő értékelő rendszert tudnak-e használni, illetve hogy a döntések eredményeinek mérhetőségén keresztül elősegíti-e munkájukat egy kockázatértékelő rendszer. Erre szintén ki lehet térni az interjúk során.

VI.2. A kutatási módszerek leírása

VI.2.1. A kockázatértékelési metrika megvalósítása

A kutatás elsődleges célja egy, az információtechnológiai auditálás során alkalmazható, széles körben elterjedt módszertanon alapuló kockázatértékelési metrika megalkotása, és erre alapozva egy olyan számítógépes rendszer esetleges megvalósítása, amely a kockázatértékelési feladatokban segédkezve, támogatási feladatokat láthat el. A kutatás a megfelelő elméleti alapozás, és módszerek kiválasztása után elsősorban gyakorlati jellegű, hiszen a megfelelő háttérre támaszkodva létre kell hozni az értékelést szolgáló módszert, az erre alapozó skálarendszert, valamint azt a segédeszközt, amely megfelelő támogatást nyújt a felhasználáshoz.

A megvalósításhoz számos előfeltétel szükséges. Először meg kell alkotni a kockázatok valamilyen gyűjteményét, amely teljes körűnek tekinthető, és az értékelés alapját képezheti. Másodszor pedig létre kell hozni a megfelelő mérési, osztályozási módszert, azaz azt a metrikát, amellyel a különböző kockázati szintek értékelhetők, és egy-egy vizsgált területre összesíthetők. Majd lehetőség szerint a megalkotott metrikát, és az ez alapján létrehozott értékelési módszert vissza kell illeszteni az auditálási módszertanba, hogy a kapott értékeket annak eszköztárával lehessen a későbbiekben kezelni.

Mint a dolgozatból kiderül, számos eddigi eredmény jól alkalmazható a kutatás előkészítésében és kivitelezésében. Mivel a cél egy széles körben alkalmazható módszer megalkotása, ezért a kockázatok meghatározása is a lehető legszélesebb körben kell, hogy történjen. Ehhez olyan auditálási módszert érdemes választani, ami egyrészt valóban széleskörű, másrészt pedig eléggé részletes ahhoz, hogy a különböző kockázatok közvetlenül vagy közvetve előállíthatóak legyenek a felhasználásával.

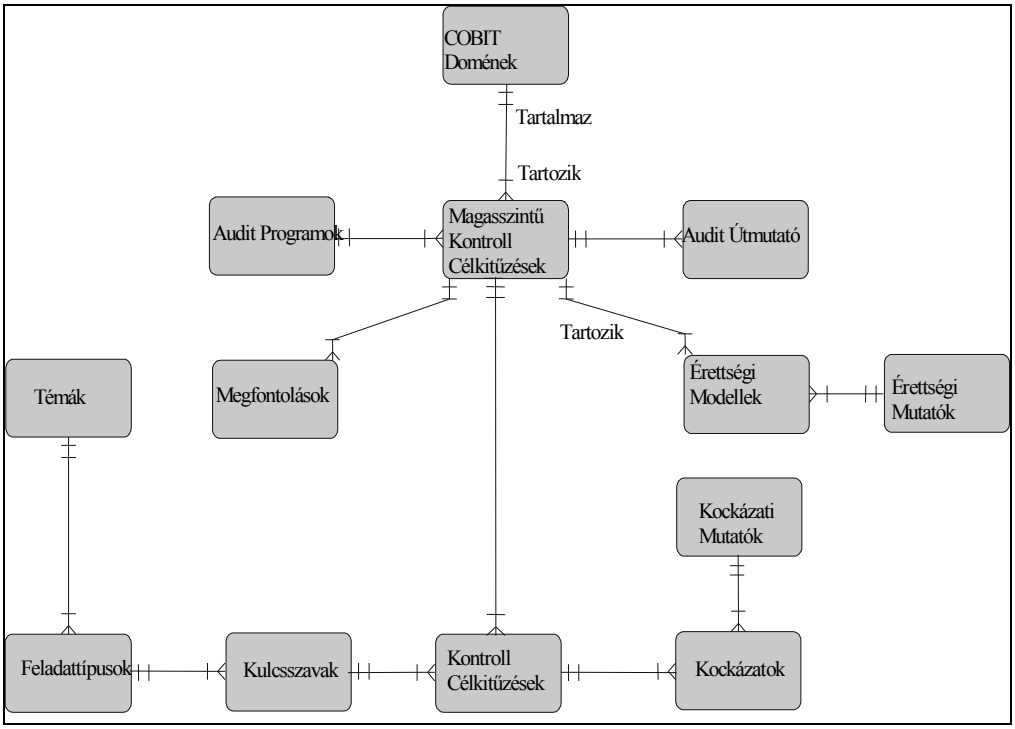
A gyakorlatban egyetlen olyan átfogó auditálási módszertan létezik, amely széles körben elfogadott, a lehető legtöbb területre kiterjed, ugyanakkor alkalmas a kockázatokig történő lebontásra. Mint a IV. fejezet áttekintő részéből is világossá válhatott, ez a COBIT. Bár az információk integritását

fenyegető tényezők teljességére vonatkozóan érték kritikák a COBIT-ot (Boritz, 2005), kétségtelenül ez a vizsgált területet legjobban fedő keretrendszer. A kutatás sikeressége érdekében tehát a kockázatértékelés alapjaként ezt a módszertant érdemes felhasználni.

A COBIT azonban nem tartalmaz olyan szintű lebontást, amely a kockázatok közvetlen vizsgálatát tenné lehetővé. Bár komoly segítséget nyújt a kockázatokra vonatkozó ellenőrző kérdések megalkotásához, maguknak a vizsgálandó kockázatoknak a kinyerése az előírásból munkát igényel. Egy már folyó kutatás során, amely a COBIT alapján egy intelligens, az auditálást segítő rendszer kialakítását célozza[36], a kockázatok is előtérbe kerültek. A projekt folyamán, annak érdekében, hogy az auditálási folyamat során érdemben felhasználható rendszert lehessen alkotni, feltétlenül szükséges a COBIT-ban csak áttételesen, a részletes kontroll célkitűzések szintjén szereplő kockázatok kibontása. A kockázatok előállítása a részletes kontroll célkitűzéseknek megfelelően történt. A COBIR-ban felhasznált adatok egy közös adatbázisban találhatók, amely felhasználható a jelen kutatás segédeszközeként is. Az adatbázis felépítésének áttekintő ábrája, adatmodellje az alábbi:

[36] A projekt címe: *COBIR – COB*IT-alapú interaktív audit és kontroll tevékenységet támogató *I*ntelligens *R*endszer

9. ábra



A COBIR adatmodell

Mint látható, a kockázatok részét képezik a kialakítandó adatbázis-struktúrának, így a jelen kutatáshoz fel lehet használni az ebből a projektből származó eredményeket.

A másik feladat magának a metrikának a megalkotása: Ehhez – mint láthattuk – elsősorban a többváltozós döntési modellek felhasználása lehet szükséges. A MAUT, illetve annak módosított változata alkalmas választásnak tűnik a megfelelő metrika létrehozásához.

A metrika működőképessé tételéhez szükség van a módszer kalibrálására is. Ez több mérési folyamat véghezvitelével, és az eredmények rögzítésével, összehasonlításával végezhető el. A mutató működése Monte Carlo szimulációval tesztelhető.

Végül a megalkotott metrikát, a felhasználhatóság érdekében vissza kell illeszteni a COBIT által garantált környezetbe. Ez szintén megoldható a COBIR projekt keretén belül, hiszen a jól működő szakértő rendszernek

szerves részét képezi a kockázatértékelési funkció. Így a megalkotandó rendszer tartalmazhatja majd jelen kutatás eredményeit is. Jelenleg a szoftveres támogatás nem része a kutatásnak, azt a vizsgálat továbbvitele esetén lehet megvalósítani.

VI.2.2. A metrika használhatóságának ellenőrzése

Amennyiben a kutatás tovább folytatható a jelenlegi eredmények elérése után is, a megalkotott kockázati metrika használhatóságát és gyakorlati előnyeit hagyományos vizsgálattal lehet ellenőrizni. Ehhez szükséges a szoftveres rendszer elkészítése. Amennyiben rendelkezésre áll a megfelelő metrika, empirikus vizsgálat keretében lehet felmérni, hogy az auditorok és vállalati felelősök milyen felhasználási módokat tartanak hasznosnak egy ilyen módszer esetében.

Bár a jelenlegi kutatásnak nem képezi részét, a későbbiekben felmerülhet, hogy a rendszer jobban igazodhatna a felhasználói igényekhez a lehetséges alkalmazók véleményének megismerésével. A felhasznált projektben is részt vettek auditálási szakértők, akik az elvárásokat közvetítették, így azokat részben már a jelenlegi kutatásban is figyelembe lehetett venni. Ugyanakkor a kockázatértékelési metrika önmagában nem befolyásolható a felhasználói igényektől függően, hiszen ez tudományos módszeren alapuló, elsősorban elméleti munkát jelent. A szakértő rendszerbe való illeszkedés természetesen lehet vizsgálni a későbbiekben.

A metrika felhasználási hatékonysága a felhasználók, azaz az auditálást végző szakemberek és az auditálást megrendelő nagyvállalatok informatikai kockázatok kezelésével megbízott vezetői körében végzett vizsgálatok segítségével ellenőrizhető a jövőben.

VII. FEJEZET
A kutatás végrehajtásának ismertetése

VII.1. Az *R* mutató kialakítása

A cél az volt, hogy elő lehessen állítani egy olyan módszert, amelynek segítségével határozottan megállapítható, hogy mekkora a vizsgált vállalatra vonatkozó kockázati érték; azaz egy olyan kockázati mérőszám kialakítása, amely az auditálás során összegyűjtött információk alapján egyértelműen meghatározza a kockázati szintet.

Ezen cél elérése érdekében a COBIT széles körben elterjedt szabályrendszere jelentette az alapot. A COBIT valójában a vállalatok által követendő gyakorlatok gyűjteménye az információtechnológiára vonatkozóan.

Felépítésében négy doménbe gyűjtve 34 kontroll célkitűzést tartalmaz, azaz olyan követendő eljárásokat, amelyek fontosak a vállalat információtechnológiai biztonsága és hatékony működése szempontjából. Ezek részletezéseként több mint 300 részletes kontroll célkitűzést említenek, amelyek a felsőbb szintű célok részletezését, pontosabb meghatározását szolgálják.[37]

Ezekből a részletes kontroll célkitűzésekből a vállalatot fenyegető kockázatok viszonylag egyszerű módon azonosíthatók. Ez az előző fejezetben bemutatott COBIR (COBIT alapú intelligens audit és kontroll tevékenységet támogató rendszer) fejlesztése során meg is történt.

A COBIT célkitűzése szerint a vállalati informatikával kapcsolatos valamennyi területre kiterjed, így az ebből előállított kockázati tényezők a lehető legteljesebbnek tekinthetők. Ezért a kutatás során a COBIT részletes kontroll célkitűzéseit vettük alapul a kockázatok számbevételéhez.

[37] 2005. 4. negyedévében jelent meg a COBIT 4. kiadása, amely a fentiektől némileg eltérő számú kontroll célkitűzést tartalmaz, és azok csoportosítása is kis mértékben változott. Ugyanakkor az új változat valójában a korábbi – és általunk is használt – 3.2-es verzió továbbfejlesztése. Az újfajta csoportosítás az értékelésben könnyen érvényesíthető.

A COBIT a kontroll célkitűzések értékelését csak oly módon teszi lehetővé, hogy a képesség-érettségi modell alapján az adott területhez egy 1-5 közötti (illetve 0 a nem értékelhető esetekben) mérőszámot rendelhetünk. Ez azonban csupán egy ordinális skálán mért változó, amelyből átlagot számítani illetve más statisztikai műveleteket végezni nem célszerű. Emiatt, és az egyszerű kezelhetőség érdekében ezeket az értékeléseket olyan módon lehet figyelembe venni, hogy a vállalat (vagy annak adott területe) informatikai kockázatát a kontroll célkitűzéshez tartozó kockázat növeli-e vagy csökkenti.

A kockázatértékelési módszer lényege tehát a következő: az auditor a vizsgálat alá vont területre vonatkozóan az egyes tényezőkre megállapítja a képesség-érettségi mutatószámokat.[38] Erre támaszkodva eldönthető, hogy az adott tényező a kockázatot növeli vagy csökkenti. Alapállapotban az elfogadási küszöb, tehát a választóvonal a növelő és csökkentő értékek között a 2,5, ez azonban csak paraméterként szerepel a modellben, tehát később változtatható. Az adatok alapján valamilyen algoritmus szerint (részletesen lásd lejjebb) megállapítható a vizsgált terület kockázata.

A legegyszerűbb algoritmus az egyszerű számtani átlag számítása. Ebben az esetben egyszerűen összeadjuk a +1 és -1 értékeket, amelyek a kockázathoz való hozzájárulást mutatják. Ez a módszer nyilvánvalóan nem képes kifinomult adatokat szolgáltatni, a gyakorlatban használhatatlan, hiszen nem állíthatjuk, hogy az egyes tényezők fontossága azonos. Ennek az egyszerű módszernek a használatával nem lehet elkerülni, hogy olyan kockázati tényezők is kioltsák egymást, amelyek a valóságban nyilvánvalóan eltérő súlyosságúak. Egy ilyen módszer segítségével nem lehet megállapítani, hogy mely területekre érdemes koncentrálni az erőforrásokat, hiszen minden probléma ugyanakkorának látszik.

Ebből kifolyólag feltétlenül szükség van fontossági súlyok bevezetésére is. Ezzel a módszerrel, amely természetesen az elterjedt kockázatértékelési eszközökben is megjelenik, lehetőség van arra, hogy az auditor mérlegelje az egyes tényezők fontosságát a vizsgált esetben. A súlyok hozzárendeléséhez

[38] Ilyen megoldáson alapuló metrika megalkotására már történtek kísérletek (Jelen, 2000).

többféle módszer is kínálkozik (Hwang – Shin – Han, 2004), az ezek közötti választás nem képezi részét a jelen kutatásnak.

A módszer alkalmazásához az auditálást végző személytől megfelelő fontossági súlyok megállapítását is el kell várnunk, és súlyozott átlagot állíthatunk elő. A kutatás során ezen súlyok megállapítása támaszkodhat a létrehozott forgatókönyvekre. A vizsgálat alatt ugyanis előállítottunk olyan halmazokat, amelyek egy-egy területre (pl. bankszektor, termelő vállalat stb.) megállapítják a vizsgálandó területeket. Ezekben az esetekben az egyes területek súlya is eltérő lesz.

VII.1.1. Az interakciók feltérképezése

Az eddigiekben vázolt súlyozás önmagában nem old meg egy másik fontos problémát: a kockázati tényezők egymásrahatását. A kutatás során azt a következtetést sikerült levonni, hogy a kockázatok értékelését nagyban lehet pontosítani, amennyiben a tényezőket nem tekintjük egymástól függetlennek, hanem figyelembe vesszük azok interakcióját is.

Ennek érdekében fel kellett térképezni, hogy két-két tényező milyen hatással van az általános kockázatra. Így például meg lehetett állapítani, hogy amennyiben az informatika stratégiai terv minősége a kockázatot növelő tényező, ugyanakkor a személyzet képzettsége a kockázatot csökkenti, akkor ezen két tényező együttesen hogyan befolyásolja a kockázati mérőszám alakulását. Ezt természetesen nem lehetett minden kétséget kizáróan megtenni. Mivel erre vonatkozó adatok nem léteznek, alapvetően szakértői becslésekre kellett hagyatkozni. Ugyanakkor ez nem áll ellentétben a COBIT szemléletével, hiszen ez egy empirikus tudásgyűjtemény, tehát az egyes pontjai sem megkérdőjelezhetetlenek.

A részletekbe menő feltáró munka eredményeként előállt egy interakciós mátrix, amely tartalmazza ezeket az együttes hatásokat (lásd az ábrát és a függelék IX.1. pontját).

10. ábra

domain_id	id	PO		PO		PO		PO		PO		PO		PO		PO		PO		PO		AI		AI		AI		AI		AI		AI		DS	
		1		2		3		4		5		6		7		8		9		10		11		1		2		3		4		5		6		1	
PO	1			1	-1	1	0	1	1	-1	1	1	1	1	1	1	0	1	-1	1	-1	1	1	1	0	1	-1	1	-1	1	-1	1	1	1	-1	1	0
				1	-1	1	-1	1	-1	1	-1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	0	-1	1	-1	1	-1	1	-1	-1	-1	1	-1	0	-1
PO	2					1	1	1	0	1	1	1	-1	1	-1	1	0	1	-1	1	1	1	-1	1	1	1	-1	1	-1	1	1	1	-1	1	0	1	1
						-1	-1	0	-1	-1	-1	-1	-1	0	-1	-1	-1	0	-1	-1	-1	0	-1	0	-1	1	-1	0	-1	-1	-1	1	-1	-1	-1	-1	-1
PO	3							1	-1	1	1	1	0	1	0	1	-1	1	-1	1	0	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	0	1	0
								1	-1	-1	-1	0	-1	0	-1	1	-1	1	-1	0	-1	0	-1	1	-1	1	-1	1	-1	0	-1	1	-1	0	-1	1	-1
PO	4									1	1	1	0	1	0	1	0	1	-1	1	0	1	0	1	0	1	-1	1	-1	1	0	1	1	1	1		
										-1	-1	-1	-1	-1	-1	-1	-1	1	-1	0	-1	0	-1	1	-1	1	-1	0	-1	0	-1	-1	-1	-1	-1	-1	-1
PO	5											1	-1	1	-1	1	0	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	0	1	-1	1	1	1	-1
												1	-1	0	-1	0	-1	1	-1	1	-1	1	-1	0	-1	1	-1	1	-1	0	-1	1	-1	-1	-1	0	-1
PO	6													1	-1	1	-1	1	-1	1	0	1	-1	1	-1	1	-1	1	-1	1	0	1	-1	1	-1	1	1
														-1	-1	1	-1	1	-1	-1	-1	-1	-1	1	-1	1	-1	1	-1	-1	-1	-1	-1	-1	-1	-1	-1
PO	7															1	0	1	-1	1	0	1	0	1	-1	1	0	1	0	1	1	1	-1	1	1	1	0
																-1	-1	1	-1	-1	-1	0	-1	0	-1	-1	0	-1	-1	-1	0	-1	-1	-1	0	-1	-1
PO	8																	1	-1	1	-1	1	-1	1	-1	1	-1	1	0	1	0	1	-1	1	1	1	1
																		1	-1	0	-1	1	-1	1	-1	1	-1	0	-1	-1	-1	0	-1	0	-1	0	-1
PO	9																			1	1	1	1	1	0	1	0	1	1	1	0	1	0	1	1	1	1
																				-1	-1	-1	-1	-1	-1	0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
PO	10																					1	-1	1	-1	1	-1	1	-1	1	0	1	-1	1	1	1	1
																						0	-1	0	-1	1	-1	0	-1	0	-1	1	-1	-1	-1	0	-1
PO	11																							1	0	1	-1	1	-1	1	1	1	-1	1	1	1	-1
																								-1	-1	1	-1	1	-1	-1	-1	1	-1	-1	-1	1	-1
AI	1																									1	0	1	-1	1	-1	1	-1	1	1	1	1
																										0	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

Az interakciós mátrix részlete

Ezek alapján az értékelési eljárás továbbfejleszthető volt. A kockázati mutató megállapítása úgy történik, hogy az auditor által meghatározott képesség-érettségi mutatószámokat és kockázati súlyokat vesszük figyelembe a mátrix egyes elemeinek kiválasztásakor, és az így kapott eredményeket összegezzük. Az egyes négyzetek tartalmának jelentése a következő ábra alapján érthető meg.

11. ábra

		AI 1	
		+	-
PO 4	+	1	0
	-	1	-1

Az interakciós mátrix mezőinek jelentése

A bal felső mező azt az értéket mutatja, amelyet akkor kap a fő kockázati mutató, ha mindkét vizsgált tényező pozitívan teljesít – ebben az esetben a kockázatot csökkentik. A jobb felső mezőben az oldalt feltüntetett tényező pozitív, a fent látható pedig negatív. A többi mező pedig szintén az ábrának megfelelően került feltöltésre.

VII.1.2. A mutató algoritmusa

Az ismertetett módszerrel olyan mérőszámot tudunk előállítani, ami meglehetősen jól tükrözi a vizsgált terület kockázatát. Az összesítés a következő képlet alapján történhet:

$$R = \sum_{i=1}^{n} w_i \frac{r_i + \sum_{j=1}^{n} r_{i,j}}{n}, \text{ ahol } \sum_{i=1}^{n} w_i = 1$$

Amelyben R a teljes kockázat mutatószáma, w_i az egyes kockázati tényezők súlya, r_i a kockázati mutató konvertált értéke (-1 vagy +1) és $r_{i,j}$ a kockázati tényezők elsőrendű interakciójából a fenti mátrix alapján előálló érték (+1, 0 vagy -1).

A képlet tehát az együtthatásokat is figyelembevevő kockázati mutatók súlyozott számtani átlagát állítja elő. Külön kiemelt az r_i érték, amely az adott kockázati tényező hozzájárulását jelenti a teljes kockázathoz. Valójában az *i*-edik tényezőnek saját magával való együtthatását értjük alatta, ez pedig a saját kockázati érték.

Könnyen felismerhető, hogy a kialakított algoritmus valójában a MAUT mutatószámának átalakítását jelenti. Amint azt korábban is láthattuk, ez a fajta megközelítés nem idegen a kockázatértékeléstől, és előnyös, hogy a korábbi kutatási eredményekkel összhangban lévő mutatót sikerült előállítani.

Az eljárás előnye, hogy a mutató értéke könnyen kiszámítható az egyes részterületekre is, így például a teljes kockázatnak néhány kontroll célkitűzésből álló részhalmazára is. A teljes mutató pedig ezeknek a részértékeknek az egyszerű összegzésével áll elő.

Amennyiben az auditor nehézkesnek találja, hogy 1 összegű súlyokat kell hozzárendelnie az egyes területekhez, a transzformáció természetesen könnyedén elvégezhető. Gyakorlatilag bármilyen súlyozás használható, ha az egyes súlyokat elosztjuk a súlyok összegével.

Felmerülhet, hogy az összegzés során valójában minden kockázati interakciót kétszer veszünk figyelembe, ugyanakkor ezt a jelenséget a súlyozással kivédjük. Ilyen módon az értékek az anyatényezők kockázati súlyainak megfelelően vehetők figyelembe, és az összegzés során a kockázati tényezők (kontroll célkitűzések) súlyait használjuk.

A mutató előállítása és a további munkálatok során a Microsoft Excel táblázatkezelő szoftvert használtam. A kutatás során világossá vált, hogy ennek a szoftvernek a képességei elegendőek a felhasznált adatmennyiség kezelésére, és alkalmas azoknak a műveleteknek az elvégzésére, amelyeket az elemzésben fel kívántam használni.

VII.2. A szimulációs kísérlet

A korábban említett okok miatt a kutatás során Monte Carlo szimulációt alkalmaztunk. A szimuláció és az eredmények előállítása több lépésben történt.

I. Először 4 különböző forgatókönyv kialakítására került sor, amely egy-egy auditálási helyzetet képez le. Így egy banki, egy termelő, egy szolgáltató és egy szoftverfejlesztő vállalatnál végzett vizsgálat megmintázására nyílt lehetőség oly módon, hogy a gyakorlati tapasztalatokra alapozva azonosítani lehetett azokat a részletes kontroll célkitűzéseket, amelyeket ezekben az esetekben vizsgálni szükséges. (A forgatókönyvekhez tartozó részletes kontroll célkitűzéseket lásd a függelék IX.2. pontjában.)

    1. Az 1. forgatókönyv szerint egy pénzintézet informatikai auditálásra kerül sor. A vizsgálat célja a banki adatkezelés, az adatkezelő rendszerek, az informatikai rendszerek biztonsága és a hozzáférések ellenőrzése. Egy ilyen fajta auditálás során természetesen nagyobb figyelmet szentelnek a technikai, technológiai jellegű kérdéseknek. A tervezés területéről elsősorban az üzem- és adatbiztonság területei lesznek fontosak.

2. A 2. forgatókönyvben egy termelő vállalat vizsgálatának terve szerepel. Az informatikához kapcsolódó területek közül elsősorban az üzletkritikus alkalmazásokkal és berendezésekkel kapcsolatos szabályozások ellenőrzése a cél. A legtöbb termelő vállalat számára az a legfontosabb, hogy a vásárlói igényeket magas szinten tudja kielégíteni, ehhez pedig elengedhetetlen a számítógépes rendszerek zavartalan működése.
3. Ez az auditálási tervminta egy szolgáltató vállalat ellenőrzésének céljából jött létre. Az elsődleges szempont a folyamatos működés fenntartása. Ezért a részletes kontroll célkitűzések közül azokat érdemes vizsgálni, amelyek az informatikai megoldások minél inkább problémamentes működtetését teszik lehetővé. Természetesen ezeknek a szempontoknak már a tervezési szakaszban is meg kell jelenniük, hiszen az eredményes kockázatkezeléshez a vállalati folyamatok teljességét szükséges ellenőrizni.
4. A 4. forgatókönyv pedig egy szoftverfejlesztő cégnél elvégzendő ellenőrzési feladatok leképezését jelenti. Egy ilyen szervezetben a legfontosabb tényezők a fejlesztési projektek hatékonysága és a külső előírásoknak és elvárásoknak való megfelelés. Éppen ezért az auditálási terv vázlatának megalkotásakor kitüntetett szerepe van a tervezési- és projektfeladatoknak, valamint a monitoring követelményeknek.

A forgatókönyvek megalkotása azért jelentős a kutatási cél szempontjából, mert így az egyes kockázatértékelési módszerek között különbséget tehetünk abból a szempontból is, hogy különböző ellenőrzési helyzetekben mennyire jól használhatóak. A szcenáriók segítségével megfigyelhetővé válnak az egyes területekre jellemző további sajátosságok is.

II. Ezek után 500 darab véletlen minta előállítására került sor, az auditálás során előálló képesség-érettségi értékek reprezentálására. A korábbi tapasztalatok és a vonatkozó szakirodalom alapján a véletlenszámok generálásakor az értékek egyenletes eloszlása volt a feltételezés, azaz ugyanakkorra az esély bármely értékelési fokozatra (a 0-tól 5-ig terjedő skálán). Természetesen a további kutatások során lehetőség van az eloszlás megváltoztatására és a további elemzésre.

A véletlenszámok generálása a forgatókönyvek számára is megtörtént. Az összehasonlíthatóság érdekében ugyanazok az esetek kerültek felhasználásra, tehát a forgatókönyveknél az 500 eset mindegyike a kontroll célkitűzések teljes körére megállapított véletlen értékek egy szűkített halmaza.

III. A továbbiakban az értékeléseket +1 és -1 értékekké konvertáltuk, ahol a +1 értékek a biztonság növekedését, a -1 értékek pedig annak csökkenését, tehát a kockázatok növekedését takarják. Erre a transzformációra két ok is volt: egyrészt az ordinális skálán mért érettségi értékek közvetlenül nyilvánvalóan nem használhatóak számszerű eredmények – például átlagok – számítására; másrészt a koncepció is az volt, hogy a kockázatokat növelő, illetve a kockázatokat csökkentő tételekre kell bontani a faktorokat. Így a kiválasztott elfogadási küszöbtől függően két részre oszlik a szimulált adatok halmaza.

Ez a küszöb a kísérletben 2,5, amely az értéktartomány közepén helyezkedik el. Mivel ez az érték szintén csak paraméterként szerepel a modellben, a későbbi kutatások során esetleg megváltoztatható. A vizsgálat során azért ez az érték lett a választóvonal, mert az egyenletes eloszlású bemeneti változókat e mentén lehetett két egyenlő részre osztani. Ugyanakkor, amennyiben változtatunk az eloszláson, szükséges lehet az elfogadási küszöb eltolása is. Ez már csak azért is megfontolandó, mivel a 0 érték a képesség-érettségi modellben kitüntetett szerepet kap, a nem létező eljárás jelölésére szolgál.

IV. A következő lépés az így előállított és transzformált értékekből a kockázati mutatószámok előállítása. Ehhez, a képesség-érettségi mutatószámokhoz hasonlóan egyenletes eloszlású súlyokat kellett rendelni, amelyek összege 1. Minden esethez külön súlyok tartoznak, tehát 500 különböző súlykészlet kerül alkalmazásra.

A kutatás során négy különböző mutató előállítása történt meg:

1. A számtani átlag számításánál egyszerűen a +1 és -1 értékeket átlagoltuk esetenként.
2. A súlyozott átlag számításánál a kontroll célkitűzésekhez rendelt +1 és -1 értékeket az előállított súlyok figyelembevételével átlagolhatók.
3. Az interakciók figyelembevételével megállapított mutató esetében a kölcsönhatási mátrix megfelelő elemeit (tehát a kontroll célkitűzésekhez rendelt +1, -1 értékeknek megfelelő metszéspontok tartalmát) átlagolandók.
4. Végül a kutatás célját jelentő *R* mutató előállítása történt meg, amely az interakciók figyelembevételével, és az egyes kontroll célkitűzések eltérő súlyozásával áll elő.

A kockázati mutatószámok kiszámítása megtörtént minden egyes esetre az 500 elemű mintában a kontroll célkitűzések – tehát a kockázati tényezők – teljességére, illetve az egyes forgatókönyvekre vonatkozóan is. Ilyen módon 500*5*4 = 10000 mutatószámot jött létre.

V. Az utolsó lépésben a kockázati tényezők egészére illetve az egyes forgatókönyvekre vonatkozó összesített kockázati mutatószámok sokaságára vonatkozó statisztikákat készítettem el. Ezek segítségével egyrészt lehetőség adódott az egyes értékelési módszerek összehasonlítására alapvető tulajdonságaik szempontjából, illetve lehetővé vált a vizsgált hipotézisek ellenőrzése is. Ezeket a mutatókat az SPSS statisztikai szoftverrel lehetett előállítani. Az elemzésekhez

komoly segítséget nyújtanak az egyes mutatók viselkedését tovább árnyaló hisztogramok is.

VII.3. Eredmények

A szimulációs kísérlet eredményei az alábbiakban foglalhatók össze. (Az eredmények alátámasztására lásd a részletes statisztikai adatokat és ábrákat a függelékben.)

I. Elsőként leginkább az szembetűnő, hogy az interakciók figyelembevételével elkészített mutatók esetében az átlagos értékek (a változó várható értéke) eltolódnak a negatív irányba. Ez azt jelenti, hogy az általunk javasolt mutatószám alkalmazásával a vizsgált szervezetek kockázatai nagyobbnak tűnhetnek, mint az egyszerű átlagolás esetében. A negatív irányba tolódás ugyanis azt jelenti, hogy a biztonsági mutató értéke alacsonyabb. Ez természetes, és valójában az auditálások során követendő egyik alapelvet, az óvatosság elvét tükrözi. Azokban az esetekben ugyanis, amelyekben nehezen eldönthető, hogy az interakciók eredménye milyen módon befolyásolja a végeredményt, a biztonság kedvéért inkább a negatív értékeket részesítettük előnyben. Ez kiderült az interakciós mátrix elemeinek összegzéséből is, mivel ennek eredménye negatív.

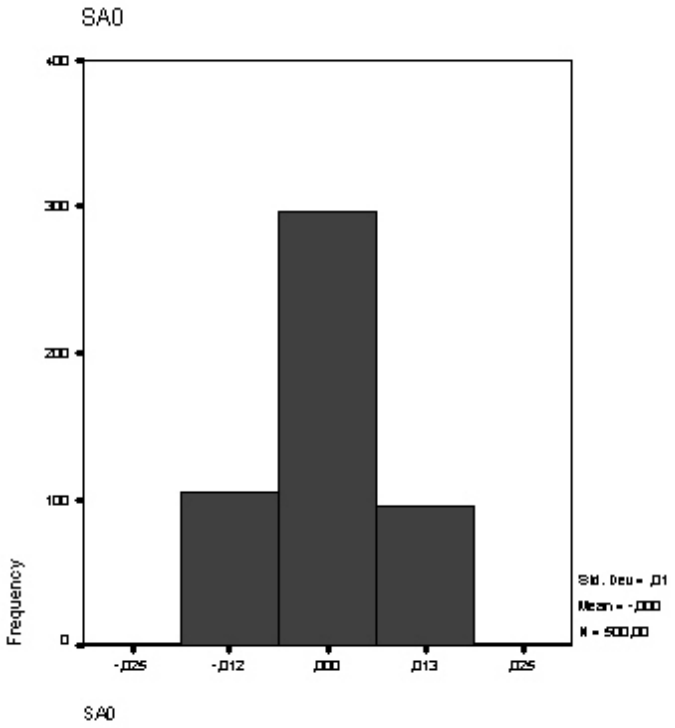
II. Az interakciók figyelembevételével meghatározott mutatók szórása némileg magasabb, mint az egyszerű átlagolással előállított esetekben. Az elsőrendű interakciókkal bővített mátrix alapján számított szórásnak az alapesethez viszonyított szórástöbblete a kockázatok együttes bekövetkezéséből adódik. A kutatásban csak az elsőrendű kapcsolatok tételes vizsgálatára nyílt lehetőség. A többedrendű interakciókból származó szórásnövekedést is lehetne tételesen vizsgálni, ez azonban jelen kutatás keretei között nem megvalósítható. Ezért kellett Monte Carlo szimulációt alkalmazni, amellyel a többedrendű kölcsönhatások, azaz minden egyéb közvetett hatás becslésére is lehetőség nyílik.

A kockázatok mérséklése szempontjából megfogalmazható üzemeltetési stratégia, illetve az informatikai funkció célkitűzése arra épülhet, hogy az így felderített szórástöbbletet igyekezzünk csökkenteni. A dolgozatban bemutatott módszer jelentősége, hogy az explicit módon megfogalmazható primer kockázatok mellet alkalmas olyan stratégiai súlypontok azonosítására is, amelyek felfedezésére másképpen nincs lehetőség.

III. A szimuláció eredményeit vizsgálva megállapíthatjuk, hogy a kockázati tényezők együttes hatását is figyelembe vevő mutatószám előjele az egyszerű számtani átlagtól csak ritkán – 0-hoz közeli értékek esetén – tér el. Ugyanakkor a mutatott kockázat nagysága, az esettől függően jelentős mértékben is eltérhet. Ennek köszönhetően ez a módszer alkalmas arra, hogy a kirívó esetekre felhívja a figyelmet, és olyan módon orientáljon a vizsgálatok során, hogy a különböző kockázati tényezők együttes hatását is felmérjük.

IV. Míg az interakciók figyelembevétele nélkül készült mutatók esetében a súlyozás használata csökkenti a mutatók szóródását, a kölcsönhatásokat is számbavevő mutatók esetében a szórás általánosságban növekszik. Ez a módszer alkalmas arra, hogy az átlagostól eltérő eseteket még inkább hangsúlyozza, és rejtett összefüggésekre hívja fel a figyelmet (lásd az eloszlási diagramokat). Áttételesen azt bizonyítja, hogy van a rejtett összefüggések aktív kezelésére, artikulálására alkalmas eljárás. A súlyozás azt is kifejezi, hogy egy adott időpontban, egy adott rendszerben milyen tényezőket tekintünk viszonylag fontosnak, veszélyesebbnek.

12. ábra

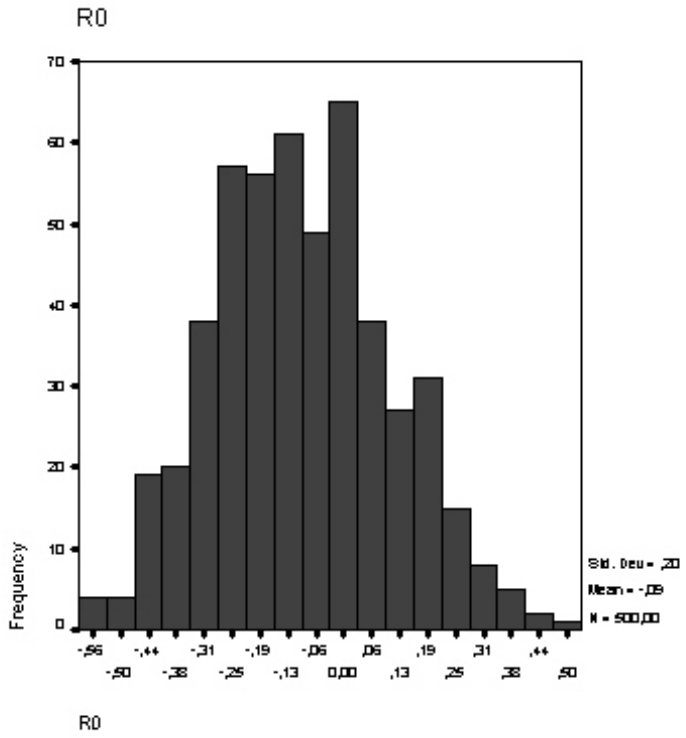


Súlyozott számtani átlagok eloszlása az összes kontroll célkitűzést tartalmazó mintára

V. A tartomány – a minimum és maximum értékek különbsége – nem változik, vagy nő az interakciók beiktatásával. (Szintén leolvasható a hisztogramokból.) Ebből következően a javasolt módszer lehetőséget teremt arra, hogy az átlagos értékektől való eltérésre jobban felhívjuk a figyelmet.

VI. A kockázatok súlyozásának hatása kisebb, mint az interakciók figyelembevételének. Tehát a súlyozott - nem súlyozott esetek között kisebb az összegbeli különbség, mint amekkora az interakciók figyelembevételének hatása jelent. Ez még inkább alátámasztja a II. pontban ismertetett állítást.

13. ábra



Az *R* mutató eloszlása az összes kontroll célkitűzést tartalmazó mintára

VII. A javasolt kockázati mutatószám és az egyszerűbb eljárások összevetéséből kitűnik, hogy az interakciókat is figyelembevevő mutató általában jobban különbözik a számtani átlagoktól a szcenáriók esetében, mint az összes kontroll célkitűzés vizsgálatakor. Ez azt bizonyítja, hogy ha kevesebb információval rendelkezünk a vizsgált területről, akkor egy ilyen mutatónak még nagyobb a jelentősége a helyes mérték megállapításában. A forgatókönyvek esetében az egyes kockázatok kivédése kevésbé fontos, mint az együtthatásuk figyelembevétele. A kutatás eredményeként javasolt mutatóval jobban kimutathatók azok a kritikus együttállások, amelyek a vállalati össz-kockázatot befolyásolják.

VIII. A mutatók konstrukciójából fakadóan az extrém esetekben (pl. csak a kockázatot növelő vagy csökkentő tényezők) nincs különbség az

értékek között, ugyanakkor a köztes esetekben, amelyek a gyakorlati életben előfordulnak, komoly eltolódás figyelhető meg.

VII.4. A hipotézisek igazolása

1. A példákból is látszik, hogy az interakciók figyelembevételével a fenti módon létrehozott mutatószám alkalmas a kockázatok értékelésére, és a „politraumás" területek azonosítására. A mutatószám használatával lehetőség nyílik az informatikai biztonsággal kapcsolatos erőforrások megfelelő allokációjára is. Mivel sikerült a feltételeknek eleget tevő kockázati mutatószámot – metrikát – előállítani, az 1. hipotézist igazolva látjuk. **Az 1. hipotézis elfogadható.**

2. A 2. hipotézis a gyakorlatban azt jelenti, hogy amennyiben elfogadjuk azt a tényt, hogy az auditálási módszertanok elsősorban gyakorlati tapasztalatokon alapulnak, akkor a korábbi auditálások során összegyűjtött információk segítségével jobb és pontosabb auditálási terveket lehet készíteni. Más megfogalmazásban: az egyes vizsgálati helyzetekben a kontroll célkitűzések kijelölése megtörténhet a korábbi auditálások tapasztalataira támaszkodva. Ráadásként az ilyen módon kialakított auditálási tervek az ellenőrzések költséghatékony végrehajtását teszik lehetővé, a pontosság és megbízhatóság feladása nélkül. A vizsgálat eredményei azt igazolják, hogy a fent említett módszerrel előállított mutató valóban alkalmas a kockázat megfelelő mérésére. Az 1. hipotézis elfogadásából következően a 2. hipotézis is elfogadható, hiszen az interakciók figyelembevételével sikerült egy kockázati mutatót létrehoznunk, és így az auditálás önreflexív voltát felhasználni az auditálási terv megalkotásához. **A 2. hipotézist elfogadtuk.**

3. A 3. hipotézis elfogadásával kapcsolatban az eredmények II. és VI. pontjában ismertetett megállapítások alapján lehet dönteni. Amint az a kutatás során világossá vált, a kockázati tényezők együttes hatásait is figyelembe vevő mutató esetében megjelennek olyan szórás-többletek,

amelyek a többedrendű interakciók következményei. Ezen összefüggések alapján megállapítható, hogy mely, korábban nem azonosított stratégiai területekre érdemes fókuszálni. **A fentiek alapján a 3. hipotézist is elfogadható.**

VII.5. Az eredmények jelentősége

A hipotézisek igazolásának jelentősége a következőkben fogalmazható meg:

Mivel valóban elő lehet állítani olyan összesített kockázati mutatót, amely figyelembe veszi az egyes tényezők együttes hatásait, ezért lehetőség nyílik a vállalati informatikai kockázatok újfajta értékelésére. Egy ilyen mérőszám segítségével korábban nem azonosítható kockázatok is előtérbe kerülhetnek. Bizonyos esetekben kockázatosnak ítélhetnek olyan területeket, amelyek a hagyományos eljárások előtt rejtve maradtak.

Mindez azt eredményezi, hogy a vállalati menedzsment pontosabb képet kaphat a szervezet informatikai kockázati szintjéről. A kölcsönhatások figyelembevétele miatt a javasolt mutató alkalmasabb a vállalat nagyobb területeinek, több kockázatforrásból álló tartományainak átfogó kockázati értékelésére. Ezáltal a menedzsment olyan eszközt kaphat kézbe, amely lehetővé teszi a stratégiai kiigazítások objektívebb alapra helyezését.

Ezen túlmenően a mód nyílik arra is, hogy a következő audit tevékenységeket pontosabban meg tudják tervezni, hiszen a vizsgálandó területek kiválasztására, az auditálási terv megalkotására a korábbiaknál pontosabb eljárás áll a rendelkezésükre.

Meg kell azonban jegyeznünk, hogy önmagában az eredmények feltárása nem elegendő a fent említett előnyök realizálásához. Ahhoz, hogy a vezetők értelmezni tudják a kapott mutatókat, szükséges, hogy a számukra is érthető formátumba, a megfelelő „nyelvre” fordítsák le azokat. Ezért az auditor feladata nem ér véget a mutató elkészítésével. További felelőssége, hogy

megfelelő kontextusba helyezze az eredményeket, ezzel fogódzót nyújtva a vállalati felelősöknek a megfelelő értelmezéshez.

Amennyiben ezek az adatok, az auditálás eredményei, és azok kockázati mutatószámokkal való alátámasztása rendelkezésre állnak, a vállalati menedzsment számára lehetővé válik, hogy az informatikával kapcsolatos erőforrásokat optimálisan osszák el. A vállalat korlátozott lehetőségeit olyan módon lehet felhasználni, hogy abból az informatikai kockázatkezelés a lehető legnagyobb hasznot húzza.

Összességében a kölcsönhatásokat is figyelembevevő kockázati mutatóval a vállalati döntéshozók olyan eszközhöz jutnak, amely megkönnyíti az informatikával kapcsolatos erőforrások allokációját és a stratégiai döntések meghozatalát.

VIII. FEJEZET
Összefoglalás

VIII.1. A dolgozat céljai

Az értekezés célja a kockázatértékelési metrikával kapcsolatos kutatás bemutatása volt. Megismerhettük a kutatás célkitűzéseit, a területhez kapcsolódó elméleti hátteret, a kutatás lehetséges módszereit és a végrehajtás menetét. A dolgozat záró részében bemutattuk az elért eredményeket és a feltevések igazolását.

A jelen kutatás az információtechnológiai auditálás egy részterületére, az informatikai rendszerekhez, folyamatokhoz, és az informatikával kapcsolatos döntésekhez köthető kockázatokkal, ezen belül a kockázatok értékelésével foglalkozik.

A kutatás célja kettős: egyrészt megalkotni a kockázatértékelés eljárását, másrészt felfedni a kockázatok pontos értékelésének előnyeit. Ennek következtében a kutatás széles kört ölel fel, és nem csupán az auditálási folyamat egy részelemét érinti, hanem megpróbál számolni az egyéb területeken kifejtett hatásokkal is.

Ezért az ismertetett elméleti háttér is széleskörű. Áttekintést adtunk az auditálás általános fogalmairól, az információtechnológiai auditálásról, az IT audithoz kapcsolódó különböző szabványosítási törekvésekről, valamint a kockázatértékelés lehetséges eljárásairól, módszertanairól, és a kockázatértékelési metrika megalkotásának lehetséges segédeszközeiről.

A kockázatértékelés fontos eleme az auditálási folyamatnak, hiszen a legtöbb vezető éppen a kockázatok felmérése érdekében kíván auditálást végeztetni. Szükség van arra, hogy a döntéshozók pontosan fel tudják mérni, milyen veszélyek fenyegetik a vállalati működést. Az információtechnológia pedig számos olyan kockázatot rejt, amely a vállalat egészére hatással van. A kockázatok pontos figyelembevételét azonban nagyban nehezíti, hogy nincs

általánosan elfogadott módszer azok értékelésére, így az egyszerű felsoroláson túl általában csak közelítő értékek megadására van lehetőség. Amennyiben pedig a kockázatok számszerűsítésére kerül sor, az legtöbbször csak egy-egy részterületre vonatkozik, és nagyban támaszkodik a szakértőknek az adott vizsgálatra korlátozott becslésére.

Egy szélesebb körben alkalmazható kockázatértékelési eljárás előrelépést jelenthet ezen a területen. Ennek létrehozásához azonban számos problémát meg kellett oldani, a megfelelő módszer kiválasztásától kezdve a kockázati kölcsönhatások értékelésén keresztül a megfelelő algoritmus megalkotásáig. A metrika megalkotásához alapos elméleti háttértudásra és gyakorlati tapasztalatokra is szükség volt.

A célként megfogalmazott kockázatértékelési eljárás megalkotása azonban megéri a fáradságot. Senki nem vonhatja kétségbe, hogy egy megfelelően, nagy körültekintéssel megalkotott kockázati metrika nagyban segítheti az auditálási folyamat hatékonyságát, és a hatékonyabb auditálások eredményeként a vállalatok erőforrás-allokációjának optimalizálását is elősegítheti az érintett területeken.

A kockázatértékelési módszer tehát nem a vállalat működésétől független terület, hanem az IT auditálás minőségének javításán keresztül a vállalat hatékony működésének segédeszköze.

VIII.2. A kutatási módszer

A kutatás során olyan kockázati mutatószámot előállítása volt a cél, amely egyrészt figyelembe veszi az egyes kockázati tényezők közötti kölcsönhatásokat is, másrészt pedig széleskörűen használható, és átfogó képet ad egy vállalat működésének informatikai kockázatairól.

Feltevésünk az volt, hogy a fent említett célokat leginkább egy olyan metrikával lehet elérni, amely az informatikai funkció összesített kockázatát mutatja, olyan módon, hogy megkülönbözteti a kockázatot növelő, illetve a kockázatot csökkentő tényezőket, figyelembe veszi ezek együttes hatásait, és

lehetőséget teremt a különböző tényezők fontossági (vagy a veszélyeztetés mértéke szerinti) súlyozására.

A kutatás újdonságát a kockázati tényezők közötti összefüggések figyelembevétele és az informatikával kapcsolatos kockázatok teljes körére való kiterjedés jelenti. Ugyanis számos kockázatértékelési módszer létezik, amelynek segítségével elő lehet állítani egy-egy terület kockázati mutatószámát, ezek azonban legtöbbször nem veszik figyelembe az egyes tényezők együttes hatásait. Ráadásul az ilyen módszerek általában nem is tekintik céljuknak, hogy széles körben alkalmazhatók legyenek, és akár vállalatok közötti összehasonlítást is lehetővé tegyenek. Ezért – bár egy-egy területen időbeli összehasonlításra alkalmazhatóak – nem használhatók széles körben annak megállapítására, hogy a vállalat milyen kockázati szinten áll versenytársaihoz képest.

A kutatás során kiterjedt vizsgálat végzésére került sor arra vonatkozóan, hogy a célként elképzelt kockázatértékelési metrikát milyen módszerrel lehet megalkotni. Az elérhető módszerek közül a többszempontú döntési modellek alkalmazhatósága volt igazolható. A kockázatok számbavételénél a széleskörűen elterjedt és igen átfogó COBIT módszertant alkalmazása volt célszerű. Ezáltal lehetővé vált a kockázatok igen széles körének figyelembevétele.

A kutatás során sikerült felmérni, hogy a COBIT kontroll célkitűzései között milyen összefüggések állapíthatók meg. A vizsgálat arra terjedt ki, hogy két – a kontroll célkitűzésekből levezethető – kockázati tényező együttes fennállása esetén milyen módon változik az összesített kockázati mutatószám. Az előálló értékeket egy kölcsönhatási mátrixban sikerült ábrázolni, amelyből megállapítható, hogy a kockázati tényezők egyes kombinációi milyen hatással vannak az összesített kockázati mutatóra. Ezekből az értékekből súlyozással áll elő a javasolt *R* összesített kockázati mutatószám.

A mutató viselkedése Monte Carlo szimulációval volt ellenőrizhető. Ennek során 500 különböző ellenőrzés leképezése, és a kapott eredmények

rögzítése történt meg. A megállapítások alátámasztására ezeket az eredményeket a matematikai statisztika eszközkészletével volt szükséges elemezni.

VIII.3. Elért eredmények, főbb megállapítások

A kutatás végrehajtása és az adatok elemzése segítségével sikerült alátámasztani a dolgozat legfőbb megállapításait. A kutatás során bebizonyosodott, hogy elő lehet állítani egy olyan informatikai kockázati mutatószámot, amely figyelembe veszi az egyes területek közötti kölcsönhatásokat. Az adatok elemzéséből világosan kiderül, hogy ez a módszer alkalmas arra, hogy hitelesen orientálja a vállalati informatika felelőseit. Lehetővé válik a kritikus területek azonosítása.

Világossá vált, hogy a korábban végrehajtott auditálások eredményei felhasználhatók arra, hogy a pontosabb és a céloknak jobban megfelelő audit tervet készítsünk. Ha figyelembe vesszük a már megvizsgált területeket, és az ott felfedezett kölcsönhatásokat, akkor lehetővé válik olyan forgatókönyvek felállítása, amelyekben felhasználjuk az egyes kockázati tényezők összefüggéseit, és ezek hatását a kockázatra. Arra is lehetőség nyílik, hogy pontosabban behatároljuk a vizsgálat szempontjából kritikus területeket. Ilyen módon a korábbinál jobb és hatékonyabban végrehajtható auditálási terveket lehet készíteni.

Sikerült bebizonyítani, hogy a javasolt kockázati mérőszám használatával olyan, az informatikával kapcsolatos, stratégiai fontosságú területek azonosítása is lehetséges, amelyeket a korábban szokásos módszerekkel nem lehet meghatározni. Erre elsősorban az teremt lehetőséget, hogy a kockázati tényezők együtthatásainak figyelembevétele olyan együttállásokat is észlelhetővé tesz, amelyek a vállalati stratégia szempontjából jelentősek, ugyanakkor felderítésükre a kockázati mutatók túl kevés dimenziója miatt nem volt lehetőség.

A kutatásnak a nemzetközi szervezetek törekvéseivel is összhangban lévő iránya megfelelő egy átfogó kockázatértékelési metrika megalkotásához.

Az elért eredmények jó kilátásokat biztosítanak a módszer használhatóságára és továbbfejlesztésére vonatkozóan. Ugyanakkor tisztában kell lenni az eddigi kutatás eredményeinek korlátaival is. Már a vizsgálat során világossá vált, hogy számos további problémát kell megoldani a módszer tökéletesítése érdekében.

VIII.4. További feladatok és kihívások

Az eddigiekben vázolt megoldás elérhető közelségbe hozta azt a célt, hogy széleskörűen elfogadható és jól hasznosítható módszert állítsunk elő. Ugyanakkor számos megoldandó feladat van még. Egyrészt a rendkívül nagyszámú változó miatt egyelőre csak arra volt lehetőség, hogy a felső szintű kontroll célkitűzések együttes hatását vizsgáljuk. A részletes kontroll célkitűzések mátrixa több mint 300x300, azaz közel százezer, a dolgozatban bemutatott négyzetet tartalmazna, egyenként 4 mezővel. Ezt a kutatás keretein belül egyelőre nem volt lehetséges feltölteni, ezért azzal a munkahipotézissel kellett élni, hogy a részletes kontroll célkitűzések a szülőobjektumukkal – tehát a felső szintű kontroll célkitűzésekkel – analóg módon viselkednek. A további kutatás során arra ügyelni kell, hogy ennek következtében ne forduljon elő ellentmondás a mátrixban.

További feladatot jelent az elsőrendű kölcsönhatásokon túlmenően a többedrendűek vizsgálata, bár ezek feltehetőleg csökkenő mértékben járulnak hozzá a módszer pontosságához.

A kutatás szempontjából az lenne ideális, ha rendelkezésre állna olyan nagy mennyiségű adat, amely auditálásokból származik, és a módszer által megkövetelt értékeléseket és súlyokat tartalmazza. Ebben az esetben nem lenne szükséges az auditor munkáját szimulálni, hanem valós adatok és tényleges szakmai értékelés alapján lehetne megállapítani mind a kockázati tényezők egymásrahatását, mind a tényezők súlyait. Mivel ilyen adatok nem hozzáférhetők, ezért a módszer használhatóságának igazolására és finomhangolására Monte-Carlo szimuláció végzésével nyílt mód. A szimuláció során a kockázati tényezők értékét és súlyát lehetett modellezni, 500 különböző

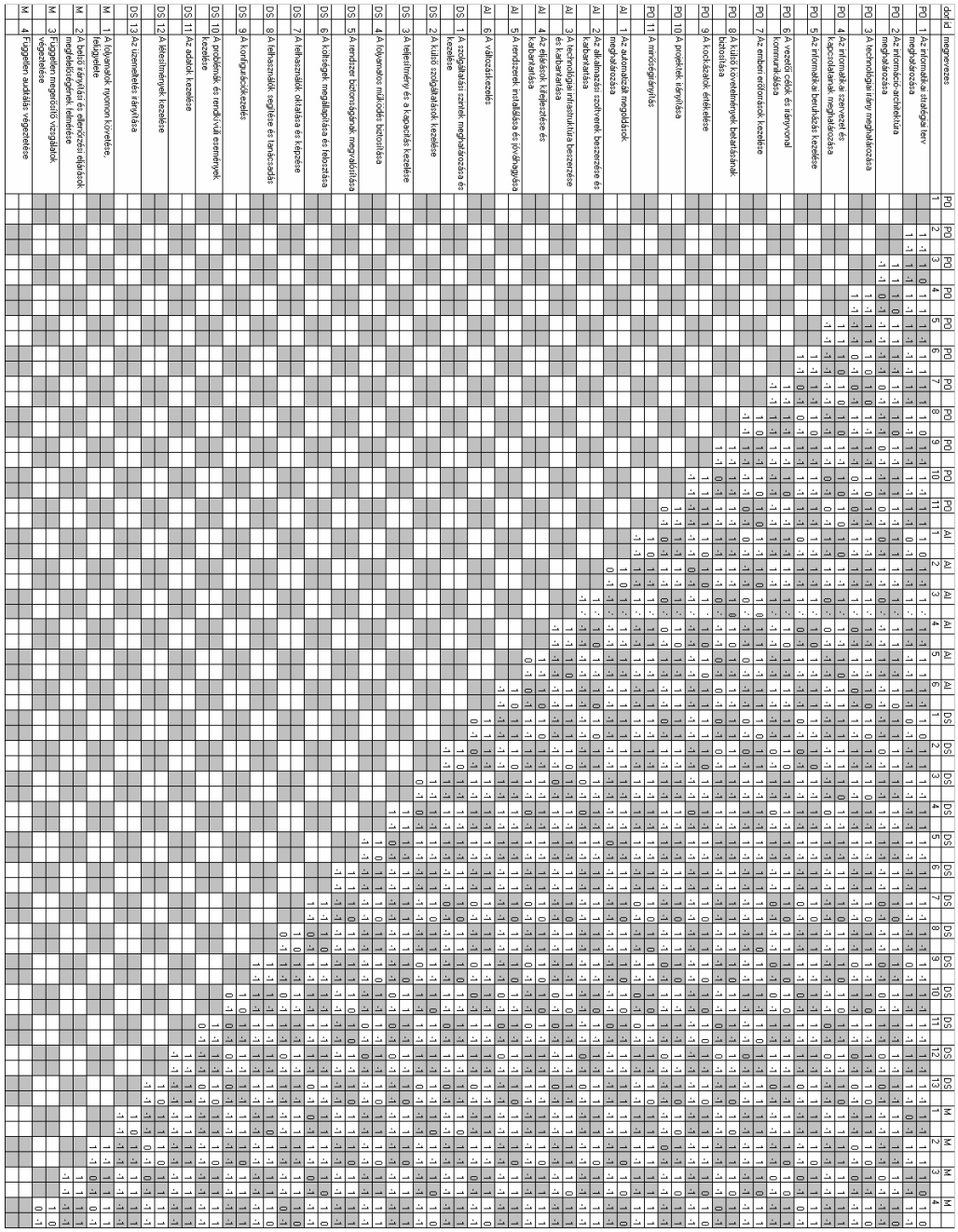
teljes auditálási eredményt produkálva. Ennek eredményeként olyan statisztikai kimutatásokat lehetett készíteni, amelyek az egyes módszerek közötti különbségek bemutatására és a javasolt változat alátámasztására használhatók.

Amennyiben mégis lehetőség lenne ténylegesen végrehajtott auditálásokból származó nagy mennyiségű adat vizsgálatára, akkor lehetőség nyílna a módszer megalkotásán túlmenően annak pontos adatokkal (súlyokkal és összefüggési mutatókkal) való feltöltésére, amely akár piaci környezetben is használható kockázatértékelési metrikát adhat eredményül. Remélhetőleg mód nyílik a kutatás folytatására, és az elért eredmények felhasználásával a gyakorlatban még jobban használható megoldást lehet előállítani.

IX. FEJEZET

Függelék

IX.1. A kölcsönhatási mátrix



IX.2. Forgatókönyvek

A vizsgálandó részletes kontroll célkitűzések az egyes forgatókönyvekben.

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
PO	1	1	Az információtechnológia mint a szervezet hosszú- és rövid távú terveinek része				
PO	1	2	Hosszú távú informatikai terv				
PO	1	3	Hosszú távú informatikai tervezés - Módszer és struktúra				
PO	1	4	A hosszú távú informatikai tervmódosítása				
PO	1	5	Az informatikai funkció rövidtávú tervezése				
PO	1	6	Az informatikai tervek kommunikációja				
PO	1	7	Az informatikai tervek megvalósulásának ellenőrzése és értékelése				
PO	1	8	A meglévő rendszerek értékelése		x		
PO	2	1	Információ-architektúra modell				
PO	2	2	Vállalati adatszótár és adatszintaktikai szabályok				
PO	2	3	Adatosztályozási rendszer				
PO	2	4	Biztonsági szintek	x			
PO	3	1	Technológiai infrastruktúratervezés				x
PO	3	2	A jövőbeni trendek és jogszabályok figyelemmel kísérése				x
PO	3	3	A technológiai infrastruktúra üzemfolytonossága		x	x	x
PO	3	4	Hardver és szoftver beszerzési tervek				
PO	3	5	Technológiai szabványok				x
PO	4	1	Informatikai Tervezési vagy Irányító Bizottság				
PO	4	2	Az informatikai funkció szervezeti elhelyezkedése				
PO	4	3	A szervezeti eredmények áttekintése				
PO	4	4	Feladatok és felelősségi körök		x	x	
PO	4	5	Minőségbiztosítási felelősség			x	
PO	4	6	Logikai és fizikai biztonsági felelősség	x		x	
PO	4	7	Tulajdonlás és kezelés		x	x	
PO	4	8	Az adatok és rendszerek tulajdonlása	x		x	
PO	4	9	Felügyelet		x	x	
PO	4	10	A feladatkörök szétválasztása			x	
PO	4	11	Az informatikai személyzettel valógazdálkodás		x	x	
PO	4	12	Az informatikai személyzet munkaköri leírásai			x	

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
PO	4	13	Informatikai kulcsszemélyek			x	
PO	4	14	A szerződéses személyzetre vonatkozó szabályok és eljárások			x	
PO	4	15	Kapcsolatok				
PO	5	1	Éves informatikai működési költségvetés				
PO	5	2	Költség-haszon monitoring		x		
PO	5	3	A költségek és a haszon igazolása		x		
PO	6	1	Pozitív informatikai kontroll környezet				
PO	6	2	A vezetés felelőssége a szabályok kidolgozásával kapcsolatban				x
PO	6	3	A szervezeti szabályok közlése				x
PO	6	4	A szabályok bevezetéséhez szükséges erőforrások				x
PO	6	5	A szabályok aktualizálása				x
PO	6	6	A szabályok, eljárások és szabványok betartása				x
PO	6	7	A minőség iránti elkötelezettség			x	x
PO	6	8	A biztonságra és a belső kontroll rendszerre vonatkozó szabályok	x			x
PO	6	9	Szellemi tulajdonjogok				x
PO	6	10	Konkrét kérdésekhez kapcsolódó szabályok			x	
PO	6	11	Az informatikai biztonsági tudatosságkommunikálása	x		x	
PO	7	1	A dolgozók felvétele és előléptetése				x
PO	7	2	A személyzet képzettsége és minősítései		x		x
PO	7	3	Feladatok és felelősségi körök				x
PO	7	4	A dolgozók képzése				x
PO	7	5	Átképzés vagy helyettesítés				x
PO	7	6	Személyes átvilágítási eljárások				x
PO	7	7	A dolgozók teljesítmény-értékelése		x		x
PO	7	8	A munkakörök változtatása és megszűntetése				x
PO	8	1	A külső követelmények áttekintése				x
PO	8	2	A külső követelmények betartásához kapcsolódó gyakorlat és eljárások				x
PO	8	3	A balesetvédelmi és ergonómiai előírások betartása				x
PO	8	4	Személyiségi jogok, szellemi tulajdon és adatáramlás				x
PO	8	5	Elektronikus kereskedelem			x	
PO	8	6	A biztosítási szerződések betartása				x
PO	9	1	Az üzleti kockázatok értékelése				
PO	9	2	Kockázatértékelési stratégia				
PO	9	3	A kockázatok azonosítása			x	
PO	9	4	A kockázatok mérése	x		x	
PO	9	5	Kockázati cselekvési terv	x		x	
PO	9	6	Kockázatviselés			x	

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
PO	9	7	A védelem kiválasztása	x		x	
PO	9	8	A kockázatértékelés melletti elkötelezettség			x	
PO	10	1	Projektirányítási keretrendszer				x
PO	10	2	A felhasználó osztály részvétele a projektkezdeményezésében				x
PO	10	3	Projekt munkacsoport tagjai és feladatai				x
PO	10	4	A projektek meghatározása				x
PO	10	5	A projektek jóváhagyása				x
PO	10	6	A projekt szakaszainak jóváhagyása				x
PO	10	7	Felső szintű projekt-terv				x
PO	10	8	Rendszer-minőségbiztosítási terv				x
PO	10	9	A megerősítő vizsgálati módszerek tervezése				x
PO	10	10	Formális projekt-kockázatkezelés				x
PO	10	11	Tesztelési terv				x
PO	10	12	Képzési terv				x
PO	10	13	Megvalósítást követő vizsgálati terv				x
PO	11	1	Általános minőségi terv		x	x	x
PO	11	2	Minőségbiztosítási stratégia		x	x	x
PO	11	3	A minőségbiztosítás tervezése		x	x	x
PO	11	4	Az informatikai szabványok és eljárások betartására vonatkozó minőségbiztosítási felülvizsgálat		x	x	x
PO	11	5	Rendszerfejlesztési életciklus módszertan			x	x
PO	11	6	Rendszerfejlesztési életciklus módszertan az alkalmazott technológia jelentős megváltoztatása esetén			x	x
PO	11	7	A rendszerfejlesztési életciklus módszertan aktualizálása			x	x
PO	11	8	Koordináció és kommunikáció		x	x	x
PO	11	9	A technológiai infrastruktúra beszerzésére és karbantartására vonatkozó keretrendszer			x	x
PO	11	10	Kapcsolattartás külső rendszermegvalósítókkal/fejlesztők kel			x	x
PO	11	11	Program dokumentációs szabványok				x
PO	11	12	Programtesztelési szabványok				x
PO	11	13	Rendszertesztelési szabványok				x
PO	11	14	Párhuzamos futtatás/kísérleti tesztelés				x
PO	11	15	A rendszer tesztelés dokumentációja				x
PO	11	16	A fejlesztési szabványok betartását ellenőrző minőségbiztosítási értékelés				x
PO	11	17	Az informatikai célkitűzések teljesítésére vonatkozó minőségbiztosítási ellenőrzés			x	x

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
PO	11	18	A minőség mérése			x	x
PO	11	19	Jelentéskészítés a minőségbiztosítási ellenőrzésekről			x	x
AI	1	1	Az információs követelmények meghatározása			x	
AI	1	2	Alternatív cselekvési lehetőségek kidolgozása			x	
AI	1	3	A beszerzési stratégia kidolgozása				
AI	1	4	A külső szolgáltatásokra vonatkozó követelmények				x
AI	1	5	Technológiai megvalósíthatósági tanulmány				
AI	1	6	Gazdasági megvalósíthatósági tanulmány				
AI	1	7	Információ-architektúra				
AI	1	8	Kockázatelemzési jelentés			x	
AI	1	9	Költséghatékony biztonsági eljárások				x
AI	1	10	Az audit szempontú nyomonkövethetőség kialakítása				x
AI	1	11	Ergonómia				x
AI	1	12	A rendszer-szoftver kiválasztása			x	
AI	1	13	A beszerzés irányítása és ellenőrzése				
AI	1	14	A szoftver-termékek beszerzése				
AI	1	15	A külső fél által végzett szoftver-karbantartás				
AI	1	16	Szerződéses alkalmazás-programozás				
AI	1	17	A létesítmények átvétele				
AI	1	18	A technológia átvétele				
AI	2	1	Kiviteli tervkészítési módszerek				x
AI	2	2	A meglévő rendszerek jelentősebb módosítása			x	
AI	2	3	A kiviteli terv jóváhagyása				x
AI	2	4	Az adatállományokra vonatkozókövetelmények meghatározása és dokumentálása			x	
AI	2	5	Program-specifikáció			x	x
AI	2	6	A forrás-adatok összegyűjtésének terve				
AI	2	7	Az inputokra vonatkozó követelmények meghatározása és dokumentálása				x
AI	2	8	Az interfészek meghatározása				x
AI	2	9	A felhasználó és a számítógép közötti interfész			x	x
AI	2	10	Az adatfeldolgozási követelmények meghatározása és dokumentálása	x			x
AI	2	11	Az outputokra vonatkozó követelmények meghatározása és dokumentálása		x	x	
AI	2	12	Kontrollálhatóság			x	
AI	2	13	A rendelkezésre állás, mint kulcsfontosságú tervezési faktor		x	x	x

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
AI	2	14	Az adatok sértetlenségét biztosítófunkciók a az alkalmazási szoftverekben	x	x	x	x
AI	2	15	Az alkalmazási szoftverek tesztelése				x
AI	2	16	A felhasználói kézikönyvek és segédletek				
AI	2	17	A rendszer kiviteli tervének felülvizsgálata			x	
AI	3	1	Az új hardverek és szoftverek értékelése			x	
AI	3	2	Preventív hardver-karbantartás			x	
AI	3	3	A rendszer-szoftverek biztonsága	x		x	
AI	3	4	A rendszer-szoftverek telepítése			x	
AI	3	5	A rendszer-szoftverek karbantartása			x	
AI	3	6	A rendszer-szoftverek változáskezelése			x	
AI	3	7	A rendszer-segédprogramok használata és monitorozása			x	
AI	4	1	Üzemeltetési követelmények és szolgáltatási szintek		x	x	
AI	4	2	A felhasználói eljárások kézikönyvei			x	x
AI	4	3	Üzemeltetési kézikönyv			x	x
AI	4	4	Oktatási anyagok				x
AI	5	1	Képzés				
AI	5	2	Az alkalmazási szoftverek teljesítményének méretezése		x	x	x
AI	5	3	Rendszermegvalósítási terv			x	x
AI	5	4	Rendszer-konverzió			x	
AI	5	5	Adat-konverzió	x		x	
AI	5	6	Tesztelési stratégiák és tervek			x	
AI	5	7	A változtatások tesztelése			x	
AI	5	8	A párhuzamos futtatás/kísérleti tesztelés kritériumai és végrehajtása			x	
AI	5	9	Végső átvételi teszt			x	
AI	5	10	Biztonsági tesztelés és jóváhagyás			x	
AI	5	11	Üzemi teszt			x	
AI	5	12	Üzemi környezetbe helyezés			x	
AI	5	13	A felhasználói igényeknek valómegfelelés értékelése			x	x
AI	5	14	A megvalósítást követő vezetői ellenőrzés			x	
AI	6	1	A változtatási kérelmek kezdeményezése és kontrollja			x	
AI	6	2	Hatás-elemzés			x	
AI	6	3	Változáskezelés			x	
AI	6	4	Kényszerhelyzeti változtatások			x	
AI	6	5	Dokumentáció és eljárások			x	
AI	6	6	Engedélyezett karbantartás			x	x
AI	6	7	A szoftver-változatok kibocsátására vonatkozó szabályok				x

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
AI	6	8	A szoftverek terítése				x
DS	1	1	A szolgáltatási szint megállapodásokra vonatkozó keretrendszer			x	
DS	1	2	A szolgáltatási szint megállapodásokban szabályozott kérdések		x	x	
DS	1	3	Teljesítési eljárások		x	x	
DS	1	4	Felügyelet és jelentéskészítés			x	
DS	1	5	A szolgáltatási szint megállapodások és szerződések felülvizsgálata		x	x	
DS	1	6	Kiterhelhető költségtételek				
DS	1	7	Szolgáltatás-fejlesztési program				
DS	2	1	Szállítói kapcsolatok			x	
DS	2	2	Kapcsolattartási felelős				
DS	2	3	A külső felekkel kötött szerződések				
DS	2	4	A külső felek minősítése				
DS	2	5	Szolgáltatás-kiszervezési szerződések				
DS	2	6	A szolgáltatások folyamatossága			x	
DS	2	7	Biztonsági megállapodások	x		x	
DS	2	8	Folyamatos ellenőrzés			x	
DS	3	1	A rendelkezésreállásra és a teljesítményre	x	x	x	
DS	3	2	Rendelkezésre állási terv	x	x	x	
DS	3	3	Monitorozás és jelentéskészítés		x	x	
DS	3	4	Modellezési eszközök			x	
DS	3	5	Proaktív teljesítményirányítás		x	x	
DS	3	6	Az üzemi terhelés előrejelzése	x	x	x	
DS	3	7	Az erőforrások kapacitás-kezelése	x	x	x	
DS	3	8	Az erőforrások rendelkezésre állása	x	x	x	
DS	3	9	Az erőforrások ütemezése		x	x	
DS	4	1	Informatikai folytonossági keretrendszer		x	x	
DS	4	2	Az informatikai folytonossági tervre vonatkozó stratégia és filozófia			x	
DS	4	3	Informatikai folytonossági terv tartalma	x	x	x	
DS	4	4	Az informatikai folytonossági követelmények minimalizálása			x	
DS	4	5	Az informatikai folytonossági terv karbantartása		x	x	
DS	4	6	Az informatikai folytonossági tervtesztelése	x		x	
DS	4	7	Az informatikai folytonossági tervhez kapcsolódó képzés			x	
DS	4	8	Az informatikai folytonossági tervszétosztása			x	
DS	4	9	A felhasználói terület által kialakított alternatív feldolgozási folyamatok,helyettesítő eljárások		x	x	

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
DS	4	10	Kritikus fontosságú informatikai erőforrások	x	x	x	
DS	4	11	Tartalék telephely és hardverek	x	x	x	
DS	4	12	A mentési anyagok külső tárolása	x		x	
DS	4	13	Értékelési és módosítási eljárások			x	
DS	5	1	A biztonsági intézkedések kezelése				
DS	5	2	Azonosítás, hitelesítés és hozzáférési jogosultság	x			
DS	5	3	Az adatok hozzáférésének biztonsága közvetlen kapcsolat esetén	x			
DS	5	4	A felhasználói azonosítók kezelése	x			
DS	5	5	A felhasználói azonosítók vezetői ellenőrzése				
DS	5	6	A felhasználói azonosítók felhasználói kontrollja				
DS	5	7	Biztonsági felügyelet	x		x	
DS	5	8	Az adatok osztályozása	x			
DS	5	9	Központi felhasználó-azonosítás és jogosultságkezelés	x			
DS	5	10	Jelentéskészítés a biztonsági előírások megsértéséről és a biztonsági tevékenységről				
DS	5	11	A rendkívüli események kezelése	x		x	
DS	5	12	Újrahitelesítés				
DS	5	13	A másik fél hitelesítése	x			
DS	5	14	A tranzakciók engedélyezése	x			
DS	5	15	Letagadhatatlanság	x			
DS	5	16	Hitelesített útvonalak	x			
DS	5	17	A biztonsági funkciók védelme	x			
DS	5	18	A kriptográfiai kulcsok kezelése	x			
DS	5	19	A rossz szándékú szoftverek megjelenésének megelőzése, felderítése és elhárítása	x		x	
DS	5	20	Tűzfal architektúrák és kapcsolódás a nyilvános hálózatokhoz	x			
DS	5	21	Az elektronikus értékek megvédése	x		x	
DS	6	1	Felszámítható költségtételek				
DS	6	2	Költségszámítási eljárások				
DS	6	3	Felhasználói számlázási és visszaterhelési eljárások				
DS	7	1	Az oktatási igények meghatározása				
DS	7	2	A képzés megszervezése				
DS	7	3	A biztonsági alapelvekre és a tudatosságra irányuló képzés	x			
DS	8	1	Help Desk			x	
DS	8	2	A felhasználói kérdések nyilvántartása			x	
DS	8	3	A felhasználói kérdések továbbítása a megoldók felé			x	
DS	8	4	A felhasználói kérdések megoldásának figyelemmel kísérése			x	

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
DS	8	5	A trendek elemzése és jelentése				
DS	9	1	A konfiguráció nyilvántartása			x	
DS	9	2	A konfiguráció bázisának nyilvántartása				
DS	9	3	A státusz nyilvántartása				
DS	9	4	A konfiguráció nyilvántartás kontrollja	x		x	
DS	9	5	Engedély nélküli szoftverek	x		x	
DS	9	6	A szoftverek tárolása				
DS	9	7	Konfigurációkezelési eljárások			x	
DS	9	8	A szoftverekre vonatkozó elszámoltathatóság				
DS	10	1	Probléma-kezelő rendszer	x	x	x	x
DS	10	2	szintekre történő továbbítása (eszkaláció)		x	x	x
DS	10	3	A problémák ellenőrzési szempontú nyomonkövethetősége		x	x	x
DS	10	4	A kényszerhelyzeti és ideiglenes hozzáférés engedélyezése	x	x		x
DS	10	5	Kényszerhelyzeti feldolgozási prioritások		x	x	x
DS	11	1	Adatelőkészítési eljárások				
DS	11	2	A forrás-dokumentumok engedélyezési eljárásai				
DS	11	3	A forrás-dokumentumok adatainak összegyűjtése				
DS	11	4	A forrás-dokumentumok hibáinak kezelése				
DS	11	5	A forrás-dokumentumok megőrzése				
DS	11	6	Adatbevitel-engedélyezési eljárások	x	x		
DS	11	7	A pontosság, teljesség és engedélyezettség ellenőrzése	x	x		
DS	11	8	Az adatbeviteli hibák kezelése	x	x		
DS	11	9	Az adatfeldolgozás sértetlensége	x	x		
DS	11	10	Az adatfeldolgozás érvényességének ellenőrzése és a szerkesztés	x	x		
DS	11	11	Az adatfeldolgozási hibák kezelése	x	x		
DS	11	12	A kimenő adatok kezelése és megőrzése	x	x		
DS	11	13	A kimenő adatok szétosztása		x		
DS	11	14	A kimenő adatok egyeztetése		x		
DS	11	15	A kimenő adatok felülvizsgálata és a hibakezelés	x	x		
DS	11	16	A kimenő adatokról készült jelentésekre vonatkozó biztonsági előírások	x			
DS	11	17	A bizalmas információk védelme adattovábbítás és szállítás közben	x			
DS	11	18	A megsemmisítendő bizalmas információk védelme	x			
DS	11	19	Az adattárolás kezelése	x	x		
DS	11	20	Megőrzési idő és tárolási feltételek	x	x		

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
DS	11	21	Adathordozókönyvtár-kezelő rendszer	x	x		
DS	11	22	Az adathordozó-könyvtár kezeléséhez kapcsolódó felelősségek	x			
DS	11	23	Mentés és helyreállítás	x	x		
DS	11	24	Mentési munkafolyamatok	x	x		
DS	11	25	A mentések tárolása	x	x		
DS	11	26	Archiválás	x	x		
DS	11	27	A bizalmas üzenetek védelme	x			
DS	11	28	Hitelesítés és sértetlenség	x			
DS	11	29	Az elektronikus tranzakciók sértetlensége	x			
DS	11	30	A tárolt adatok sértetlenségének folyamatos fenntartása	x	x		
DS	12	1	Fizikai védelem	x		x	x
DS	12	2	Az informatikai telephelyre vonatkozó információk elrejtése	x			
DS	12	3	A látogatók kísérése	x			x
DS	12	4	A személyzet egészség- és munkavédelme				
DS	12	5	A környezeti tényezőkkel szembeni védelem	x		x	
DS	12	6	Szünetmentes áramforrás	x	x	x	
DS	13	1	A feldolgozási üzemeltetési eljárások és utasítások kézikönyve			x	
DS	13	2	Az indítási folyamat és egyéb üzemeltetési eljárások dokumentációja			x	
DS	13	3	A gépi műveletek ütemezése	x	x	x	
DS	13	4	Eltérések a gépi műveletek előírt ütemezésétől	x	x	x	
DS	13	5	A feldolgozás folytonossága	x	x	x	
DS	13	6	Üzemeltetési naplók			x	
DS	13	7	A speciális nyomtatványok és outputeszközök védelme				
DS	13	8	Távoli üzemeltetés	x		x	
M	1	1	A monitoring adatok összegyűjtése		x		x
M	1	2	A teljesítmény értékelése		x	x	x
M	1	3	A felhasználói elégedettség értékelése		x	x	x
M	1	4	Vezetői jelentések		x		x
M	2	1	A belső irányítás és ellenőrzésmonitorozása				x
M	2	2	A belső kontroll eljárások kellő időben történő alkalmazása				x
M	2	3	Jelentés a belső kontroll szintjéről				x
M	2	4	Megerősítő vizsgálatok a biztonságra és a belső kontrollok működésére vonatkozóan				x
M	3	1	Az informatikai szolgáltatások biztonságára és belső kontrolljára vonatkozó független tanúsítás/jóváhagyás				

Terület	Kontroll célkitűzés	Részletes kontroll célkitűzés	Megnevezés	1. forgatókönyv (bank)	2. forgatókönyv (termelő vállalat)	3. forgatókönyv (szolgáltató)	4. forgatókönyv (szoftverfejlesztő)
M	3	2	A külső szolgáltatókra vonatkozó biztonsági és belső kontroll szempontú függetlentanúsítás/jóváhagyás				
M	3	3	Az informatikai szolgáltatások eredményességének független értékelése		x	x	
M	3	4	A külső szolgáltatók eredményességének független értékelése				
M	3	5	A törvényi és jogszabályi előírások, valamint a szerződéses kötelezettségek betartásának független megerősítése				
M	3	6	A törvényi és jogszabályi előírások, valamint a szerződéses kötelezettségek külső szolgáltatók általi betartásának független megerősítése				
M	3	7	A független megerősítést nyújtó szervezet szakmai kompetenciája				
M	3	8	Az audit funkció proaktív közreműködése				
M	4	1	Auditálási, ellenőrzési szabályzat				x
M	4	2	Függetlenség				x
M	4	3	Szakmai etika és szabványok				
M	4	4	Szakmai kompetencia				
M	4	5	Tervezés				
M	4	6	Az audit végrehajtása				
M	4	7	Jelentéskészítés				
M	4	8	A javaslatok végrehajtásának nyomonkövetése				x

IX.3. Alapstatisztikák

IX.3.1. A kontroll célkitűzések teljességére

	Számtani átlag	Súlyozott átlag	Interakciós átlag	R
Várható érték	-0,0029	0,0000	-0,0894	-0,0921
Standard hiba	0,0076	0,0003	0,0083	0,0088
Medián	0,0000	-0,0002	-0,0933	-0,1017
Módusz	-0,0588	-	-0,2319	-
Szórás	0,1696	0,0060	0,1866	0,1970
Minta varianciája	0,0287	0,0000	0,0348	0,0388
Csúcsosság	-0,0340	-0,2504	-0,2241	-0,3271
Ferdeség	0,1338	0,0948	0,2041	0,1980
Tartomány	1,0588	0,0321	1,1160	1,0799
Minimum	-0,5294	-0,0160	-0,6252	-0,5809
Maximum	0,5294	0,0160	0,4908	0,4991
Összeg	-1,4706	-0,0149	-44,6857	-46,0320
Darabszám	500,0000	500,0000	500,0000	500,0000
Konfidenciaszint(95,0%)	0,0149	0,0005	0,0164	0,0173

IX.3.2. 1. forgatókönyv

	Számtani átlag	Súlyozott átlag	Interakciós átlag	R
Várható érték	-0,0207	-0,0006	-0,1713	-0,1806
Standard hiba	0,0111	0,0004	0,0116	0,0123
Medián	-0,0588	-0,0008	-0,1830	-0,1936
Módusz	0,0588	-	-0,1830	-
Szórás	0,2476	0,0086	0,2583	0,2753
Minta varianciája	0,0613	0,0001	0,0667	0,0758
Csúcsosság	-0,1956	-0,3377	-0,3423	-0,3585
Ferdeség	0,0068	0,0764	0,1121	0,1986
Tartomány	1,5294	0,0502	1,4967	1,5973
Minimum	-0,7647	-0,0243	-0,9150	-0,9046
Maximum	0,7647	0,0258	0,5817	0,6926
Összeg	-10,3529	-0,2836	-85,6275	-90,3076
Darabszám	500,0000	500,0000	500,0000	500,0000
Konfidenciaszint(95,0%)	0,0218	0,0008	0,0227	0,0242

IX.3.3. 2. forgatókönyv

	Számtani átlag	Súlyozott átlag	Interakciós átlag	R
Várható érték	-0,0112	-0,0002	-0,0765	-0,0788
Standard hiba	0,0117	0,0004	0,0124	0,0130
Medián	-0,0667	-0,0002	-0,1000	-0,1025
Módusz	-0,0667	-	-0,1000	-
Szórás	0,2627	0,0091	0,2762	0,2913
Minta varianciája	0,0690	0,0001	0,0763	0,0848
Csúcsosság	-0,0897	-0,2952	-0,1291	-0,2008
Ferdeség	0,1478	-0,0297	0,2789	0,2213
Tartomány	1,4667	0,0492	1,4833	1,5328
Minimum	-0,7333	-0,0243	-0,7417	-0,7717
Maximum	0,7333	0,0249	0,7417	0,7611
Összeg	-5,6000	-0,0875	-38,2583	-39,4160
Darabszám	500,0000	500,0000	500,0000	500,0000
Konfidenciaszint(95,0%)	0,0231	0,0008	0,0243	0,0256

IX.3.4. 3. forgatókönyv

	Számtani. átlag	Súlyozott átlag	Interakciós átlag	R
Várható érték	-0,0110	-0,0001	-0,1181	-0,1207
Standard hiba	0,0098	0,0003	0,0107	0,0112
Medián	-0,0435	0,0001	-0,1322	-0,1326
Módusz	-0,0435	-	-0,1486	-
Szórás	0,2192	0,0074	0,2384	0,2504
Minta varianciája	0,0481	0,0001	0,0568	0,0627
Csúcsosság	-0,1149	-0,2138	-0,2449	-0,4347
Ferdeség	0,0044	-0,0701	0,1746	0,1497
Tartomány	1,3043	0,0395	1,2935	1,2936
Minimum	-0,6522	-0,0208	-0,7500	-0,7326
Maximum	0,6522	0,0187	0,5435	0,5610
Összeg	-5,4783	-0,0696	-59,0362	-60,3368
Darabszám	500,0000	500,0000	500,0000	500,0000
Konfidenciaszint(95,0%)	0,0193	0,0006	0,0209	0,0220

IX.3.5. 4. forgatókönyv

	Számtani átlag	Súlyozott átlag	Interakciós átlag	R
Várható érték	-0,0110	-0,0002	-0,1079	-0,1127
Standard hiba	0,0114	0,0004	0,0124	0,0128
Medián	0,0000	0,0000	-0,1176	-0,1226
Módusz	0,0000	-	0,0221	-
Szórás	0,2550	0,0087	0,2767	0,2860
Minta varianciája	0,0650	0,0001	0,0766	0,0818
Csúcsosság	-0,4120	-0,2970	-0,3816	-0,4685
Ferdeség	0,0342	-0,1892	0,2155	0,0850
Tartomány	1,3750	0,0457	1,4191	1,4674
Minimum	-0,6250	-0,0233	-0,7279	-0,8038
Maximum	0,7500	0,0224	0,6912	0,6636
Összeg	-5,5000	-0,1090	-53,9412	-56,3517
Darabszám	500,0000	500,0000	500,0000	500,0000
Konfidenciaszint(95,0%)	0,0224	0,0008	0,0243	0,0251

IX.4. Statisztikai összesítő tábla

A statisztikákban és a hisztogramokban az egyes rövidítések jelentése a következő:

SZTA – számtani átlag,

SA – súlyozott átlag,

KA – a kölcsönhatások figyelembevételével meghatározott átlag,

R – a kölcsönhatások figyelembevételével és súlyozással meghatározott *R* mutató.

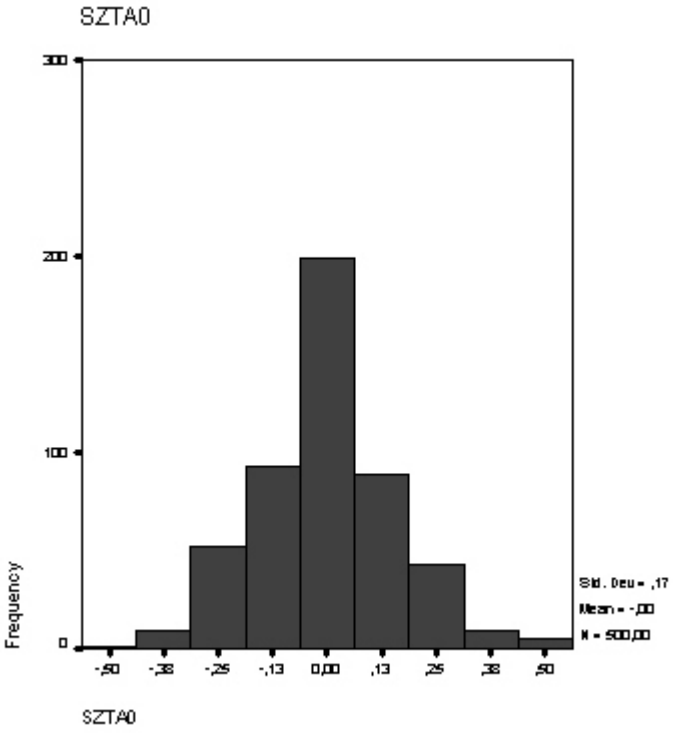
A kódok után található számok a forgatókönyv sorszámára utalnak. A **0** a kontroll célkitűzések teljes körének jelölésére szolgál.

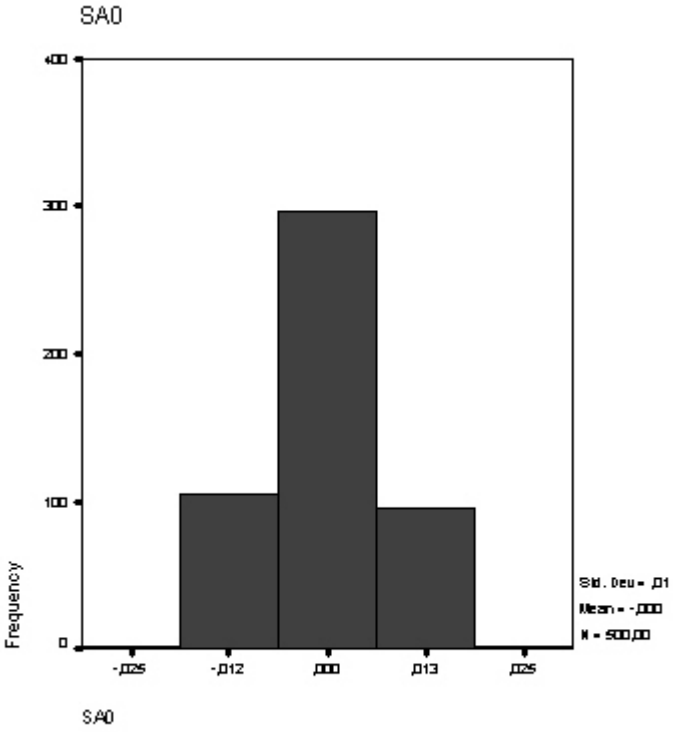
Statistics

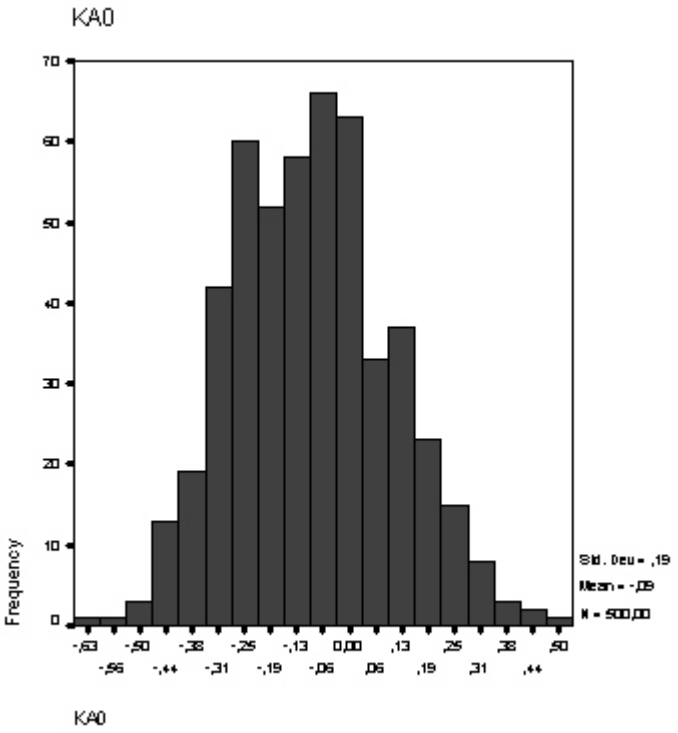
		SZTA0	SA0	KA0	R0	SZTA1	SA1	KA1	R1	SZTA2	SA2	KA2	R2	SZTA3	SA3	KA3	R3	SZTA4	SA4	KA4	R4
N	Valid	500	500	500	500	500	500	500	500	500	500	500	500	500	500	500	500	500	500	500	500
	Missing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mean		-,0029	-,0002	-,0893	-,0919	-,0205	-,0006	-,1711	-,1803	-,0114	,0000	-,0789	-,0789	-,0108	,0000	-,1181	-,1206	-,0111	-,0002	-,1090	-,1128
Std. Error of Mean		,00764	,00029	,00836	,00881	,01105	,00041	,01155	,01231	,01174	,00042	,01239	,01303	,00977	,00035	,01065	,01120	,01150	,00041	,01238	,01279
Median		,0000	,0000	-,0900	-,1000	-,0600	,0000	-,1800	-,1900	-,0700	,0000	-,1000	-,1000	-,0400	,0000	-,1300	-,1300	,0000	,0000	-,1200	-,1200
Mode		-,06	,00	-,11	-,10	,06	,00	-,05	-,17	-,07	,00	-,23	-,26	-,04	,00	-,08	-,12	,00	,00	-,13	-,17(a)
Std. Deviation		,17082	,00652	,18670	,19705	,24705	,00915	,25836	,27526	,26254	,00946	,27696	,29131	,21844	,00779	,23815	,25036	,25721	,00921	,27674	,28603
Variance		,02918	,00004	,03486	,03883	,06103	,00008	,06675	,07577	,06893	,00009	,07671	,08486	,04772	,00006	,05672	,06268	,06616	,00008	,07659	,08182
Skewness		,134	,059	,198	,193	,008	,088	,108	,196	,147	,047	,278	,220	,004	,055	,174	,149	,033	-,153	,218	,094
Std. Error of Skewness		,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109	,109
Kurtosis		-,114	-,226	-,227	-,329	-,208	-,145	-,342	-,357	-,091	-,402	-,144	-,200	-,093	-,163	-,243	-,436	-,439	-,462	-,376	-,472
Std. Error of Kurtosis		,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218	,218
Range		1,06	,04	1,12	1,08	1,52	,05	1,50	1,59	1,46	,04	1,48	1,53	1,30	,04	1,29	1,29	1,38	,04	1,42	1,46
Minimum		-,53	-,02	-,63	-,58	-,76	-,02	-,92	-,90	-,73	-,02	-,74	-,77	-,65	-,02	-,75	-,73	-,63	-,02	-,73	-,80
Maximum		,53	,02	,49	,50	,76	,03	,58	,69	,73	,02	,74	,76	,65	,02	,54	,56	,75	,02	,69	,66
Sum		-1,47	-,08	-44,65	-45,97	-10,27	-,30	-85,57	-90,17	-5,68	-,01	-38,44	-39,43	-5,39	-,01	-59,05	-60,28	-5,53	-,12	-53,98	-56,38
Percentiles	10	-,2400	-,0100	-,3300	-,3400	-,2900	-,0100	-,5000	-,5500	-,3300	-,0100	-,4190	-,4590	-,3000	-,0100	-,4190	-,4390	-,3800	-,0100	-,4890	-,4990
	20	-,1200	-,0100	-,2500	-,2600	-,2900	-,0100	-,4100	-,4200	-,2000	-,0100	-,3200	-,3300	-,2200	-,0100	-,3200	-,3400	-,2500	-,0100	-,3400	-,3600
	30	-,1200	,0000	-,2000	-,2100	-,1800	-,0100	-,3200	-,3400	-,2000	-,0100	-,2300	-,2470	-,1300	,0000	-,2500	-,2600	-,1300	-,0070	-,2700	-,2800
	40	-,0600	,0000	-,1400	-,1500	-,0600	,0000	-,2500	-,2700	-,0700	,0000	-,1600	-,1700	-,0400	,0000	-,1900	-,2000	-,1300	,0000	-,1900	-,1700
	50	,0000	,0000	-,0900	-,1000	-,0600	,0000	-,1800	-,1900	-,0700	,0000	-,1000	-,1000	-,0400	,0000	-,1300	-,1300	,0000	,0000	-,1200	-,1200
	60	,0600	,0000	-,0500	-,0500	,0600	,0000	-,1000	-,1200	,0700	,0000	-,0300	-,0100	,0400	,0000	-,0700	-,0600	,0000	,0000	-,0500	-,0500
	70	,0600	,0000	,0100	,0100	,0600	,0000	-,0200	-,0230	,0700	,0000	,0770	,0700	,1300	,0000	,0000	,0100	,1300	,0100	,0300	,0570
	80	,1200	,0000	,0800	,0800	,1800	,0100	,0680	,0900	,2000	,0100	,1680	,1800	,1300	,0100	,0600	,0900	,2500	,0100	,1500	,1500
	90	,2400	,0100	,1700	,1800	,2900	,0100	,1700	,1700	,3300	,0100	,2900	,2990	,3000	,0100	,2690	,2300	,3800	,0100	,2590	,2500

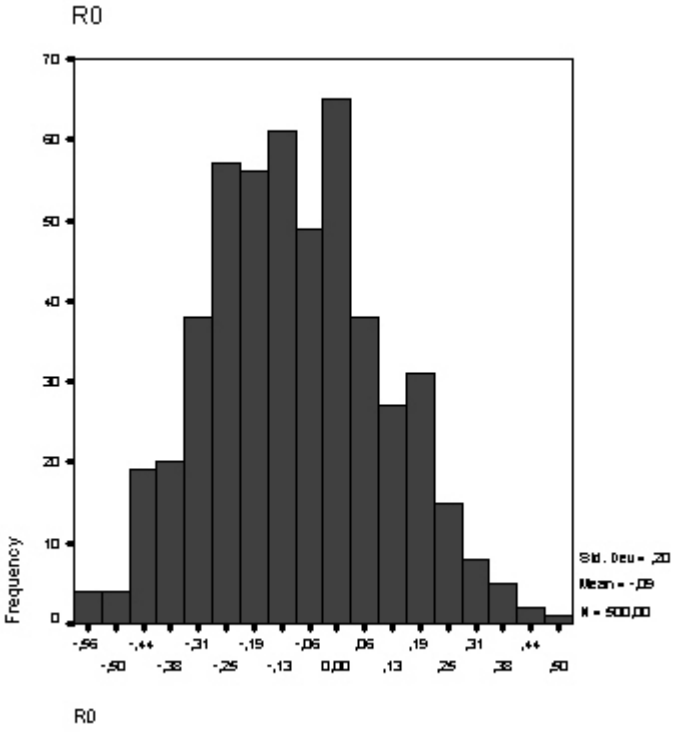
a Multiple modes exist. The smallest value is shown

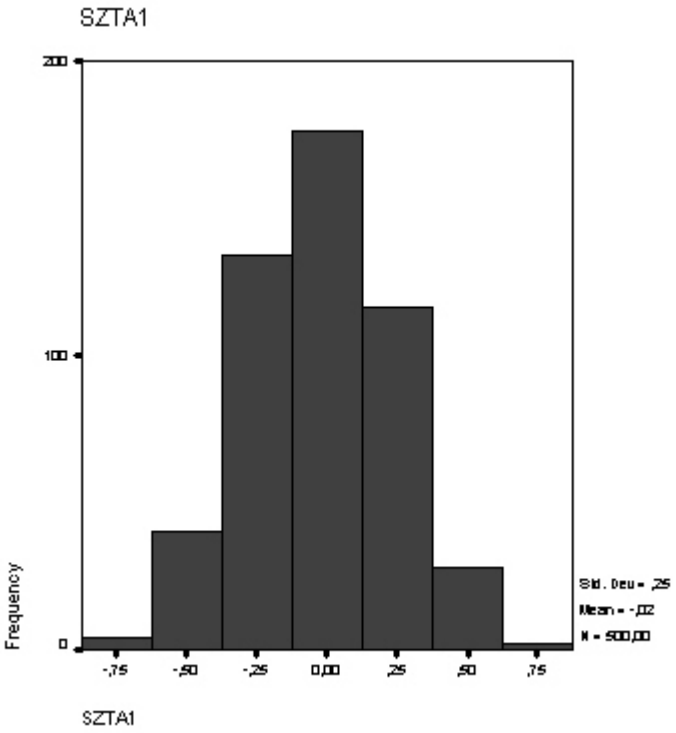
IX.5. Hisztogramok

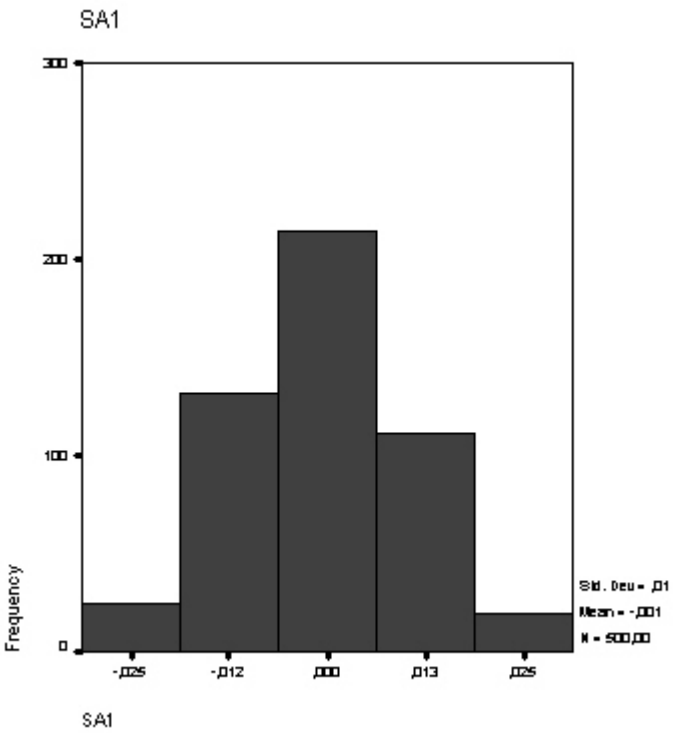


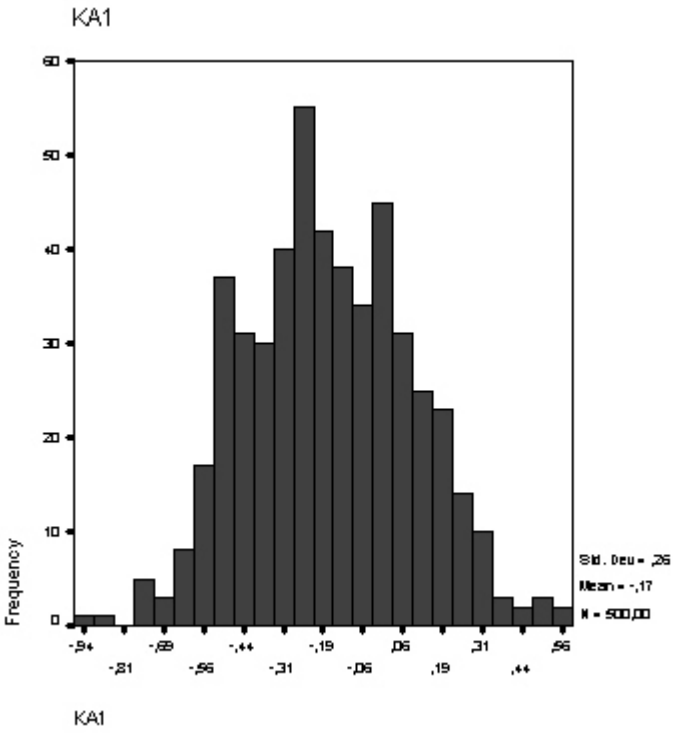


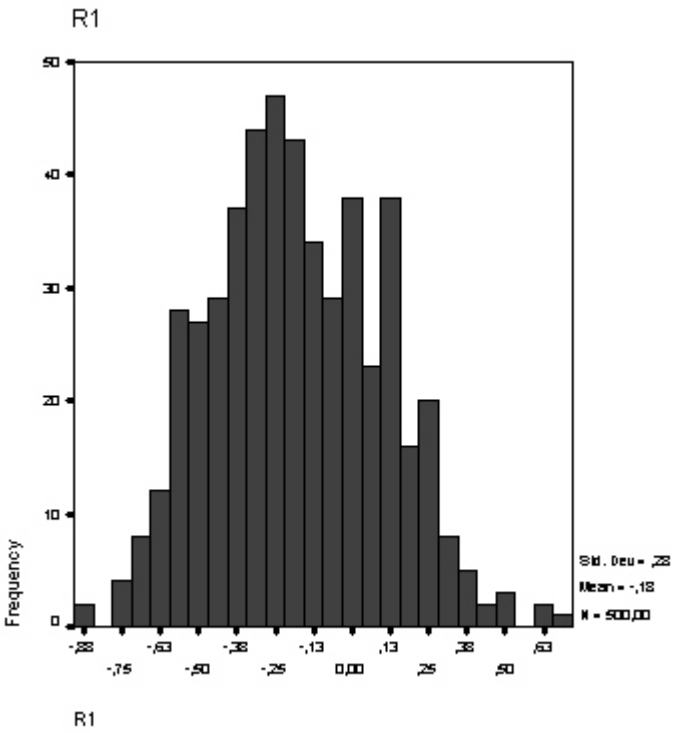

KA0
Frequency
Std. Dev = ,19
Mean = -,09
N = 500,00
KA0

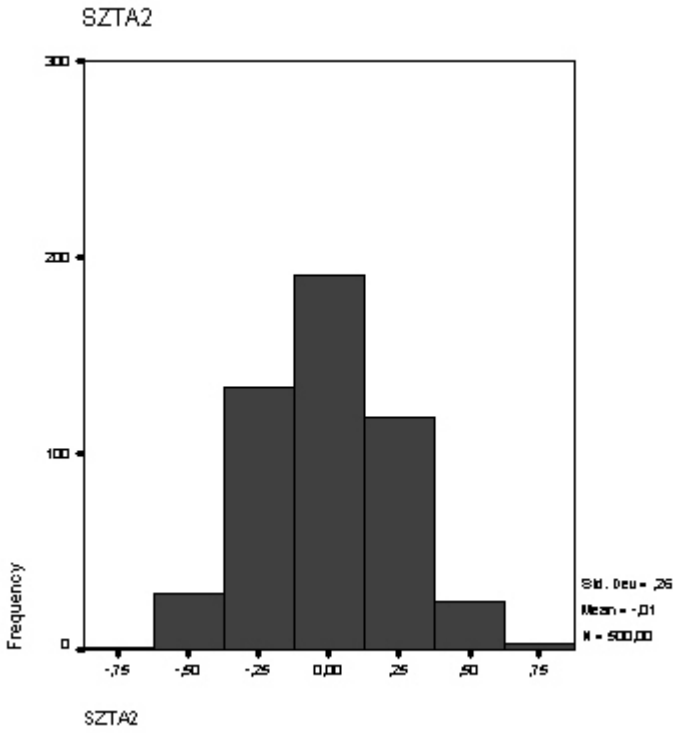

R0
Frequency
Std. Dev = ,20
Mean = -,09
N = 500,00
R0

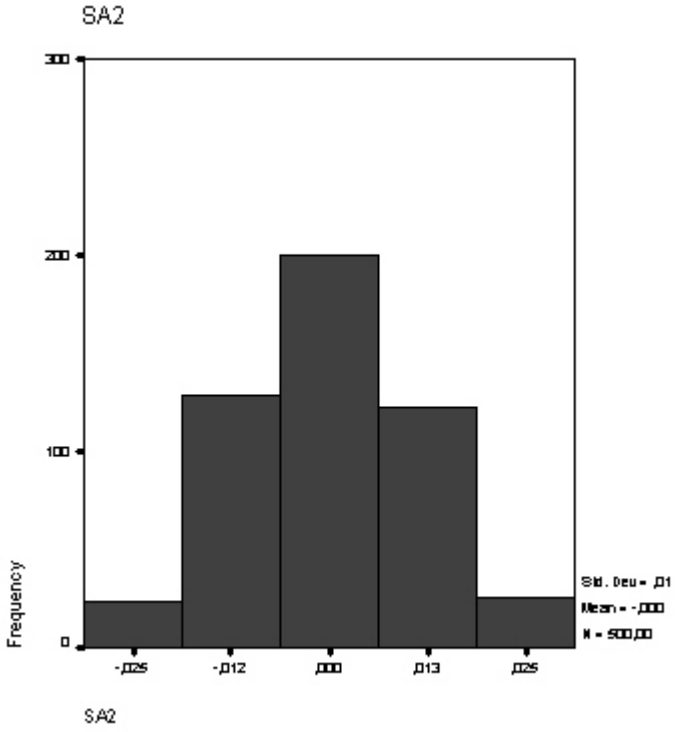

SZTA1
200
100
0
Frequency
Std. Dev = ,25
Mean = -,02
N = 500,00
-,75
-,50
-,25
0,00
,25
,50
,75
SZTA1

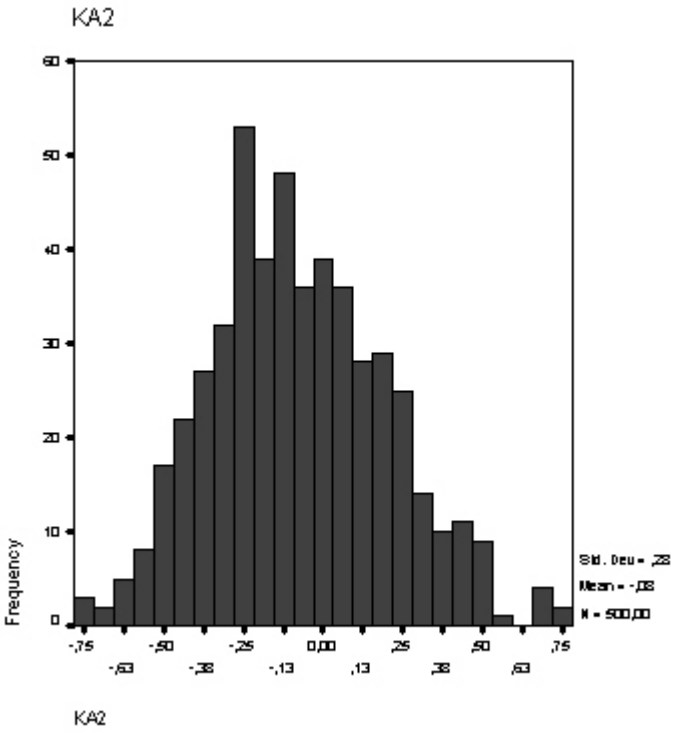

SA1
300
200
100
0
Frequency
Std. Dev = ,01
Mean = -,001
N = 500,00
-,025
-,012
,000
,013
,025
SA1

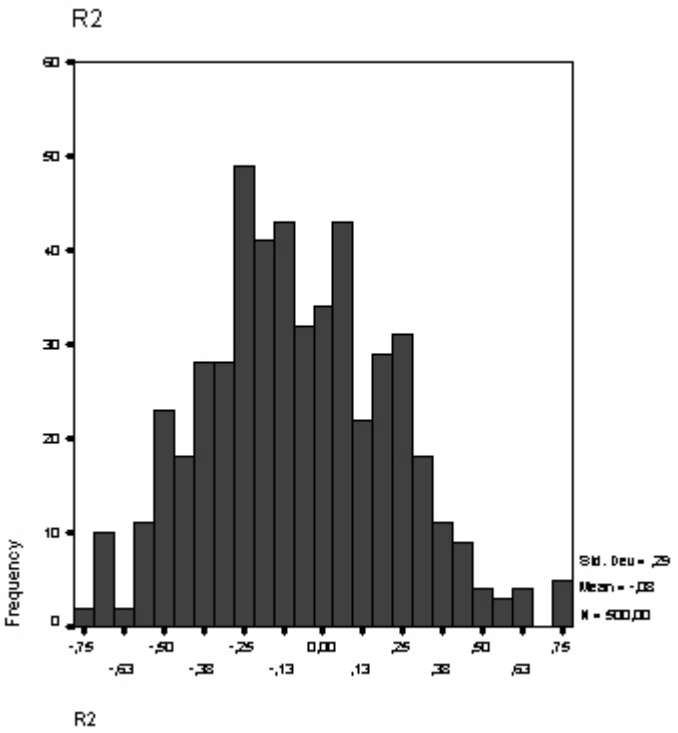

KA1
Frequency
Std. Dev = ,26
Mean = -,17
N = 500,00
KA1

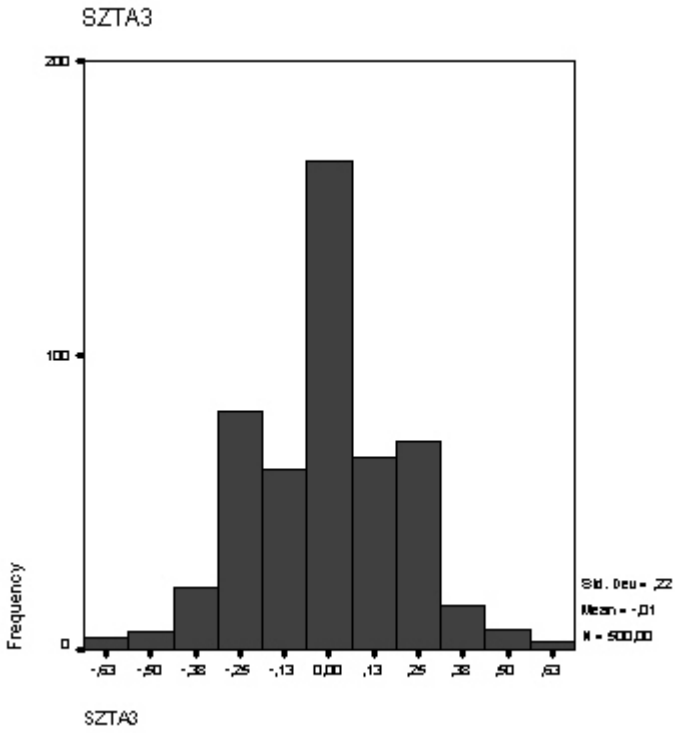

R1
Frequency
Std. Dev = ,28
Mean = -,18
N = 500,00
R1

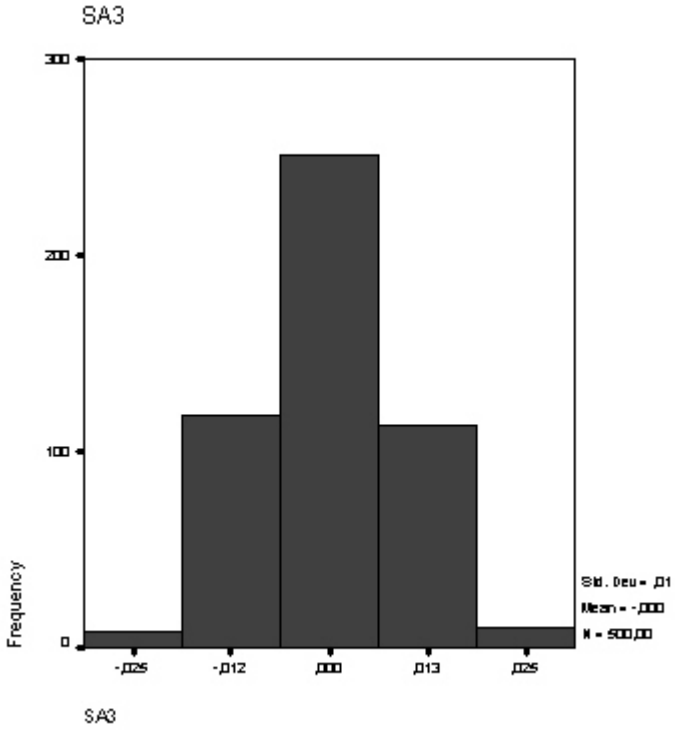

SZTA2
300
200
100
0
Frequency
Std. Dev = ,26
Mean = -,01
N = 500,00
-,75
-,50
-,25
0,00
,25
,50
,75
SZTA2

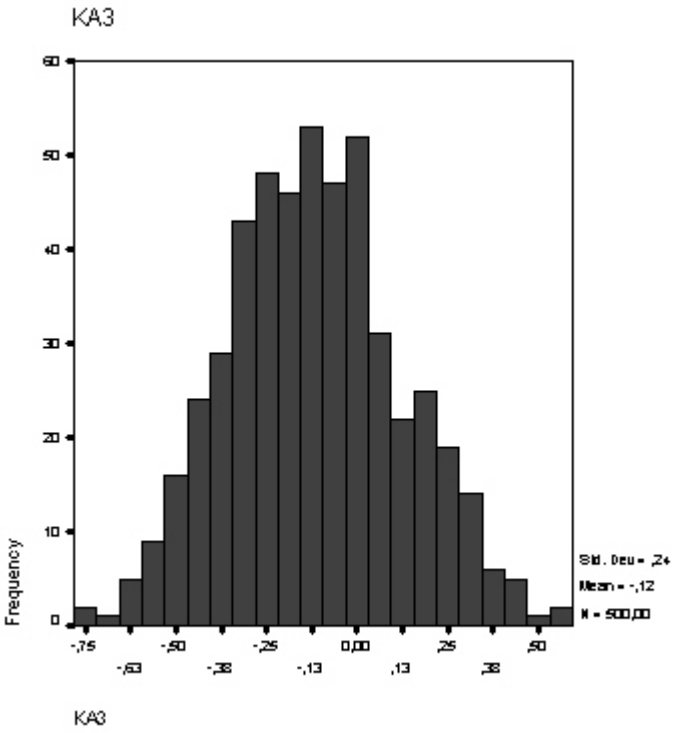

SA2
300
200
100
0
Frequency
Std. Dev = ,01
Mean = -,000
N = 500,00
-,025
-,012
,000
,013
,025
SA2

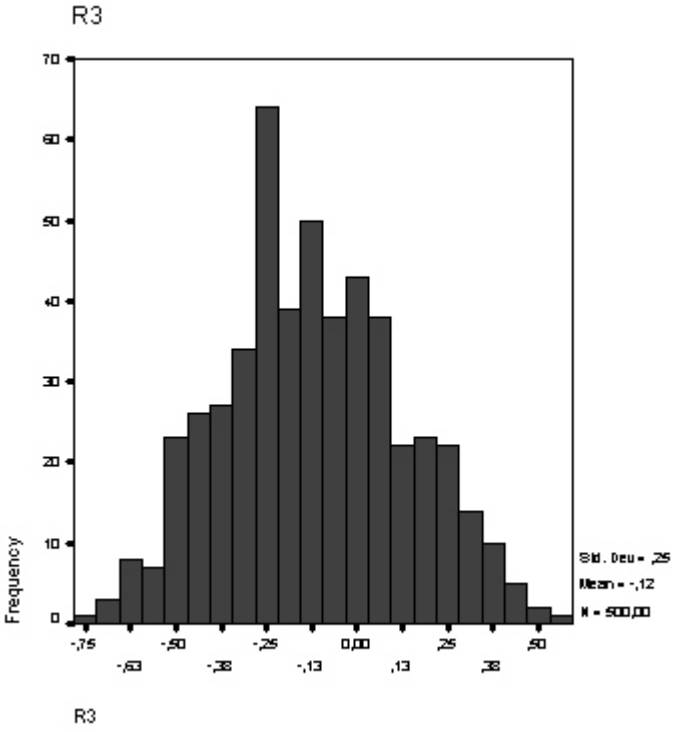

KA2
Frequency
Std. Dev = ,28
Mean = -,08
N = 500,00
KA2

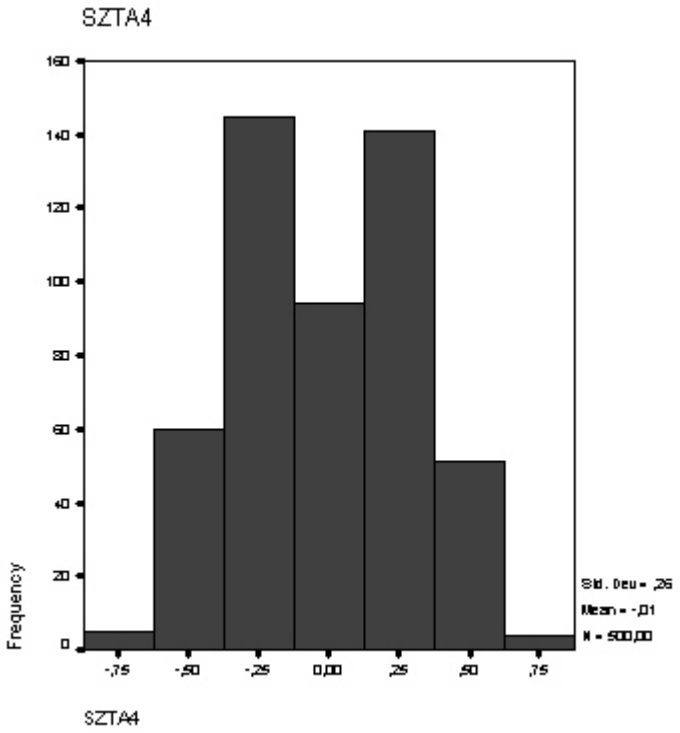

R2
Frequency
Std. Dev = ,29
Mean = -,08
N = 500,00
R2

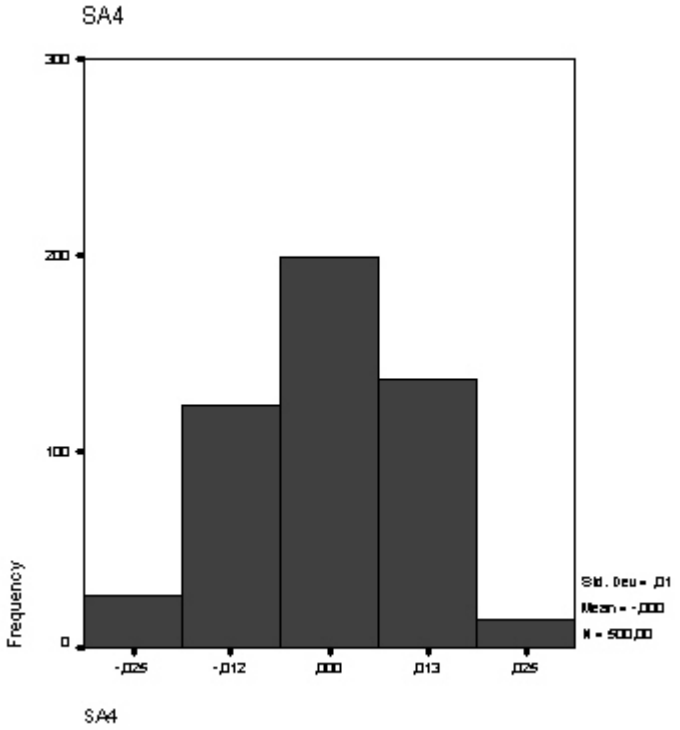

SZTA3
200
100
0
Frequency
Std. Dev = ,22
Mean = -,01
N = 500,00
-,63
-,50
-,38
-,25
-,13
0,00
,13
,25
,38
,50
,63
SZTA3

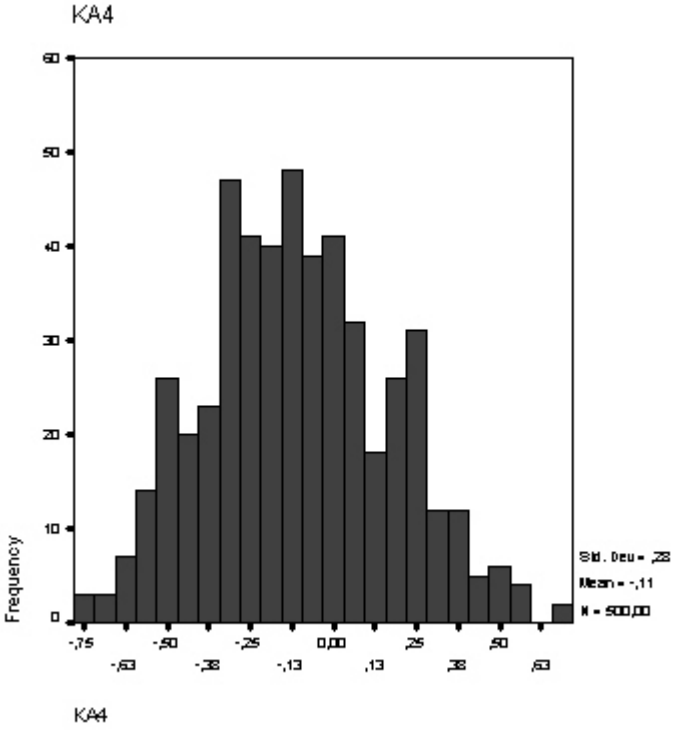

SA3
300
200
100
0
Frequency
Std. Dev = ,01
Mean = -,000
N = 500,00
-,025
-,012
,000
,013
,025
SA3

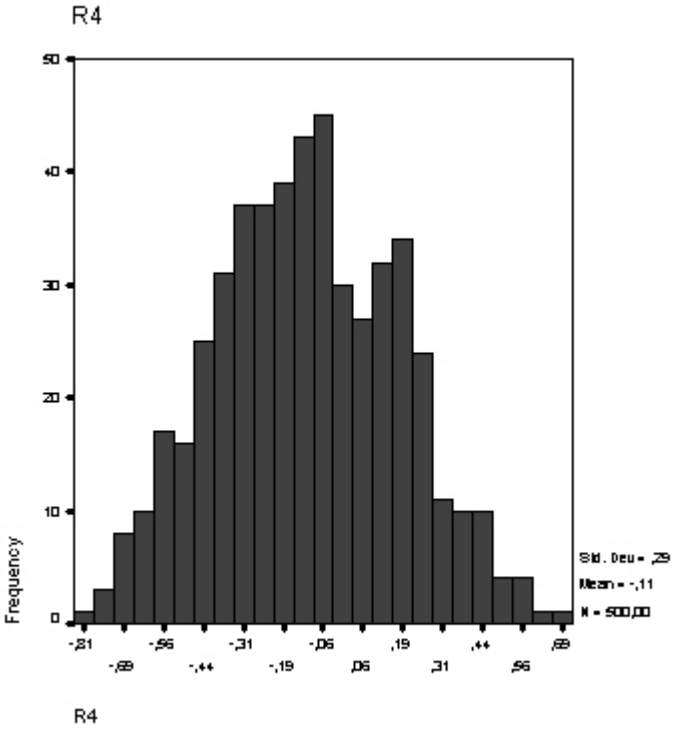

KA3
Frequency
Std. Dev = ,24
Mean = -,12
N = 500,00
KA3


R3
Frequency
Std. Dev = ,25
Mean = -,12
N = 500,00
R3


SZTA4
Frequency
Std. Dev = ,26
Mean = -,01
N = 500,00
SZTA4


SA4
Frequency
Std. Dev = ,01
Mean = -,000
N = 500,00
SA4


KA4
Frequency
Std. Dev = ,28
Mean = -,11
N = 500,00
KA4


R4
Frequency
Std. Dev = ,29
Mean = -,11
N = 500,00
R4

Hivatkozások

Könyvek, monográfiák:

1. Albrecht, Karl G. [1987]: BrainPower. Prentice-Hall, New York.
2. Borda József [2001]: Irányítás és informatika. Információrendszerek ellenőrzése. Saldo, Budapest.
3. Cangemi, Michael P. – Singleton, Tommie [2003]: Managing the Audit Function – A Corporate Audit Department Procedure. 3rd edition. John Wiley & Sons, New York.
4. Champlain, J. [2002]: Practical IT Auditing. Second Edition, Warren, Glorham & Lamont, Boston.
5. Edwards, W. – Newman, J.R. [1982]: Multiattribute Evaluation. Sage Publications, Beverly Hills.
6. Gallegos, Frederick – Allen-Senft, Sandra – Manson, Daniel P. [1999]: Information Technology Control and Audit. Auerbach/CRC Press, New York.
7. Golden, B.L. – Harker, P. T. – Wasil, E. A. [1989]: The Analytic Hierarchy Process – Applications and Studies. Springer-Verlag, New York.
8. Haimes, Yacov [1998]: Risk modeling, assessment and management. Wiley & Sons, New York.
9. Hwang, C. L. – Yoon, K. P. [1995]: Multiple Attribute Decision Making. Sage Publications, Beverly Hills.
10. Kő Andrea [2003]: Információrendszerek auditálása. BKÁE, Budapest.
11. Ködmön József [1999]: Kriptográfia – az informatikai biztonság alapjai. Computerbooks, Budapest.
12. Longman [1995]: Longman Dicitionary of Contemporary English. 3rd Pkg Edition, Pearson P T R.
13. MÉK [2003]: Pusztai Ferenc (főszerk.): Magyar Értelmező Kéziszótár. Akadémiai Kiadó, Budapest.
14. Nyikos László [2000]: Közpénzek ellenőrzése. Perfekt, Budapest.
15. Robertson, Jack C. – Davis, Frederick G. [1988]: Auditing. Fifth Edition, Business Publications, Plano.
16. Saaty, Thomas L. [1980]: The Analytic Hierarchy Process. McGraw-Hill, New York.
17. Weber, Ron [1999]: Information Systems Control and Audit. Prentice Hall, New York.

18. Zeleny, Milan [1982]: Multiple Criteria Decision Making. McGraw-Hill, New York.

Folyóiratcikkek:

19. Alles, Michael G. – Kogan, Alexander – Vasarhelyi, Miklos A. [2004]: Restoring auditor credibility – tertiary monitoring and logging of continuous assurance systems. International Journal of Accounting Information Systems, Vol. 5, Issue 2, pp. 183-202.

20. Asare, Stephen – Cohen, Jeffrey – Trompeter, Greg [2005]: The effect of non-audit services on client risk, acceptance and staffing decisions. Journal of Accounting and Public Policy, Volume 24, Issue 6, pp. 489-520.

21. Ashenden, Debi [2005]: Looking out into a world of threat. Computer Fraud & Security, Vol. 2005, Issue 3, pp. 13-15.

22. Bedford, Tim – Cooke, Roger [1999]: A new generic model for applying MAUT. European Journal of Operational Research, Vol. 118, pp. 589-604.

23. Borcherding, K. – Eppel, T. – Winterfeldt, D. von [1991]: Comparison of weighting judgements in multiattribute utility measurement. Management Science, Vol. 37., pp. 1603-1639.

24. Boritz, J. Efrim [2005]: IS practitioners' views on core concepts of information integrity. International Journal of Accounting Information Systems, Vol. 6, Issue 4, pp. 260-279.

25. Brown, R. Gene [1962]: Changing audit objectives and techniques. Accounting Review, Vol. 37, Issue 4, pp. 696-704.

26. Brown, William – Nasuti, Frank [2005]: Sarbanes-Oxley and Enterprise Security: IT Governance – What It Takes to Get the Job Done. Information Systems Security, Vol. 14, Issue 5, pp. 15-28.

27. Brugha, Cathal M. [2004]: Phased multicriteria preference finding. European Journal of Operational Research, Vol. 158, Issue 2, pp. 308-316.

28. Charette, Robert N. [1996]: The mechanics of managing IT risk. Journal of Information Technology, Vol. 11, pp. 373-378.

29. Ciechanowicz, Zbigniew [1997]: Risk analysis – Requirements, conflicts and problems. Computers & Security, Vol. 16, Issue 3, pp. 223-232.

30. Coles, Robert S. – Moulton, Rolf [2003]: Operationalizing IT risk management. Computers and Security, Vol. 22, Issue 6, pp. 487-493.

31. Covert, Edwin – Nielsen, Fran [2005]: Measuring Risk Using Existing Frameworks. Information Systems Security, Vol. 14, Issue 1, pp. 21-25.

32. Crockett, Margaret – Foster, Janet [2004]: Using ISO 15489 as an Audit Tool. Information Management Journal, Vol. 38, Issue 4, pp. 46-53.

33. Damianides, Marios [2004]: How does SOX change IT? Journal of Corporate Accounting & Finance, Vol. 15, Issue 6, pp. 35-41.

34. Dennis, Anita [2004]: Taking Account of History. Journal of Accountancy, Vol. 197, Issue 5, pp. 84-86.

35. Dickie, John [1997]: The changing face of security – Planning an IT system. Computer Audit Update, Vol. 1997, Issue 4, pp. 19-24.

36. Dilla, William N. – Stone, Dan N. [1997]: Response scales in risk judgments – The effects of representation, fineness and user choice. Journal of Information Systems, Vol. 11, Issue 2, pp. 75-96.

37. Dodds, Rupert – Hague, Ian [2004]: Information security – more than an IT issue? Chartered Accountants Journal, Vol. 83, Issue 11, pp. 56-57.

38. Dull, Richard B. – Tegarden, David P. [2004]: Using control charts to monitor financial reporting of public companies. International Journal of Accounting Information Systems, Vol. 5, Issue 2, pp. 109-127.

39. Dyer, J. S. – Fishburn, P. C. – Steuer, R. E. – Wallenius, J. – Zionts, S. [1992]: Multiple Criteria Decision Making, Multiattribute Utility Theory – The Next Ten Years. Management Science, Vol. 38., Issue 5

40. Fagin, Ronald – Wimmers, Edward L. [2000]: A formula for incorporating weights into scoring rules. Theoretical Computer Science. Vol. 209, pp. 309-338.

41. Flesher, Dale L. – Previts, Gary John – Samson, William D. [2005]: Auditing in the United States – a historical perspective. Abacus, Vol. 41, Issue 1, pp. 21-39.

42. Flowerday, Stephen – Solms, Rossouw von [2005]: Continuous auditing – verifying information integrity and providing assurances for financial reports. Computer Fraud & Security, Vol. 2005, Issue 7, pp. 12-16.

43. Forman, Ernest H. [1993]: Facts and fictions about the analytic hierarchy process. Mathematical and Computer Modelling, Vol. 17, Issues 4-5, pp. 19-26.

44. Friedland, Norman [2002]: Audit History – How We Got To Enron. Corporate Board, Vol. 23, Issue 134, pp. 9-13.

45. Hale, John C. – Landry, Timothy D. – Wood, Charles M. [2004]: Susceptibility audits – A tool for safeguarding information assets. Business Horizons, Vol. 47, Issue 3, pp. 59-66.

46. Henning, Ronda R. [2005]: Designing for Disaster – Building Survivable Information Systems. The Journal of Defense Software Engineering, Vol. Oct., pp. 6-10.

47. Hermanson, Dana R. – Hill, Mary Callahan – Ivancevich, Daniel M. [2000]: Information Technology-Related Activities of Internal Auditors. Journal of Information Systems, Vol. 14, pp. 39-53.

48. Hilary, Gilles – Lennox, Clive [2005]: The credibility of self-regulation: Evidence from the accounting profession's peer review program. Journal of Accounting and Economics, Vol. 40, Issues 1-3, pp. 211-229.

49. Hwang, Sung-Sik – Shin, Taeksoo – Han, Ingoo [2004]: CRAS-CBR – Internal control risk assessment system using case-based reasoning. Expert Systems, Vol. 21, Issue 1, pp. 22-33.

50. Karabacaka, Bilge – Sogukpinar, Ibrahim [2005]: ISRAM – information security risk analysis method. Computers & Security, Vol. 24, Issue 2, pp. 147-159

51. Lainhart IV, John W. [2000]: COBIT – A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities. Journal of Information Systems, Vol. 14, Issue 1, pp21-26.

52. Laliberte, Scott [2004]: Risk Assessment for IT Security. Bank Accounting & Finance, Vol. 17, Issue 5, pp. 38-42.

53. Leem, Choon Seong –Lee, Hong Joo [2004]: Development of certification and audit processes of application service provider for IT outsourcing. Technovation, Vol. 24, Issue 1, pp. 63-71.

54. Lenstra, Arjen – Voss, Tim [2004]: Information Security Risk Assessment, Aggregation, and Mitigation. Lecture Notes in Computer Science, Vol. 3108, pp. 391 – 401.

55. Liu, Fang – Dai, Kui – Wang, Zhiying – Ma, Jun [2005]: Research on Fuzzy Group Decision Making in Security Risk Assessment. Lecture Notes in Computer Science, Vol. 3421, pp. 1114 – 1121.

56. Lord, Alan T. [2004]: ISACA model curricula 2004. International Journal of Accounting Information Systems, Vol. 5, Issue 2, pp. 251-265.

57. Macartney, Leslie [2004]: CISA and CISM – Internationally Recognized for Future Success. Certification Magazine, Issue Dec., pp. 34-35.

58. Morency, John [2005]: Best practice, practice, practice. Network World, Vol. 22, Issue 1, p. 37.

59. Murthy, Uday S. – Groomer, Michael [2004]: A continuous auditing web services model for XML-based accounting systems. International Journal of Accounting Information Systems, Vol. 5, Issue 2, pp. 139-163.

60. Nolan, Richard – McFarlan, F. Warren [2005]: Information Technology and the Board of Directors. Harvard Business Review, Vol. 83, Issue 10, pp. 96-106.

61. Olson, Eric G. [2005]: Strategically managing risk in the information age – a holistic approach. Journal of Business Strategy, Vol. 26, Issue 6, pp. 45-54.

62. Ozier, Will [2003a]: Introduction to Information Security and Risk Management. IT Audit, Vol. 6.

63. Ozier, Will [2003b]: Risk Metrics Needed for IT Security. IT Audit, Vol. 6.

64. Parker, Xenia Ley [2001]: Understanding Risk. Internal Auditor, Feb2001, Vol. 58, Issue 1, pp. 61-65.

65. Rezaee, Zabihollah [2005]: Causes, consequences, and deterence of financial statement fraud. Critical Perspectives on Accounting, Vol. 16, Issue 3, pp. 277-298.

66. Saaty, Thomas L. [1989]: Decision Making, Scaling, and Number Crunching. Decision Sciences, Vol. 20., Issue 2.

67. Schmidt, Chris [2005]: The Driver's View. Internal Auditor, Vol. 62, Issue 3, pp. 29-32.

68. Smith, E. – Eloff, J. H. P. [2002]: A Prototype for Assessing Information. Technology Risks in Health Care. Computers & Security, Vol. 21, Issue 3, pp. 266-284.

69. Solms, Basie von [2005]: Information Security governance – COBIT or ISO 17799 or both? Computers & Security, Vol. 24, Issue 2, pp. 99-104.

70. Stewart, Andrew [2004]: On risk – perception and direction. Computers & Security, Vol. 23, Issue 5, pp. 362-370.

71. Stoffel, Laurent [2002]: Risk Assessment. Computer Fraud & Security, Vol. 2002, Issue 8, pp. 17-19.

72. Tregear, Jonathan [2001]: Risk Assessment. Information Security Technical Report, Vol. 6, Issue 3, pp. 19-27.

73. Trites, Gerald [2004]: Director responsibility for IT governance. International Journal of Accounting Information Systems, Vol. 5, Issue 2, pp. 89-99.

74. Turley, James S. [2004]: Get Ready for the EU's 8th Directive. Directorship, Vol. 30, Issue 6., pp. 18-21.

75. Vendrzyk, Valaria P. – Bagranoff, Nancy A. [2003]: The evolving role of IS audit – a field study comparing the perceptions of IS and financial auditors. Advances in Accounting, Vol. 20, pp. 141-163.

76. Vijayan, Jaikumar [2003]: IT Managers See Need for Risk Metrics. Computerworld, Vol. 37, Issue 23, pp. 1-2.

77. Vranceanu, Radu [2005]: Financial Architecture and Manager Dishonesty – Lessons from US Corporate Scandals. Acta Oeconomica, Vol. 55, Issue 1, pp. 1 – 22.

78. Vroom, Cheryl – Solms, Rossouw von [2004]: Towards information security behavioural compliance. Computers & Security, Vol. 23, Issue 3, pp. 191-198.

79. Wilson, Piers [2005]: Risk control – A technical view. Computer Fraud & Security, Vol. 2005, Issue 5, pp. 8-11.

80. Yoke, Chuck [2005]: For service management ITIL have to do. Network World, Vol. 22, Issue 27, p. 35.

Konferenciakötetek, egyéb publikációk:

81. Fan, Zhiping – Ma, Jin [1999]: An Approach to Multiple Attribute Decision Making Based on Incomplete Information on Alternatives. in: Proceedings of the 32nd Hawaii International Conference on System Sciences, pp. 1-5.

82. GAO [1999]: Information Security Risk Assessment – Practices of Leading Organizations. GAO Reports AIMD-00-33, Washington, 50p.

83. ITGI [2004]: IT Governance Institute: COBIT Mapping – Overview of International IT Guidance. IT Governance Institute, Rolling Meadows.

84. Jelen, George [2000]: SSE-CMM Security Metrics. NIST and CSSPAB Workshop, Washington http://csrc.nist.gov/csspab/june13-15/jelen.pdf 2004.07.08.

85. MTA-ITA [2000]: MTA Információtechnológia Alapítvány: Angol-magyar fogalomjegyzék az információrendszer ellenőrzéshez. http://www.mtaita.hu/Audit_Concepts_Translation.pdf 2003.10.05.

86. Nyikos László – Kresalek Péter [2003]: Könyvvizsgálat – Ellenőrzés. ÁSZ-FEMI tanulmány, T33, Budapest.

87. Saunders, John H. [1994]: A Comparison of Decision Accuracy in AHP and Point Allocation. in: Proceddings of the Third International Symposium on the Analytic Hierarchy Process. ISAHP, Washington, DC.

88. Saunders, John H. [2002]: A Dynamic Risk Model for Information Technology Security in a Critical Infrastructure Environment. in: Proceedings of the Conference on Risk Management in Water Resources, American Society of Civil Engineers, Santa Barbara.

89. Schmitt, C. et al. [2002]: The MAUT-Machine – An Adaptive Recommender System. in: ABIS-Workshop Proceedings, ABIS, Hannover, pp. 83-91.

90. Schreck, Franziska [2002]: Multi-criteria decision aid as a tool in the management of produced water in the offshore oil industry. TRITA-LWR Master Thesis, Royal Institute of Technology, Stockholm

91. Seyhan, Erhan [1999]: Multicriteria Decision Making – Methodology, Modeling Approaches, Solution Procedures. Thesis, EGE University, Izmir

92. Sudár Erika – Pető Dávid – Gábor András [2004]: Modeling the Penetration of the Information Society Paradigm. Lecture Notes in Artificial Intelligence 3035, pp. 185-193.

Szabványok, előírások és ajánlások:

93. 84/253/EEC [1984]: 84/253/EEC The Eighth Council Directive on the approval of persons responsible for carrying out the statutory audits of accounting documents. Council Directive, Brussels.

94. AS/NZS 4360:2004 [2004]: Standard Australia / New Zealand: AS/NZS 4360:2004 Risk management.

95. Basel [2004]: Basel Committee on Banking Supervision: International Convergence of Capital Measurement and Capital Standards. Bank For International Settlements, Basel.

96. BS 7738-1:1994 [1994] British Standard: BS 7738-1:1994 Specification for information systems products using SSADM (Structured Systems Analysis and Design Method). Implementation of SSADM version 4.

97. CC [1999]: CSE – SCSSI – BSII – NLNCSA – CESG – NIST – NSA: Common Criteria and Methodology for Information Technology Security Evaluation.

98. COBIT [2000a]: COBIT Framework. 3rd edition. IT Governance Institute, Rolling Meadows.

99. COBIT [2000b]: COBIT Management Guidelines. 3rd edition. IT Governance Institute, Rolling Meadows.

100. COBIT [2000c]: COBIT Control Objectives. 3rd edition. IT Governance Institute, Rolling Meadows.

101. COBIT [2000d]: Kontroll irányelvek. 3rd edition. magyar fordítás. http://www.ihm.gov.hu/data/25738/3Cobit-ContrObjectives.pdf 2003.05.07.

102. COSO [1992]: Committee of Sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework. COSO, Jersey City.

103. COSO [2004]: Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework. Executive Summary. COSO, Jersey City.

104. ISO 6592:2000 [2000] International Organization for Standardization: ISO 6592:2000 Information technology. Guidelines for the documentation of computer-based application systems.

105. ISO 9000-3 [1991]: International Organization for Standardization: ISO 9000-3 Quality Management and Quality Assurance Standards – Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software. ISO, Switzerland.

106. ISO TR 13334 [1996-2001]: International Organization for Standardization: ISO TR 13334 Information Technology – Guidelines for the Management of IT Security. ISO, Switzerland.

107. ISO/IEC 12207 [1995] International Organization for Standardization – International Electrotechnical Commission: ISO/IEC 12207 Information Technology – Software life cycle processes.

108. ISO/IEC 15408 [1999]: International Organization for Standardization – International Electrotechnical Commission: ISO/IEC 15408 Evaluation Criteria for Information Technology Security.

109. ISO/IEC 17799 [2000]: International Organization for Standardization – International Electrotechnical Commission: ISO/IEC 17799 Code of Practice for Information Security Management.

110. ISO/IEC TR 15504-5:1999 [1999] International Organization for Standardization – International Electrotechnical Commission: BS ISO/IEC TR 15504-5:1999 Information technology. Software process assessment. An assessment model and indicator guidance.

111. ITB [1994a]: Informatikai Tárcaközi Bizottság: Informatikai biztonsági módszertani kézikönyv 8. sz. ajánlás. ITB, Budapest, http://www.itb.hu/ajanlasok/a8

112. ITB [1994b]: Informatikai Tárcaközi Bizottság: Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás. ITB, Budapest, http://www.itb.hu/ajanlasok/a12 2003.10.10.

113. ITIL [1989]: British Office of Government Commerce: IT Infrastructure Library (ITIL). Central Computer and Telecommunications Agency (CCTA), London.

114. MSZ ISO/IEC 9126:2000 [2000]: Magyar Szabvány: MSZ ISO/IEC 9126:2000 Informatika. Szoftvertermékek értékelése. Minőségi jellemzők és használatuk irányelvei.

115. NIST [1996]: National Institute of Standards and Technology (NIST): Generally Accepted Principles and Practices for Securing Information Technology Systems. Special Publication 800-14, USA.

116. TickIT [1994]: British Department of Trade and Industry: TickIT Guide to Software Quality Management System Construction and Certification. DTI, London.

Weboldalak:

117. BS7799 [2004]: http://www.bs7799-iso17799.com 2004.10.10.

118. CRAMM [2004]: http://www.gammassl.co.uk/topics/hot5.html 2004.10.02.

119. HSOR [2004]: http://www.hsor.org/what_is_or.cfm?name=mutli-attribute_utility_theory 2004.08.10.

120. Micksch, Allan [2000]: Information systems risk analysis, assessment and management. SANS Institute, http://www.sans.org/infosecFAQ/policy/risk.htm 2004.07.20.

121. Wikipedia [2004]: http://en.wikipedia.org/wiki/Risk_assessment 2004.07.24.