**Óbudai Egyetem**

Doktori (PhD) értekezés
tézisfüzete

# Supporting Enterprise Governance on IT Security Bases
# Vállalatok kormányzásának támogatása informatikai biztonsági módszerekkel

Dr. Szenes Katalin

Témavezető:
Dr. Hermann Gyula

**Alkalmazott Informatikai Doktori Iskola**

Budapest, 2014. február

## I. A kutatás előzményei

Az IT auditot, informatikai biztonságot támogató COBIT-nak, az ISACA módszertanának, de tankönyveinek, és az ISO ide tartozó szabványainak és irányelveinek is deklarált célja, hogy támogassák, az informatikai szolgáltatás javításával, az informatika vállalati irányítását [CRM, COBIT 1998, COBIT 2000, COBIT 4.0 - 2005, COBIT Map - 2006, COBIT 4.1 - 2007, COBIT 5 - 2010, 11, 12], [ISO G73, 27001, 27002, 27005, 38500, 27000, 12207]. Itt ISACA az Information Systems Audit and Control Association-t rövidíti, ennek módszertana a COBIT = Control OBjectives for Information Technology, az ISACA-képesítésére pályázó informatikai ellenőrök vizsgafelkészítő tankönyve pedig a CRM = CISA Review Manual. ISO az International Standard Organization rövidítése.

A javasolt célok, és az ezeket támogató intézkedések nagyrésze, de többnyire ezek hatóköre is az informatika szakterületén belül marad. Mégha az intézmény stratégiai céljai szerepelnek is valahol, ott is az IT-nek adnak feladatot. Tapasztalataim alapján érdemes kiterjeszteni e módszerek tanulságait a többi szakterületre, sőt, a legfelső vezetésre is, átfogva így az intézmény teljes működését [12, 15]. A fordított kapcsolatokkal, a stratégia közvetlen informatikai biztonsági felhasználásával a fentemlített ISACA és ISO anyagok nem foglalkoznak, pedig a stratégiai alapokkal igazolt biztonsági célokat, különösen, ha azok az intézmény működését is javítják, könnyebb elfogadtatni [16].

A legjobb szakmai gyakorlat közvetítésének jelentős a tradícionális hagyománya. Az ISACA hét információkritériumot jelölt meg, ezek a rendelkezésre állás, bizalmasság, sértetlenség, célra vezetés, hatékonyság, a szabályozási követelményeknek való megfelelés és a megbízhatóság [CRM, COBIT]. Ebből az első három ISO alapkövetelmény is - az informatikai szolgáltatások minőségéhez tűznek ki célt [ISO 27000, 27001]. Részben ezek feldolgozása, részben mindennapi tapasztalataim segítettek egy általánosabb, és sokkal bővebb, a vállalat irányítását, működését is jellemző kiválósági kritériumrendszerem megfogalmazásához [14, 15].

A jelenlegi ISACA és ISO "legjobb szakmai gyakorlat" defenzív, a fókuszban a hibák javítása, és következményeik orvoslása áll. Ehelyett egy proaktív, a statégiai célok támogatásából kiinduló, a kockázatokat a működés javítását támogató célokkal kezelő módszertan viszont közvetlenül szolgálhatja az intézmény boldogulását [6, 9, 14].

Mind az ISACA módszertana, tankönyvei, mind az ISO szabványok és irányelvek helyenként következetlenek, hiányosak, sőt, néha ellentmondásosak is. Ezt dolgozatomban részletesen elemzem. Amikor már megjelentek a COBIT 5-ön végzett munkánk első végleges eredményei, akkor derült ki, hogy a projekt vezetői úgy döntöttek, kihagyják belőle az ellenőrzési cél

fogalmát [COBIT 5, 2012]. A COBIT 5 Subject Matter Expert Team tagjaként olyan részletfeladatokat kellett ellátnom, amelyekből ez a tendencia nem derült ki.

Nyíltan vállalták, hogy összecsúszott a cél az intézkedéssel, a "mit" és a "hogyan" [Guldentops, 2012]. Ennek több oka is lehetett. Fontosnak tartom a "control - kontroll" szó pontatlan alkalmazását, ami általában intézkedést jelentett, de néha célt is. Ez ellen többször is felléptem javítási javaslataimban, hiába [CRM]. Azt sem sikerült kiemeltetni, hogy az ellenőrzési cél nem az ellenőr, hanem az intézmény célja, az ellenőrzési intézkedéssel kapcsolatos legfontosabb szerepköröket sem neki kell ellátnia. Ez is csökkenthette az ellenőrzési cél jelentőségét, legalábbis egyes szakértők szemében.

Sok specifikus célt, például információk gyűjtését, elemzését szolgáló biztonsági eszköz áll ma már rendelkezésre. Olyan eszközt azonban nem láttam, ami tapasztalatok, tanácsok gyűjtését, visszakeresését, köztük kapcsolatok feltárását támogatja, ráadásul úgy, hogy ezeket a "recepteket" számítástechnikai ismeretek nélkül is meg lehessen fogalmazni, és fel is lehessen használni. Tehát akár a legfelső vezetés, az üzleti szakterület, és az olyan támogató szakterületek is használhatnák, mint a HR, pénzügy, stb. Ezért érdemesnek látszott elővenni régi, először robotok gondolkodásának támogatására, majd párhuzamos és konkurrens folyamatokból álló rendszerek működését modellező, a mesterséges intelligencia egyes eredményeit is felhasználó szakértői rendszeremet. Ez nem igényel bonyolult leírásokat, fel tudja dolgozni a feltételekhez kötött célokból összeállított recepteket, és ezek alternatíváit [1, 3, 4, 5, 7]. Tehát szakértői rendszerre van szükség.

Ezért indultam ki párhuzamos és konkurrens folyamatok együttműködésének tervezésére és szimulációjára az 1980-as évek elejétől fejlesztett módszertanomból, a PCUBE-ból. PCUBE = P3 - Planning Parallel and Concurrent Process Systems. Ezt kezdtem biztonsági problémák reprezentálására használni, ezért neveztem el módszertanomat PCUBE-SEC-nek (a "SECurity" szót felhasználva) .

## II. Célkitűzések

Az ISACA és az ISO anyagaiban ismertetett, ún. "legjobb szakmai gyakorlat" követése hozzájárulhat ahhoz, hogy egy cég elégedett legyen saját belső informatikai szolgáltatásával. Sajnos, ezek a szakmai anyagok csak véletlenszerűen utalnak arra, hogy ehhez nemcsak az IT erőforrásaira, munkatársaira van szükség, hanem az üzleti, vagy a támogató szakterületekére is [CRM, COBIT], [ISO G73, 38500]. Célom, hogy tisztázzam ezt a következetlenséget, és bemutassam, hogyan pontosítható, hogy ki, mivel járulhat hozzá, nemcsak az informatikai,

hanem a többi szakterület szolgáltatásainak javításához is. Ehhez három dimenziót kell elhatárolni: az intézkedések tárgyát, az intézkedő szerepkört illetve szakterületet, és a működésnek azt a területét, ahol a javítandó probléma van. Az intézkedő és a javítandó terület egybe is eshet, de akkor ezt jelölni kell.

Célom, hogy a informatikai biztonságtól, ellenőrzéstől származó javaslatokat, akár az informatikára vonatkoznak, akár intézményi hatókörre, könnyebben el tudja fogadni a legfelső vezetés, és az üzleti szakterület is, akkor is, ha nincsenek számítástechnikai szakismereteik. Ehhez célszerűbb pozitívan hozzáállni a jelenlegi negatív, bajelhárító, illetve a bajok következményeit enyhítő megközelítés helyett. Legyen *az üzleti siker* a *deklarált* fókusz. Célom, hogy erre a proaktív, eleve a *stratégiai célok teljesítését* célzó megközelítésre segítsem áttérni módszertanom felhasználóit.

Annak érdekében pedig, hogy az informatikai biztonsági és ellenőrzési, sőt, az általánosítás után az intézmény működését megcélzó módszereket

- *közvetlenül* használhassuk ki a stratégia megvalósításában, és
- fordítva, azokat a szakmai részcélokat könnyebb legyen elfogadtatni a legfelső vezetéssel és az üzleti szakterületekkel, amelyeket az informatikai biztonsági, biztonsági és ellenőrzési szakértők éppen a vállalati célok érdekében szeretnének megvalósítani, bár közvetlenül "csak" a biztonságot javítják,

az informatikai kockázatok kezelésénél is, át kell térni az informatikai *problémák elhárításáról* az intézményi *célok szolgálatára*.

Emellett érdemes létrehozni egy *közvetlen, kölcsönös* kapcsolatot is az intézmények irányítása, és a már hiányosságoktól, ellentmondásoktól megtisztított, majd az informatika szintjéről az intézményi működésre kiterjesztett, e célból definiált, ún. *intézményi* biztonság között.

Mindezek feltétele, hogy kiigazítsuk az ismeretanyagot, feloldjuk ellentmondásait, tisztázzuk következetlenségeit, következetesen pontosítsuk a véletlenszerű utalásokat a stratégiai célokra, az ezek megvalósításában szereplő szervezetekre illetve szerepkörökre, és azokra a tevékenységekre, amelyeket érdemes végrehajtaniok ezeknek a célok érdekében. Első lépés az intézkedések céljának, és maguknak az intézkedéseknek, azaz a "*mit* akarunk elérni" és a "*hogyan* érjük el" szétválasztása. Ezek összecsúszása ugyanis, mint említettük, már súlyos következményekkel is járt [COBIT 5, 2012].

További fejlesztési lehetőségeket is célul tűztem ki a PCUBE-SEC felhasználók támogatására. A "mit" és "hogyan" tovább finomítható, részletezhető olyan dimenziókkal, amelyek kifejezik, "milyen területen" teszünk valamit, illetve "melyik terület" javul az adott tevékenységekkel. El kell választani a stratégiai célokat az *elérésükhöz szükséges* részcéloktól. Hangsúlyozni kell, hogy a részcélok, és az azokat szolgáló intézkedések, bár *szükségesek* ahhoz, hogy a legjobb szakmai gyakorlatot kövessük, általában nem feltétlenül *elégségesek* a célok eléréséhez. Fontos, hogy deklaráltan elválasszuk egymástól a célok / intézkedések meghatározójának, engedélyezőjének, végrehajtójának, és a végrehajtás ellenőrzőjének szerepkörét illetve szakterületét. Célom mindezzel az, hogy követhető recepteket is adjak módszertanom felhasználójának.

Javasolok neki konkrét, a stratégiai célokat szolgáló részcélokat is. Ezt a kiválósági kritériumok rendszerének felállításával érem el. Ezek egy részét ki lehet alakítani az I. fejezetben említett, az informatikára vonatkozó ISO és ISACA követelményekből, hiányosságaikat kijavítva, majd kiterjesztve jellemzőiket az informatikáról az egész vállalati működésre [COBIT], [ISO 27000, 27001], [13, 14, 15, 16].

Annak érdekében, hogy

- mindezek alkalmazását bemutathassam, és
- az informatikai kockázatkezelési gyakorlatot is felválthassam egy elsősorban a stratégiai célokat szolgáló, és csak másodsorban problémaelhárító, ráadásul már működési szintű kockázatkezeléssel,

azonosítani kell a vállalati működés alappilléreit.

A kockázat definícióját is ki kell tisztítani, majd a működés szintjére kell emelni, és ezután már lehet közvetlenül a stratégiához is kötni.

Célom, hogy a receptek ne általánosságokat tartalmazzanak, hanem mérhető, skálázható, konkrét legyen mind a ráfordítás, mind az eredmény, mind az a "mérték". amennyire a célokat egy adott helyzetben sikerült elérni.

A sok hasznos tanács tárolására és visszakeresésére, összefüggéseik feltárására is érdemes eszközt fejleszteni.

Az értekezésemben leírt PCUBE-SEC módszertannal és eszközzel ezen célok megvalósításához szeretnék hozzájárulni.

## III. Vizsgálati módszerek

**1. A vállalati működés mérhető támogatásának kialakítása, részben az informatika hatóköréből a vállalati működés szintjére általánosított hagyományos módszerekre támaszkodva, részben új fogalmak, és ezekre támaszkodó, skálázható módszerek bevezetésével**

### 1.1 A hagyományos informatikai biztonsági és IT audit módszerek ellentmondásainak és hiányosságainak tisztázása

Abból a hipotézisből indultam ki, hogy az ISACA COBIT módszertanában, és a CISA kézikönyvben ismertetett legjobb szakmai gyakorlat felhasználási esélyeit, az ötlettárház azon folyamatos bővítése ellenére, amit a COBIT 1998 és 4.1 közötti vonulatban tapasztalhattunk, rendkívüli mértékben rontják az apró hiányosságok, ellentmondások, következetlenségek. Ugyanez tapasztalható az ISO szabványaira, és irányelveire is [COBIT 4.1], [COBIT 5, 2012], [ISO 27000 család].

Véleményem szerint jelentősen megnehezíti az informatikai ellenőrök munkáját, hogy, mint már említettük, kimaradt az "ellenőrzési cél" fogalma a COBIT 5-ből, megszüntetve ezzel a célok, és az elérésükre javasolt intézkedések szétválasztásának lehetőségét. Azt is érdemes ismételten hangsúlyoznunk, hogy az informatikai ellenőrzési cél nem az ellenőr, hanem az egész intézmény célja kell legyen, valamint, hogy azok az intézkedések, amelyeket a kézikönyvek, szabványok, irányelvek javasolnak, szükségesek, de nem feltétlenül elégségesek az adott célok eléréséhez.

Számos további problémát is sikerült feltárnom. Az sem egyértelmű, hogy a különféle szintű célok kitűzéséért melyik szerepkör / szakterület a felelős. A COBIT-ból, az informatikai folyamatok ismertetését nem számítva, az ISO szabványokból, ajánlásokból pedig az ISO 27001 Annex A kivételével, hiányzik:

- a célok, és az elérésükhöz ajánlott részcélok transzparens összerendelése,
- az intézkedő intézményi szakterületek / szerepkörök azonosítása,
- az intézkedők felelősségi körének azonosítása,

tehát a javasló / elrendelő, engedélyező, végrehajtó, végrehajtást ellenőrző felelősségi kör azonosítása is, és e különböző munkaköri leírási elemek szigorú szétválasztása.

Disszertációmban részletesen feltártam e problémákat, és eszerint módosítottam a tradícionális definíciókat. Így a PCUBE-SEC-ben a célok, és az azokat *szolgáló* intézkedések egyértelműen megkülönböztethetőek, és meg is különböztetendőek. Módszertanom további előnye, hogy elválnak egymástól mind a célok, mind az intézkedések meghatározójának, az intézkedések engedélyezőjének, végrehajtójának, és a végrehajtás ellenőrzőjének szerepkörei, illetve szakterületei.

**1.2 Az intézményi működés alapvető tényezőinek azonosítása, és a fenti problémák megoldása után egy olyan új, hatdimenziós fogalomrendszer kialakítása, amely a módszerek hatókörét az informatika szintjéről a vállalati működés szintjére emeli. Az új módszertan kibővítése konkrét mérési és skálázási lehetőségekkel.**

Vizsgálataim során feltártam, hogy, bár csak véletlenszerűen, de már a tradícionális módszertanok is túlnyúltak az informatika hatókörén, bár nem a célok kijelölésében, hanem inkább a szereplőkre, a végrehajtókra való utalásokban, már ahol ilyen utalás egyáltalán szerepelt. Ez vezetett affelé, hogy érdemes meghatározni olyan szempontokat, amelyek irányába e módszereket ki lehetne terjeszteni. Ezeket az irányokat neveztem el az útmutatások *dimenzióinak*.

Hat dimenziót sikerült azonosítanom: a célt, az ezt szolgáló intézkedést, az intézkedés értelmezési tartományát, értékkészletét, és erőforrásait, valamint a módszertanom felhasználójának szempontrendszere szerint elvárt eredmény várható érvényesülési területét.

Ezután viszont már érdemes volt kiterjeszteni a tradícionális eredmények e kijavított verzióit az informatikáról az intézményi működés területére. Ez azt jelenti, hogy a fenti dimenziók már nemcsak az informatika, hanem az egész intézményi működés területéről felvehetnek értékeket. Így tehát a PCUBE-SEC tanácsait ki lehetett terjeszteni erre a bővített területre.

A gyakorlati használhatóságot illetően abból a hipotézisből indultam ki, hogy a PCUBE-SEC felhasználója hasznát látná, ha sikerülne e hat dimenziót konkrét attribútumokkal is jellemezni. Első választásként a különféle hasznos osztályozási lehetőségek adódtak, így a PCUBE-SEC felhasználók számára biztosítható "receptjei" már nem általánosságokkal foglalkoznak, hanem mérhető, skálázható, konkrét információt adnak a ráfordításról, annak eredményéről, és arról "mértékről", hogy mennyire sikerült a célokat egy adott helyzetben elérni. Ezek az információk persze nem tudnak abszolút, forintosítható számértéket adni, hanem a különféle választási lehetőségek közötti relatív különbséget adják meg. Igaz ez a fenti hat dimenzió valamennyi elemére. A PCUBE-SEC egymáshoz képesti értékelést biztosít, de azt akár összetett módon is, tehát egyszerre vehető figyelembe a felhasználói

szmpontrendszer a célokat kijelölni jogosult szereplők súlyozásánál, majd aztán a célokhoz vezető részcélok egymáshoz képesti jelentőségénél. Így egy adott részcélnál a részcél fontosságát mintegy "tovább súlyozhatja" annak a szakterületnek, vagy munkaköri szereplőnek a fontossága, aki az adott részcélt meghatározta.

Abból a hipotézisből indultam ki, hogy előfordulhat, hogy két alsóbb rendű cél két különböző felhasználói szempontot érvényesít, de azt is meg kell engedni, hogy ugyanazon cél felé tartsanak, így a PCUBE-SEC definícióit eszerint alakítottam ki. Ezeket a disszertációban részletesen ismertetem.

## 2. A stratégia és a biztonság között egy olyan közvetlen kapcsolat létrehozása, amely lehetővé teszi, hogy az e biztonságra, illetve a stratégiai célok elérésére való törekvés egymást kölcsönösen támogathassa. Ehhez egy önmagában is használható, az intézmények irányítását, működésük javítását is szolgáló, ún. kiválósági kritériumrendszer kialakítása.

### 2.1 Az intézményi stratégiai célok szükséges feltételeihez PCUBE-SEC "receptek", az ún. kiválósági kritériumrendszer kialakítása

Ha a PCUBE-SEC abban is segíteni akarja felhasználóját, hogy stratégiai és a biztonsági céljait egymás támogatására felhasználhassa, akkor érdemes egy olyan minta működési cél rendszert kialakítani, amelynek céljai, mégha némelyik a másik rovására teljesíthető is, esélyesek arra, hogy stratégiai célok megvalósulását támogassák, és arra is alkalmasak, hogy belőlük összetett célokat lehessen képezni, amelyek szintén stratégiai célok szükséges feltételei lehetnek. Ez vezetett a működés javítását szolgáló, ún. kiválósági kritériumrendszer kialakítása gondolatához.

Abból a hipotézisből indultam ki, hogy ehhez, mégha csak részben is, felhasználhatóak a COBIT információkritériumai, a már említett javítások és általánosítások után. Természetesen új, a rendezett működést explicit módon megkövetelő kritériumokat is definiálnom kellett.

### 2.2 Az intézmények fennmaradása, sőt, piaci helyzetük folyamatos javulása, és a biztonság közötti kölcsönös, egymást támogató kapcsolat létrehozása

Tapasztalataim szerint az intézmények jelentősen erősíthetik piaci pozíciójukat, ha meghatározzák stratégiájukat, és úgy működnek, hogy a lehető legjobban hozzájáruljanak stratégiai céljaik eléréséhez. Azt kell tehát *konkrét teendőkre* lefordítani, hogy mit kell e

"lehető legjobb hozzájárulás" érdekében tenni. Erre viszont a PCUBE-SEC működési céljai, és az ezekhez hozzájáruló működési tevékenységek egy alkalmas eszköztárat biztosíthatnak.Egy olyan biztonság definíciót kellett tehát kialakítani, amely, a PCUBE-SEC lehetőségein keresztül, e biztonság, és az intézményi működés javítása között hoz létre közvetlen kapcsolatot. Ezzel elérem, hogy a stratégia támogatható legyen ennek a működési biztonságnak az eszközeivel, illetve a működés biztonsági célok igazolhatóak legyenek stratégiai célokkal.

Abból a hipotézisből indultam ki, hogy, ha a PCUBE-SEC hatókörét az informatikáról a vállalati működésre általánosítjuk, a biztonságot is érdemes ezzel a hatókörrel definiálni, ezért érdemes egy működési biztonsági feltételrendszert kialakítani. Feltételeztem, hogy ez a PCUBE-SEC felhasználóját akkor támogatja intézményi stratégiája szolgálatában, ha követelményei kézzelfoghatóak, konkrétak, teljesítésük mértéke mérhető, sőt, a teljesítésüket előre jelezhető feltételektől lehet függővé tenni.

Bár ehhez a működési biztonsághoz utam az informatikai speciális eset általánosításán keresztül vezetett, mégsem egy hagyományos definíciót általánosítottam a disszertációmban, hanem újonnan alakítottam ki ezt a fogalomrendszert. Ezért feltételeztem, hogy, annak ellenére, hogy a követendő irányt, gyakorlati tapasztalataimon kívül, az informatikai tanulságok elemzése is mutatta, annak végleges megfogalmazását, hogy mikor tekinthető biztonságosnak az intézményi informatikai rendszer, ebből az új PCUBE-SEC definícióból érdemes levezetni. Ugyanis így biztosítható, hogy az informatika az intézményi stratégiát szolgálja.

## 3. A működésjavítási, és egyéb problémák megoldásához felhasználható, szakértői és felhasználói receptek tárolásának, újrafelhasználásának, feldolgozásának technikai lehetősége

Abból a hipotézisből indultam ki, hogy hasznos lehet egy olyan technikai segédlet, amely lehetővé teszi, hogy a szakmai legjobb gyakorlat tanácsait, és a PCUBE-SEC felhasználók tapasztalatait egyetlen tudásbázisba lehessen eltárolni úgy, hogy a felhasználó kérdésére ezt az információt vissza is lehessen keresni, természetesen a kérdéshez illeszkedő válasz formájában.

Mivel a PCUBE-SEC-et a legfelső vezetés, és az intézmény üzleti, és nem informatikával foglalkozó támogató szakterületei számára is hozzáférhetővé akarom tenni, kell, hogy legyen legalább egy olyan felhasználói felülete, amely számítástechnikai szakismeretek nélkül is viszonylag kényelmesen használható. Egy lehetséges megoldás, ha  régebbi, a mesterséges

intelligencia alapú szakértői rendszerek terén elért eredményeimet alkalmazom a PCUBE-SEC tudásbázis felállítására, és a benne lévő információ feldolgozására úgy, hogy a felhasználó választ kapjon kérdéseire.

Először meg kell határozni, milyen kérdésre milyen választ tudunk adni. A PCUBE-SEC módszertanból eredően a kérdés egy kívánt működési, speciális esetben stratégiai cél, a válasz pedig azon célok és teendők együttese, amelyek elérése illetve végrehajtása a megadott célhoz vezet. Követve a PCUBE-SEC filozófiáját, nem érdemes biztosan célravezető módszert keresni. Ha megelégszünk a szükséges részcélok és teendők egyfajta rendezett sorozatával, azonnal adódik, hogy fel lehetne használni eredetileg párhuzamos és konkurrens folyamatokból álló rendszerek modellezésére alkotott, már említett PCUBE, azaz $P^3$-nevű rendszeremet (**P**lanning and simulation of **P**arallel and concurrent **P**rocess systems) [4, 5].

Ennek készítésében segítségemre voltak azok a listakezelési tapasztalatok, amelyeket egyetemi doktori dolgozatom készítésekor szereztem. Ez robotok gondolkodásának támogatására, ezen belül konkrétan arra készült, hogy a robot bizonyos helyzeteket kezelni tudjon [1], [Dahl, et al., SIMULA 67, 1970].

A folyamatmodellezési problémák megoldásában, főleg a folyamatok idő- és erőforráskezelési lehetőségeinek specifikálásában egyrészt a SIMULA 67, másrészt, a konkurrencia leírási lehetőségeire vonatkozó követelmények kialakításakor, Hoare, és a konkurrens Pascal tudásanyagára támaszkodtam [Dahl, et al., SIMULA 67, 1970], [Hoare, 1978], [Hansen, 1977].

Az ilyen specifikációkkal először a T-PROLOG, a PROLOG-ban készült, ugyanilyen célú eszköz fejlesztéséhez járultam hozzá [Szeredi, P., Futo, 1977], [2, 3].

## 4. Az intézményi működés alappillér rendszere. Módszertan a stratégiai célok támogatására, és a működési kockázatok kezelésére

A tradícionális módszertanok definícióiból gyakran kimarad, mi a stratégiai értelme a kockázatok kezelésének. Védelmi, defenzív hozzáállásukkal a már bekövetkezett bajok elhárítására koncentrálnak [ISO 27000, ISO 27001, ISO 27002, 27005, G73, 38500],[CRM, COBIT 4.1 - Glossaries]. Először abból a hipotézisből indultam ki, hogy a problémák megoldásához meg kell nyerni a legfelső vezetést, az összes üzleti és támogató szakterületet. Ezért kialakítottam egy, az intézményi stratégiai célokhoz közvetlenül kötődő, a szereplők felelősségét is mutató kockázatfogalmat [6, 9, 14]. Alkalmazása során kiderült, hogy nemcsak

a problémák kezelése, hanem a problémák lelőhelye is túlmutat az informatikán, így áttértem a működési kockázatok kezelésére [16]. Ehhez viszont meg kell nyerni az összes szakterület közreműködését. Így jutottam el ahhoz a hipotézishez, hogy a stratégiai célokhoz kell a működési kockázatok kezelését kötni.

Abból indultam ki, hogy a PCUBE-SEC feladatmegoldási receptjei a nem informatikai szakterületek számára is érthetőbbek, rendszerezettebbek, könnyebben követhetőek lesznek, ha lehetőség van annak kijelölésére, milyen területen van valami javítandó, mit lehet itt megváltoztatni, milyen eszközökkel. Ha ezek a részletek megvannak, könnyebb lesz részletes számítástechnikai ismeretek nélkül is használni a PCUBE-SEC-et, így bővebb körtől kaphatunk mind megoldási recepteket, mind támogatást ezek megvalósításában. Ennek érdekében bontottam három olyan dimenzióra az intézményi működést, melyek segítségével pontosabban lehet e három kérdésre válaszolni. Ezek a szervezet, a szabályozás, és a technika.

A tradícionális módszertanok informatikai kockázatkezelési megközelítése, a kockázatkezelési ciklusok, és az irántuk támasztott követelmények is az említett defenzív megközelítésen alapulnak [CRM], [ISO 27005]. Így a célokat általában az informatikai biztonságiak próbálják meg kitűzni, ezek legjobb szakmai gyakorlat szerinti és törvényi, meg egyéb megfelelőségi helyességét, majd teljesítésüket az informatikai auditorok ellenőrzik [ISO 27001, 27005], [CRM, COBIT]. Tapasztalatom szerint viszont még a problémák kiküszöböléséhez is könnyebb az összes szakterületet megnyerni, de az intézmény biztonsági helyzetét is javító célokhoz is kapunk ötleteket, ha a defenzív módszer helyett proaktív, a kockázatok helyett az üzleti boldogulást a középpontba helyező ciklust tervezünk. Ezt először az intézményi működés informatikai részterületére fejlesztettem ki [6, 9]. A fenti okokból ezt is érdemes volt általánosítani az egész működésre [16, 17].

## IV. Új tudományos eredmények

### 1. téziscsoport

**Egy olyan, az intézmények működésének fejlesztésére alkalmas módszertant alakítottam ki, amely segíti felhasználóját saját, az intézményi stratégiát szolgáló szempontrendszerének kialakításában. Támogatja, hogy eszerint a szempontrendszer szerint értékelhesse - egymáshoz képest súlyozhassa, nemcsak magukat a célokat, de az azokat kitűző szakterületek / intézményi szerepkörök jelentőségét is, a célokat szolgáló részcélok, illetve az ezeket szolgáló intézkedések**

**használt, valamint az intézkedéseket meghatározó, engedélyező, végrehajtó, és eredményüket ellenőrző egyes szakterületeket / intézményi szerepköröket.**

**1.1 tézis: A hagyományos, az intézményi informatika javítását szolgáló informatikai biztonsági szabványok, irányelvek, IT audit módszertanok átvizsgálásakor feltártam a következetlenségeket, hiányosságokat, és bemutattam ezek hátrányos következményeit.**

Átvizsgálva az Information Systems Audit and Control Association (ISACA) Control OBjectives for Information Technology (COBIT) módszertanában, és tankönyveiben, valamint az International Standard Organization (ISO) szabványaiban és irányelveiben ismertetett, az informatikai rendszerek tökéletesítésére javasolt célokkal és intézkedésekkel foglalkozó definíciókat, számos következetlenséget, hiányosságot sikerült azonosítani [CRM, COBIT 1998, 2000, 2005, 2006, 2007], [ISO 27000, G73, 27001, 27002, 27005, 38500], [12, 13]. Ezek közül legsúlyosabb az ún. ellenőrzési cél, és az ellenőrzési intézkedés, a "mit" és a "hogyan" összecsúszása [COBIT 2012], [Guldentops, 2012]. Kimutattam, hogy egyes esetekben ezek a hibák milyen károsan befolyásolták a magyar törvények egyes fontos részleteit [11].

A tradícionális definíciók problémáinak javításai közül a következő szempontok voltak a legfontosabbak [11, 12, 15] :

- a célok, és az elérésükre javasolt intézkedések szigorú szétválasztása
- a célok és a részcélok összerendelésének lehetősége
- az intézkedő intézményi szakterületek / szerepkörök azonosítása
- az intézkedők felelősségi körének azonosítása - azaz a javasló / elrendelő, engedélyező, végrehajtó, végrehajtást ellenőrző felelősségi köré, és ezek szigorú szétválasztása
- a definíciókba, az intézményi felelős bevezetésével, annak nyomatékos hangsúlyozása, hogy az informatikai ellenőrzési cél nem az informatikai ellenőr célja, sok esetben mégcsak nem is az informatikai szakterületé, hanem az egész cégé, és a cég érdekét kell, hogy szolgálja, és
- kitűzéséért a legfelső vezető a felelős, természetesen delegálhat valakit maga helyett
- annak hangsúlyozása, hogy a célok elérésére javasolt intézkedések szükségesek, de nem feltétlenül elégségesek az adott célok eléréséhez.

**1.2 tézis: Azonosítottam az intézményi működés alapvető tényezőit. Kialakítottam egy olyan - a stratégiát e tényezőkön keresztül szolgáló - irányítási módszertant, amely a cél - intézkedés - értelmezési tartomány - értékkészlet - erőforrás ötös összetett, kölcsönös összefüggésein alapul, és amelybe, hatodik dimenzióként, felvettem módszertanom, a PCUBE-SEC felhasználója szempontrendszere szerint elvárt eredmény várható érvényesülési területét is. Ebben a fogalomrendszerben kiküszöböltem a fenti definíciós problémákat. Ezután már az informatikai helyzet javításánál szélesebb kört célozhattam meg, az intézményi működés szintjét.**

Ebben a hatos fogalomrendszerben a célok, és az azokat *szolgáló* intézkedések egyértelműen megkülönböztethetőek, és meg is különböztetendőek. Ez a fogalomrendszer támogatja a fenti szempontok teljesítését.

Lehetővé teszi mind az előre kitűzött, a felhasználói szempontrendszer szerint meghatározott célok részcélokra bontását, mind a mindennapi gyakorlat szintjén kitűzhető célok - akár speciálisan az intézmény valamelyik szakterületére specifikusan jellemző célokból - olyan, egyre összetettebb célok alkotását, amelyek közelebb visznek az elérni kívánt célok teljesüléséhez. Támogatott az így készült "receptek" egyszerű, számítástechnikai szakértelem nélkül is használható formájú nyilvántartása, szükség esetén azokkal az intézkedésekkel együtt, amelyek hozzájárulhatnak megvalósulásukhoz.

A hat dimenzió egymás közötti kapcsolatainak kifejezésére olyan, a velük végzendő műveletek mindennapi gyakorlatában jól használható attributumkészletet ajánlottam, amelyet a PCUBE-SEC felhasználó könnyen kiegészíthet. A dolgozatban ajánlott számos attributumra talán legfontosabb példa a részcélok, és az azokat szolgáló intézkedések értékelésére - súlyozására jól használható, úgynevezett "távolság". Ez a távolság nem matematikai, hanem bizonyos információk kiértékelésére alkalmas, szubjektív mérőszám. Megállapításának módjait a dolgozat részletesen tárgyalja. Ez, alacsonyabb rendű cél esetén, az e célnak valamely előre megadott felhasználói céltól való távolsága egy másik részcélhoz képest, mely részcél távolság értékét mérhetjük akár ugyanattól a céltól, vagy akár egy másiktól. Ha a két részcél ugyanazon felhasználói cél "felé tart", akkor e két részcél jelentőségét lehet érdemes a PCUBE-SEC segítségével összehasonlítani, ugyanazon célhoz viszonyítva. Ha a másik, az előbbivel összehasonlítandó részcél egy másik magasabb szintű célt "vesz célba", akkor e két magasabb szintű cél egymáshoz képesti jelentősége is súlyozható [13, 14, 16, 17].

Nemcsak a cél, hanem az intézkedés, és az erőforrás is vizsgálható ilyen hierarchikus módon. Mindkettő konkrét példányához rendelhető "alacsonyabb rendű", abban az értelemben, hogy

az alacsonyabb rendű szükséges a magasabb rendűhöz, persze itt sem állítjuk, hogy elégséges is lenne. A PCUBE-SEC támogatja, hogy e háromfajta hierarchia akár különböző szintű elemei is kapcsolódhassanak egymással olyan attributumokon keresztül, mint például a távolság. Például egy adott célhoz tartozó részcél megvalósítását szolgáló intézkedéshez szükséges erőforrás távolsága az eredeti adott céltól akkora lesz, mint a részcél távolsága. Tehát sikerült a PCUBE-SEC működési céljait és intézkedéseit úgy definiálni, hogy *olyan súlyozott, komplex kapcsolatokat is létrehozhasson felhasználója, amelyben a fogalomrendszer több dimenziója is egyszerre szerepel.*

A PCUBE-SEC felhasználói köre így nemcsak az informatikai, és az azzal kapcsolatos szakterületekből állhat, hanem a legfelső vezetéstől, az üzleti szakterületeken át, egészen a kiszolgáló területekig nyújt támogatást.

**2. téziscsoport. Kialakítottam egy olyan működési biztonság definíciót, amely szerint az intézmények biztonságát konkrét, skálázható, akár előre jelezhető mértékben teljesülő paraméterektől is függő követelmények teljesítése alapján ítélhetjük meg. A definíció biztosítja, hogy az így jellemzett biztonságra, illetve a stratégiai célok elérésére való törekvés egymást kölcsönösen támogathassa. Közvetlen kapcsolatot hoztam létre, a PCUBE-SEC lehetőségeivel, e biztonság, és az intézményi működés javítása között.**

**Kimutattam, hogy az intézmények piaci előmenetele támogatható a működési biztonság eszközeivel, illetve a működés biztonsági célok igazolhatóak stratégiai célokkal. Ezzel a működési biztonság fogalommal összhangban értelmeztem az intézmény informatikai rendszere biztonságát.**

Módszertanom stratégiai céljaik támogatásával segíti az intézmények boldogulását, piaci helyzetük javítását.

**2.1 tézis: Felállítottam egy, az intézmény működésének javítását szolgáló, ún. kiválósági kritériumrendszert, amelynek elemeit, vagy az azokból alkotható összetett követelményeket a PCUBE-SEC az intézmény stratégiai céljai *szükséges* feltételeként ajánlja felhasználójának.**

E kritériumok alapja részben az ISACA hét, ún. információkritériumból álló rendszere, ezekből három az ISO szabványokban is szerepel [COBIT, CRM], [ISO 27000, 27001]. Ezek következetlenségeit ki kellett tisztázni [13, 14], majd általánosítani kellett az informatikáról az intézményi működés területére [16, 17]. Új kritériumokat is fejlesztettem, először az

informatikai rendszerekre, ezeket a gyakorlatban is alkalmaztam már, majd, némi változtatás után, kiterjesztettem a működés területére [12, 15]. Ma már kritériumaim 2 csoportba oszthatóak: az egyik az intézmény vagyontárgyainak kezelésére, a másik az intézmény irányítására ad - úgynevezett kiválósági - kritériumokat [16, 17]. Az első csoportba tartozik a rendelkezésre állás, bizalmasság, integritás, a másodikba pedig a hatékonyság, célravezető jelleg, a funkcionalitás, a bármiféle előírásoknak való megfelelés, a kockázatkezelés kiválósága, a megbízhatóság, és a rend.

A kritériumokat úgy határoztam meg, hogy kövessék a "mindennapi gyakorlatot", tehát van köztük olyan, amelynek a teljesítésére való törekvés rontja egy másik kritériumnak való megfelelés esélyeit. A PCUBE-SEC felhasználójára bízom, hogy eldöntse, egy adott helyzetben melyik kritérium, vagy esetleg egy másféle cél, mennyire fontos a stratégiai célok elérésében. A célok összehasonlítását a PCUBE-SEC cél-attributumokkal támogatja. Ezeket részletesen tárgyalom a disszertációban. Az összehasonlítást kifejezhetjük bármiféle n-essel, ez állhat számokból, de lehet akár a (kicsi, közepes, nagy) hármas is. A költségek számíthatósága érdekében azonban ekkor is érdemes az akár szubjektív, akár objektív értékekhez számokat is rendelni.

Az ilyen viszonyító jellegű "osztályozás" nem idegen az audit gyakorlatától. A CMM, a SEI (Software Engineering Institute) a COBIT-ba már 2000-ben beépített Capability Maturity Model-jének audit célokra átírt változatában az intézmények érettsége egy, 0 és 5 közé eső számmal adható meg. Ez az éretlennek, kezdetinek, ismételhetőnek, definiáltnak, irányított - mérhetőnek és optimalizáltnak felel meg. Az egyes szintek jelentését az ISACA lényegében egy - egy tanácshalmazzal írta le [COBIT 2000]. A PCUBE-SEC szerint az ilyen "kifejező számok" - vagy másféle értékek, pl. olyanoké, mint "kicsi, nagy, közepes" - összehasonlításának eredménye lesz a kezelendő információ.

E kritériumok a számítástudomány jelen tárgyunktól eltérő területeken is bizonyítottak már. Nagy Gabriella idős, vagy fogyatékos emberek életlehetőségeit beszéddel irányítható rendszerekkel támogató, ún. Ambient Assisted Living rendszerek tervezése és megvalósítása kiértékelésére, Nagy Tibor István és Tick József pedig katonai szenzorok értékelésére alkalmazta ezeket a kritériumokat [G. Nagy, 2013], [Nagy T. I., J. Tick, 2014].

**2.2 tézis: A PCUBE-SEC értelmezési tartományán, az intézményi működés területén definiáltam egy, a stratégiai célokhoz, és a piaci, valamint a szabályozási környezethez is illeszkedő, olyan "működési biztonság" fogalmat, amelyet konkrét, mérhető, akár előre jelezhető paraméterektől is függő követelmények teljesítése**

**jellemez, skálázható mértékben teljesíthető előfeltételekkel. Az intézmény informatikai rendszere biztonságát ennek a működési biztonságnak speciális eseteként definiáltam, így mérhető, és előre jelezhető követelmények irányíthatják az informatikai rendszer fejlesztését és vizsgálatát is.**

Az intézményi működés alappillérein olyan rendszert kell megvalósítani, amely előre jelezhető, mérhető, skálázható módon, úgy, és annyira szolgálja a kiválósági kritériumokat, ahogy azt - az intézmény érdekei szerint - a felső vezetés meghatározza. A működési biztonság pontos definícióját és felhasználási lehetőségeit részletesen elemzem a dolgozatban.

Előírásai közé tartozik, hogy a PCUBE-SEC felhasználónak meg kell határoznia, mennyire teljesüljenek az adott vizsgált helyzetben az egyes kiválósági kritériumok. Így minél jobban törekszünk a működési biztonság tökéletesítésére, annál jobban - azaz a stratégiát annál jobban szolgálva - fog az intézmény működni [16, 17]. A működési biztonság alkalmazása tehát megkívánja, hogy a PCUBE-SEC felhasználó vagy maga ismerje az intézmény érdekeit, vagy támaszkodhassék ilyen ismeretekre.

Az intézményi biztonság, és a kritériumok definíciója együtt részletes útmutatást is ad, hogy a kritériumok elérését támogató működési részcélokat és ezekhez a működési tevékenységeket hol, és hogyan kell megkeresni a működés összetett rendszerében. Bár eredetileg ez a működési biztonság koncepció is az intézményi informatika, és az intézményi stratégiai célok összefüggéseit kutató vizsgálataimnak az eredménye, dolgozatomban már az intézményi biztonság speciális eseteként volt célszerű meghatározni az intézményi informatikai rendszer biztonságát [7, 8, 12]. Ennek előnye, hogy az intézményi informatikai rendszer fejlesztésekor mérhető és előre jelezhető mértékben lehet az intézmény működését fejleszteni, stratégiáját szolgálni. Vizsgálatakor pedig pontosan megadott jellemzőket lehet számonkérni [15].

**3. tézis**

**Kialakítottam egy olyan technikai eszközrendszert a PCUBE-SEC tudásbázis kialakítására és e tudásbázis feldolgozásának támogatására, amely lehetővé teszi működésjavítási, problémamegoldási szakértői és felhasználói receptek tárolását és újrafelhasználását.**

A receptek elérendő működési célokat, és / vagy azok eléréséhez szükséges feltételeket javasolhatnak. Egy feltétel újabb működési célok, és / vagy működési intézkedések legalább egyelemű sorozata. Működési célnak nevezzük itt az egyes intézményi szakterületek céljait.

Ezek eléréséhez *szükségesek* a feltételeket alkotó célok és tevékenységek. Egy adott működési célhoz egy másik cél elérése is hozzájárulhat, mint feltétel.

Speciális esetben e működési cél, természetesen, stratégiai cél is lehet. Ugyanahhoz a működési célhoz tartozhat többféle ilyen sorozat is. A feldolgozás során a PCUBE-SEC először a tudásbázisban első helyen álló alternatívával próbálkozik. Sikertelenség esetén tér vissza a következő alternatívához. Egy, a rendszernek megadott működési célra a rendszer feltételek legalább egyelemű sorozatával válaszol. A "siker" itt azt jelenti, hogy a felhasználó működési céljához a PCUBE-SEC olyan feltételeket ad ki, amelyeket a felhasználó az adott feldolgozási folyamatban már nem kíván "tovább bontani", azaz nincs szüksége olyan feltételekre, amelyek az addig nyertekhez adnának további szükséges feltételeket.

Ez a felhasználói támogatás hasonlít ahhoz, amelyet a PROLOG nyújt általános, vagy a T-PROLOG párhuzamos és konkurrens folyamatokból álló rendszerekkel kapcsolatos problémákra. Azonban ezektől lényegesen eltér mind a támogatás jellege, mind technikai megoldása.

Ami a támogatást illeti, egyrészt az eredményül kapott feltételek mind *szükségesek* az adott cél eléréséhez, de szinte soha nem elégségesek. Másrészt a tudásbázis egy adott cél érdekében történő "lekérdezése", egy adott cél feltételei keresése nem akkor ér véget, ahogy a PROLOG, vagy a T-PROLOG esetében, tehát nem akkor, amikor a megadott felhasználói cél "elfogy", összes feltételei "kiesnek". A PCUBE-SEC feldolgozást általában már ezelőtt megállítja a felhasználó, hiszen a kapott, többnyire teendőkből, és a megadottnál "alacsonyabb rendű" célokból álló listát már be is vezetheti a munkahelyén. Az "alacsonyabb rendű" ugyanis itt nem értékítélet, hanem azt jelzi, hogy az eredmény céljai és teendői a gyakorlati teendők és célok szintjéről közelítik azt a célt, amelyet a felhasználó megadott a PCUBE-SEC-nek. Általában ez a megadott cél közelebb van stratégiai célokhoz, mint az eredmények. Ezek a "levezetett" célok, amelyeket a PCUBE-SEC "válaszol" a felhasználó "kérdésére", a megadott stratégiai, vagy legalábbis működési célra. Pontosabban ezeknek a tudásbázisból vett eredmény céloknak / teendőknek, mint lépéseknek a kapott sorrendje mutatja a PCUBE-SEC felhasználójának a működés javítása érdekében bejárandó utat.

A PCUBE-SEC megvalósítása is eltér a PROLOG-étől, vagy a T-PROLOG-étól. Maga a PROLOG előbb FORTRAN-ban, majd CDL-ben (Compiler Description Language) készült, és programozott mintaillesztésen alapult, a T-PROLOG implementációs nyelve pedig a PROLOG volt [Kowalski], [Szeredi, P., Futo, 1977], [2].

A PCUBE-SEC architektúra pedig négyrétegű. Egyes rétegeihez más-más implementációs módszer és típusrendszer tartozik. A legfelső a recepteket "író / olvasó" felhasználói réteg. Az itteni feldolgozásokat a 2. réteg nem diszjunkt fák bejárásával valósítja meg. Ennek a programja 3. szinten egy általánosan is használható, de erre a célra fejlesztett listakezelő nyelvben készült. Ezt pedig a 4. szint implementálja [4, 5].

A PCUBE-SEC egyik érdekessége, hogy nemcsak legfelső rétegét lehet érdemes használni, hanem a harmadikat is. A legfelső szinthez, a receptek kezeléséhez nincs szükség számítástechnikai szakismeretekre, de a listakezelő szinthez igen. Itt listával reprezentálható problémákat lehet megoldani.

A PCUBE-SEC architektúra egy részét 1976-ban, egyetemi doktori dolgozatom részeként, a robotvezérlés "gondolkodási" részének támogatására készítettem, akkor még a rezolúció elve alapján, SIMULA 67-ben [1], [Dahl, et al., SIMULA 67, 1970]. Ebből néhány alapötletet felhasználtam párhuzamos és konkurrens folyamatokból álló rendszerek modellezésére. Ezt arendszert funkciója alapján neveztem el PCUBE-nak, vagy $P^3$-nek, - a **P**lanning and simulation of **P**arallel and concurrent **P**rocess systems rövidítéseként [Szenes, 1987], [Szenes 1988]. A PCUBE másik alapja a SIMULA 67 nyelv gazdag folyamatkezelési tárháza, a Concurrent Pascal monitor-, és Hoare input guard fogalma volt [Dahl, et al., SIMULA 67, 1970], [Hoare, 1978], [Hansen, 1977]. A "monitort" korábban, javaslatom alapján, Futó Iván és Szeredi János már a T-PROLOG-ba is beépítette, "erőforrás" néven [2]. Enélkül nem is lehet konkurrens folyamatokat modellezni, hiszen éppen ez a típus az, amiért a párhuzamos (részben egyidőben is végrehajtható) folyamatok "versenyeznek", konkurrálnak.

IT audit- és informatikai biztonsági területen a PCUBE tudásbázis feldolgozási lehetőségei alapelveit először alkalmazásfejlesztési területen használtam fel [7, 8]. Az informatikai biztonságot és ellenőrzést támogató, valamint a ma már az intézmények működése javításával foglalkozó felhasználási lehetőségeket disszertációmban részletesen kifejtem.

**4. téziscsoport**

**Felépítettem az intézményi működés alappillér rendszerét. Kifejlesztettem a PCUBE-SEC stratégia támogató működési kockázatkezelési módszertanát, fogalomtárral, és rendszerszervezési segédlettárral együtt.**

### 4.1 Kialakítottam az intézményi működés alappillérrendszerét, a PCUBE-SEC alapdefiníciók és segédletek értelmezési tartományának és értékkészletének gyakorlati célú partícionálása érdekében

A stratégiai célok elérése érdekében kitűzendő működési célok / végrehajtandó működési tevékenységek értelmezési tartománya az intézményi működés egésze. Annak érdekében, hogy a PCUBE-SEC felhasználó mind a legjobb szakmai gyakorlat receptjeiben, mind saját tapasztalataiban könnyebben *azonosíthassa és rendszerezhesse,* hogy a működés mely területén van teendő, mely területén kell valamilyen részcélt kitűzni, ez a teendő / részcél a működés melyik részén fog változtatni, a működés mely eszközeivel, a PCUBE-SEC három olyan dimenzióra bontja az intézményi működést, amely e három kérdés mindegyikénél pontosítja a választ.

Ez valóban három kérdés, hiszen, ha valamin változtatunk, az lehet, hogy egy másik területen hat, egy harmadik terület eszközeivel.

Ezen követelmények teljesítésére definiáltam *az intézményi működés alappillér rendszerét,* amely az intézmények működését három fő szempont alapján tárgyalja, ezek: a szervezet, a szabályozás, és a technika. Ez a *három dimenzió megfelel a fenti követelményeknek.Jól használhatóak a PCUBE-SEC összes, a működési területen értelmezett definíciója hatókörének pontosításánál.* Megkönnyíti a rendszer számítástechnikai szakértelem nélküli használatát is, hiszen "fogasokat", osztályozási szempontokat kínál a célok és a teendők különféle attributumaihoz. Mindez különösen fontos a kiválósági kritériumokkal kapcsolatos teendők, de esetleges részcélok meghatározásakor is.

Először ezt az alappillér rendszert az informatikai biztonsági architektúra partícionálására definiáltam [6], majd kiterjesztettem az informatikára, mint értelmezési tartományra, az értékkészletet akkor még nem tisztáztam [12]. Auditálási tapasztalataim azonban bebizonyították, hogy fontos az értékkészlet explicit azonosítása is, és érdemes kiterjeszteni mind az értelmezési tartományt, mind az értékkészletet az intézményi működés összes területére [11, 13, 14, 16, 17].

### 4.2 Megalkottam a PCUBE-SEC stratégiatámogató működési kockázatkezelési módszertanát, fogalomtárát, és rendszerszervezési segédlettárát

A módszertan *fogalomtára* önmagában, a PCUBE-SEC tudásbázisfeldolgozási támogatása, sőt, a rendszerszervezési segédlettár nélkül is használható lehet, hiszen

- kijavítottam benne a tradícionális kockázatkezelési definíciók következetlenségeit,

- az *elérendő célokra* összpontosít, és nem a hagyományos defenzív, problémafeltáró megközelítésen alapul, amely, legalább utólag, igyekszik felszámolni ezek káros következményeit, és amely e következmények üzleti hatásával általában nem foglalkozik

- nem specializálódik az informatikára, hanem a teljes intézményi működés, azaz az üzleti, vezetési, és támogató szakterületek együttese alkotja mind a módszer értelmezési tartományát, mind értékkészletét.

Ahogy azt a disszertációban részletesen elemeztem is, a 27000-es család kockázat definíció tárgyú kereszthivatkozásai zavarosak, hivatkoznak definiálatlan fogalmakra is, a kockázat mérésének leírása hiányos, és a minőséget jellemző valószínűség fogalmat, a "likelihood"-ot használja olyankor, amikor konkrét mennyiségekre lenne szükség, így a "probability" helyesebb lenne. Következetesebbek a G73-as irányelv definíciói, de sem ez, sem a 38500-as szabvány nem köti a bekövetkezett problémák elhárítását valamilyen kívánt üzleti eredményhez [ISO 27000, ISO 27001, ISO 27002, 27005, G73, 38500]. Az ISACA sem foglalkozik a bekövetkezett károk üzleti értékével [CRM, COBIT 4.1 - Glossaries].

Mindezen problémák kiküszöbölésére alkottam meg először egy, a hagyományostól eltérő informatikai kockázat fogalmát, majd kiterjesztettem ezt az egész működési területre, így jött létre a "vagyontárgy kockázat" (asset risk) [6, 9, 12. 16]. Ez *explicit* módon tükrözi az éppen vizsgált vagyontárgy stratégiai értékét. A proaktív hozzáállással összhangban, nemcsak a "fenyegetésekkel" foglalkozunk, hanem, sőt, elsősorban, a *stratégia* a jelenleginél jobb szolgálatára törekszünk. Azt, hogy mi számít jobbnak, a rendszerszervezési segédlettár segít megállapítani. Ez támogatja a tényleges helyzet, és a teendők feltárását az intézmény felső vezetőinek, és többi, egy adott területet jól ismerő dolgozójának valamennyire mindenképp szubjektív véleménye kinyerésével és feldolgozásával. A dolgozatban részletesen elemzem azokat a formulákat, amelyek leírják a vagyontárgy kockázat, a felhasználói célok eléréséhez mindenesetre szükséges, bár nem feltétlenül elégséges intézményi erőfeszítések, valamint az e célok elérését a vagyontárgy támadásán keresztül akadályozó külső / belső támadások közötti összefüggéseket, itt csak utalni tudunk majd ezekre.

Definiáltam a *stratégiai alapú, cél-, és működési kockázatkezelés kiválóságot*, rövid nevén a *kockázatkezelés kiválóságát,* a legfelső vezetésnek a stratégia meghatározásával, és rendszeres felújításával kapcsolatos felelősségéből kiindulva. A definíció számonkérhető, pontosan meghatározott kötelességeket ró mind a legfelső vezetésre, mind a személyzet többi részére.

Ahhoz, hogy a PCUBE-SEC a vállalatirányítást biztonsági módszerekkel, a működés biztonságát pedig stratégiai célokkal segítsen megalapozni, egy *rendszervezési módszertani segédlettárat* alakítottam ki. Ennek alkalmazását a disszertációban egy stratégiai alapú, cél-, és működési kockázatkezelési folyamatra mutattam be.

Ott részletesen ismertetem a folyamat ajánlott lépéssorozatát, a módszertan - választási pontoktól, a rendszeresen ismétlendő műveleteken át, az e lépéssorozat ismétlendő részéhez való visszatérésig. Ennek alapjait először szintén az informatika speciális esetére hoztam létre, "Requirement specification system / activity Steps Driven evaluation / modelling Method", röviden "RSDM" néven [6].

Itt csak az azóta folyamatosan továbbfejlesztett segédlet újszerű, más területen is használható vonásait emelem ki.

Az ISACA egy ötletét saját tapasztalataim alapján módosítva, nem biztonsági, nem is stratégiai, hanem *Informatikai irányító bizottság felállítását javaslom* [CRM], [17]. Ez állandó bizottság. Célja, a PCUBE-SEC filozófiájával összhangban, hogy együttműködési platform legyen a stratégiai célok kijelöléséért felelős legfelső vezetés, az e célokat üzletiekre lebontó szakterületek, valamint a célok teljesítéséhez járuló részcélok és tevékenységek meghatározásáért, és végrehajtásáért is felelős szak- és támogató területek között. Az ötletet alkalmazva sikerült elérni, hogy ezek a szereplők, az érdekellentéteiken alapuló hagyományos huzakodás helyett összefogjanak, megtalálva közös érdeküket, munkahelyük piaci sikerét [9, 12, 16, 17].

A második fontos rendszerszervezési segítséget a *"folyamattulajdonosok"* kijelölésében adom. Ezt is meg tudtuk csinálni, Informatikai irányító bizottságunk segítségével. Ehelyett adattulajdonosokat kellene kijelölni, mind az ISACA ajánlásai, mind a Magyarországon a pénzintézetekre érvényes törvényi előírás szerint [CRM, COBIT], [10]. Sok helyen láttam már, hogy elkezdték, azt nem, hogy befejezték, és főleg nem, hogy rendszerezetten folytatták volna. Ha ugyanis a *fejlesztés megkezdése előtt* nem kezdik el dokumentálni az adatösszefüggéseket is, utólag ezek feltárása egy kész, összetett, sokelemű számítástechnikai rendszerben már szinte reménytelen. Az üzleti és a támogató folyamatok viszont kialakításuk / létrejöttük után is könnyen azonosíthatóak, felelősükkel, azaz "tulajdonosukkal" együtt. A stratégiai cél - részcél - folyamattulajdonos - stb. táblázatok könnyen létrehozhatóak, és segítségükkel már teljesíthetjük az itt a fogalomtár bevezetésekor említett azonosítási követelményeket. A többi, itt említett fogalom segítségével további rendkívül hasznos táblázatokat, kérdőíveket szerkeszthetünk a folyamatok és azok

tulajdonosai köré, sőt, a részcélokat, az intézkedéseket, de magukat az éppen szereplő szervezeti egységeket / szerepköröket is többféleképpen súlyozhatjuk, a folyamat stratégiai jelentősége szerint, ahogy ezt már korábbi publikációimban részletesen ismertettem [9, 11].

A harmadik itt említésre méltó, de talán legfontosabb rendszerszervezői segédlet a *mérési rendszer* kialakítása. Itt eredményül sosem számokat, hanem összehasonlító relációkat kapunk. A disszertációban sok hasznos, a fogalomtáron alapuló összefüggést mutatok be. Legérdekesebbek talán azok az összehasonlítások, amelyek a kiválósági kritériumok egymástól való sokszor ellentmondásos függőségét mutatják. Egyik ilyen példa a vagyonelem támadásra való "érzékenysége", és a támadás valószínűsége közötti kapcsolat. Egyrészt az érzékenység - természetesen többek között - az elem karbantartásának minőségén kívül függ, például, a "bizalmasság" kiválósági kritérium teljesítésétől, a támadás valószínűsége pedig függ - többek között - az elem stratégiai értékétől, azaz valamely stratégiai céltól való "távolságától". Másrészt az elem távolságát a "rendelkezésre állási" kritériumtól, sajnos, sokszor növelik a bizalmasságára tett erőfeszítések, ahogy azt az intézmények irányításának minősége, és a támadások valószínű sikere közötti komplex összefüggések tárgyalásánál már korábban kimutattam [14].

A "távolságot" azért vezettem be, hogy támogassa az intézményi működés alapvető tényezői jellemzőinek összehasonlítását. A kockázatbecslést végző rendszerszervező kifejezheti ennek segítségével, mi a cégvezetés véleménye az egyes vagyonelemek stratégiai fontosságáról. Ezt a PCUBE-SEC a vagyonelemekhez, és az egyes stratégiai, vagy azok megvalósítását támogató részcélokhoz köthető kockázat becslésébe a következőképpen építi be:

risk (asset, goal) ~ distance (asset, goal) *
probability (asset, goal, attack) *
vulnerability (asset, goal, effort)

(A "*" azt fejezi ki, hogy a vele összekötött "tényezők" a baloldallal egyenesen arányosak.)

Itt "attack" a vagyonelem külső / belső forrású támadását, "effort" azokat az erőfeszítéseket jelenti, amelyek *hozzájárulhatnak* ahhoz, hogy a vagyonelem a (fenti értelemben) a "lehető legjobban" *szolgálja* a "goal" célt. Hasznos lehet, ha ez a cél egy kiválósági kritérium. A "vulnerability" pedig, mint látni fogjuk, egy sérülékenységet kifejező kapcsolat a 3 "paramétere" között.

Fontos itt is a *hozzájárulást* hangsúlyoznunk, elhárítva a biztos siker hamis reményét.

Az itt szereplő kvantitatív, számszerűsíthető valószínűségre, a probablility-re a gyakorlatban a PCUBE-SEC a következő hipotéziseket ajánlja:

/1 **ha** distance (asset1, goal) < distance (asset2, goal)

**akkor**
probability (asset1, goal, attack_x) > probability (asset2, goal, attack_y)
[ahol attack_x, attack_y támadás jöhet akár konkurrens féltől, akár belső ellenségtől

[azaz, **ha** asset1 az adott "goal"-hoz közelebb van,
**akkor** a teljesítéséhez "jobban hozzá tud járulni", mint asset2,
azaz annak valószínűsége, hogy valamilyen attack_x éri asset1 vagyonelemet,
nagyobb, mint azé, hogy valamely attack_y támadás éri asset2-t

/2 **ha** attack_x **és** attack_y ugyanattól az akár külső-, akár belső támadótól jön,
**akkor** a támadó remélt haszna is meghatározó tényező lehet
(különböző támadók hasznát is megpróbálhatnánk persze,
összehasonlítani egy rögzített vagyonelemre, de ezzel itt nem foglalkozunk):

probability (asset1, goal_intr, attack_x) : probability (asset2, goal_intr, attack_y)
~ distance (asset1, goal_intr) : distance (asset2, goal_intr)
ahol goal_intr a támadó egy célja

E megfontolások felhasználásával egy adott "goal_x" cél elérésének költségét alulról, ahogy ezt a disszertációban részletesen elemzem is, a következőképpen becsülhetjük:

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{o}\sum_{f=1}^{3}\sum_{g=1}^{3} \text{cost}\,(g_i, a_j, e_k, p\_d_f, p\_r_g)$$

ahol:

cost ( achievement (goal_x)) a "goal_x" cél elérésének költségét jelenti

$g_i$ : a goal_x cél eléréséhez hozzájáruló célok i= 1, ... n
$a_j$: a $g_i$ célok eléréséhez szükséges vagyonelemek j=1, ... m
$e_k$: a személyzet az $a_j$ vagyonelemekkel kapcsolatos erőfeszítései k=1, ...o
(itt a "kapcsolatos" természetesen nem öleli az összes kívánatos tevékenységet,
csak azokat, amelynek elvégzését tervbe veszik az adott helyzetben)

$p\_d_f$ : az $e_k$ erőfeszítéshez tartozó pillér értelmezési tartomány f=1, ...3
(az erőfeszítést alkotó tevékenységek értelmezési tartománya)
$p\_r_g$ : az $e_k$ erőfeszítéshez tartozó pillér értékkészlet $e_k$ g=1, ...3
(az erőfeszítést alkotó tevékenységek értékkészlete tartománya,
azaz a tevékenység befolyásol valamit a $p_d_g$pillérben).

Fontos megjegyezni, hogy a különféle, önmagukban hasznos célok egymást esetleg - már említett módon - rontó, hatását, de a megvalósításukhoz hozzájáruló erőfeszítések egymást akadályozó, esetleg kioltó hatását sem vettük itt figyelembe. Ezekkel érdemes lehet finomítani az ilyen becsléseket.

## V. Az eredmények hasznosítási lehetősége

A kiválósági kritérium rendszer követelményeinek, és az e kritériumok szerint, valamint a működés alappillérei szerinti osztályozási lehetőségeknek az alkalmazását részletesen

bemutattam a kiszervezési projektek buktatóinak tárgyalásakor. Már a szerződéskötés előtt tanácsos *mindkét* felet megvizsgálni, mennyire felelnek meg e kritériumoknak. Az összes szempont szerint egyszerre érdemes csoportosítani a hiányosságokat, és a javítási teendőket. Mátrixot is mutattam arra, hogy ez az információ hogyan tehető transzparenssé, mutatva azt is, mit kell megjavítani lehetőleg még a szerződéskötés előtt. Ha a Vevő és a Szállító is követi részletes, a PCUBE-SEC proaktív hozzáállása alapján adott útmutatásomat, *mindketten* haszonnal vehetnek részt egy olyan folyamatban, ahol pedig általában nem mindig nyer mindkét fél [11].

Az intézményi működés felülvizsgálata és javítása nemcsak ilyen rendkívüli helyzetben esedékes, érdemes erre rendszeres időközönként visszatérni. Egy PCUBE-SEC tudásbázis sokat segíthet mind a vizsgálati szempontok, mind a vizsgálat eredményeképp kapott teendők meghatározásában.

Még nem foglalkoztam azzal, hogyan lehetne alkalmazni a PCUBE idő-, és erőforráskezelési lehetőségeit a PCUBE-SEC-ben, pedig az intézményi működés területén is elképzelhetőek olyan felhasználói receptek, amelyekben jelentősége van a feltételek, azaz a részcélok / teendők egymás közötti sorrendjének, vagy amelyeknél korlátosan rendelkezésre álló erőforrások használatát kell adott időintervallumon belül megoldani. Ütemezési feladatok megoldásának támogatását szolgáltatás-orientált architektúrákra már vizsgáltam [7].

Érdemes lehet megvizsgálni, kiterjesszem-e a vagyonkockázat fogalmát, a proaktív megközelítéssel összhangban, úgy, hogy ne csak vagyonelemekkel, hanem a működési pillérrendszer másféle erőforrás jellegű elemére is, például emberi erőforrásra is alkalmazható legyen?

A kockázatkezelésnél felmerülő feladatok megoldásának, és ezek költségeinek vizsgálatánál érdemes lehet figyelembe venni a műveletek, és az ezek eléréséhez hozzájáruló célok esetleges kölcsönös függőségét is.

## VI. Irodalmi hivatkozások listája

**Az alábbiakban a következő rövidítéseket használom:**

Information Systems Audit and Control Association; Rolling Meadows, Illinois, USA helyett: "editor: ISACA"

[COBIT] ha mindegy, hogy melyik COBIT verzióról van szó, 1998-tól 2012-ig

[CRM] ha mindegy, hogy melyik verziójú CISA Review Technical Information Manual-ról van szó, 1999-től 2012-ig

**Megjegyzés:** az ISACA folyóirat jelenlegi címe: ISACA Journal
korábbi címe ez volt: IS Control Journal (Information Systems Control Journal)

[1] [COBIT 1998] COBIT Executive Summary, April 1998 2nd Edition; Released by the COBIT Steering Committee and the Information Systems Audit and Control Foundation, editor: ISACA

[2] [COBIT 2000] COBIT® 3rd Edition, July 2000; Released by the COBIT Steering Committee and the IT Governance Institute™ ; editor: ISACA

[3] [COBIT 4.0,] COBIT® 4.0 Control Objectives, Management Guidelines, Maturity Models Copyright © IT Governance Institute® , 2005; editor: ISACA

[4] [COBIT Map] COBIT Mapping; Overview of International IT Guidance, 2nd Edition; Copyright © IT Governance Institute®, 2006; editor: ISACA

[5] [COBIT 4.1] COBIT® 4.1 Framework, Management Guidelines, Maturity Models Copyright © IT Governance Institute® , 2007; editor: ISACA

[6] [COBIT 5, 2010] COBIT® 5 Design Paper Exposure Draft © 2010 ISACA, working paper

*SME - **Subject Matter Experts csoport tagként** közreműködtem a következő 2 munkaanyag elkészítésében:*
[7] [COBIT 5, 2011] COBIT 5.0 Vol. I – The Framework" and "COBIT 5.0 Vol. IIa – Process Reference Guide © 2011 ISACA, working paper
[8] [COBIT 5, 2012] Enabling Processes - COBIT 5 An ISACA Framework
Copyright © 2012 ISACA

*a következő könyvsorozat elkészítésében 1999-től évente közreműködöm, a CRM 2011 kivételével, mint a **Quality Assurance Team** tagja:*

[9] [CRM] 1998 - 2012 CISA Review Technical Information Manual
published yearly; editor: ISACA

[10] [Dahl, et al., SIMULA 67, 1970] Dahl, J., Myhrhaug, B., Nygaard, K.: SIMULA 67 Common Base Language; Norwegian Computing Centre, Oslo, Norway, 1970

[11] [Guldentops, 2012] Guldentops, E.:Where Have All the Control Objectives Gone? They Have Picked Them Every One...; ISACA Journal Vol. 4, 2011, © 2012 ISACA; editor: ISACA, p. 1-4

[11] [Hansen, 1977] Hansen, P. B.: The architecture of concurrent programs Prentice Hall, Englewood Cliffs, New Jersey, 1977

[12] [Hoare, 1978] Hoare, C. A. R.: Communicating sequential processes Comm. of the ACM, Vol. 21, No. 8. Aug. 1978 pp. 666-671

[13] [ISO 12207] Magyar Szabvány MSZ ISO/IEC 12207:2000; Magyar Szabványügyi Testület; Informatika. Szoftveréletciklus-folyamatok (megfelel: az ISO/IEC 12207:1995 verziónak: Information technology. Software life cycle processes)

[14] [ISO 27000] International Standard ISO/IEC 27000 First edition 2009-05-01; Information technology — Security techniques — Information security management systems — Overview and vocabulary; Reference number: ISO/IEC 27000:2009(E); Copyright © ISO/IEC 2009

[15] [ISO G73] ISO Guide 73:2009 (E/F) - First edition 2009 Première édition 2009; Risk management — Vocabulary; Management du risque — Vocabulaire © ISO 2009

[16] [ISO 27001] International Standard ISO/IEC 27001 First edition 2005-10-15; Information technology - Security techniques - Information security management systems - Requirements; Reference number: ISO/IEC 27001:2005 (E); Copyright © ISO/IEC 2005

[17] [ISO 27002] International Standard ISO/IEC 17799 First edition 2005-06-15; Information technology — Security techniques — Code of practice for information security management; Reference number: ISO/IEC 27002:2005(E); Copyright © ISO/IEC 2005

[18] [ISO 27005] International Standard First edition 2008-06-15; Information technology — Security techniques — Information security risk management; Reference number: ISO/IEC 27005:2008(E); Copyright © ISO/IEC 2008

[19] [ISO 38500] International Standard First edition 2008-06-01. Corporate governance of information technology; Gouvernance des technologies de l'information par l'entreprise; Reference number: ISO/IEC 38500:2008(E); Copyright © ISO/IEC 2008

[20] [G. Nagy, 2013] G. Nagy: An interpretation of the COBIT information criteria to operational criteria of voice controlled Ambient Assisted Living systems; in Procds. of the 5th IEEE International Symposium on Logistics and Industrial Informatics, September 5–7, 2013, Wildau, Germany, p. 49-53

[21] [T. I. Nagy, J. Tick, 2014] T. I. Nagy, J. Tick: Self-Organization Issues of Wireless Sensor Networks, in Procds. of the 12th IEEE International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, Slovakia, January 23-25. 2014, p. 29-33

[22] [Szeredi, P., Futo, 1977]: Szeredi, P., Futo, I.: PROLOG Kézikönyv (PROLOG Reference Manual - Hungarian), Journal Számológép, No 3, 4; editor: NIMIGÜSZI, Budapest, 1977.

[23] [Warren, 1974]: Warren, D. H. D.: WARPLAN: A system for generating plans DCL Memo 76, Dept. of Artificial Intelligence, University of Edinburgh, Scotland, 1974

## VII. A tézispontokhoz kapcsolódó tudományos közlemények

[1] Szenes, K.: Automatikus programgenerálás és robotvezérlés a rezolúció elve alapján; egyetemi doktori disszertáció; ELTE TTK Matematikus Szak.

védés: 1976. egyetemi doktori cím: 1977.

[2] Futó, I., Szeredi, J., Szenes, K.: A modelling tool based on mathematical logic – T-PROLOG; Acta Cybernetica, 1981., Szeged, Hungary, p. 363 - 375

[3] Szenes, K.: An application of a parallel systems planning language in decision support - production scheduling; Procds. of the IFIP W.G. 5.7 Working Conf. APMS (Advances in Production Management Systems), Bordeaux, France, 24 - 27 Aug., 1982.
ed.: G. Doumeingts & W. A. Carter, North Holland, 1984., p. 241 - 249
hivatkozott rá a Computer Abstracts: No. 1827

[4] Szenes, K.: PCUBE - an AI system for planning process systems; Procds. of the 5th Symp. on Microcomputer and Microprocessor Applications, Budapest, Hungary, 29. Sept. - 1. Oct., 1987., ed.: OMIKK-TECHOINFORM, p. 551-562

[5] Szenes, K.: Planning the activity schedule of process systems by the means of an AI based system; Procds. of the 27th International MATADOR Conf., 20-21. Apr., 1988., Manchester, ed.: B. J. Davies, UMIST, MACMILLAN Education Ltd.,1988., p. 139 - 144

[6] Szenes, K.: Building a Corporate Risk Management Methodology and Practice EuroCACS 2002 - Conf. for IS Audit, Control and Security Copyright 2002 ISACA, Rolling Meadows, Illinois, USA 24-27 March 2002, Budapest, Hungary

[7] Szenes, K.: On the Intelligent and Secure Scheduling of Web Services in Service Oriented Architectures - SOAs Procds. of the 7th International Symposium of Hungarian Researchers on Computational Intelligence; Budapest, Hungary, 24-25 November, 2006, p. 473-482

[8] Szenes, K.: A szolgáltatás - orientált architektúrák biztonsági kérdései Hungarian - On the security of service-oriented architectures; in: Az Informatikai biztonság kézikönyve, 23. aktualizálás; Verlag Dashöfer, 2006. december, 2.5.1.1 old. - 2.5.14.14 old. - 134 oldal

[9] Szenes, K.: Kockázatkezelés szempontrendszerrel irányított értékelési módszerrel; Hungarian - Classification systems based evaluation in risk management; in: Az Informatikai biztonság kézikönyve, 32. aktualizálás ; Verlag Dashöfer, 2009. február, 8.6.1. old. - 8.6.5.2.2.6 old. - 62 oldal

[10] Szenes, K.: Az informatikai biztonsággal kapcsolatos törvényekről és rendeletekről; Hungarian - On the Hungarian laws and regulations dealing with IT security in: Az Informatikai biztonság kézikönyve, 33. aktualizálás; Verlag Dashöfer, 2009. május, 3.4.1. old. - 3.4.34. old. - 34 oldal

[11] Szenes, K.: Az informatikai erőforrás-kihelyezés auditálási szempontjai, I., II. rész; Hungarian - Auditing outsourcing of IT resources, Part I., Part II. in: Az Informatikai biztonság kézikönyve, Verlag Dashöfer, I. rész: 36. aktualizálás, 2010. február, 8.10. 1. old. – 26. old. (26 oldal), II. rész: 39. aktualizálás, 2010. december 8.10. 27. old. – 158. old. (132 oldal) (összesen 158 oldal)

[12]: Szenes, K.: "IT GRC versus ? Enterprise GRC but: IT GRC is a Basis of Strategic Governance" EuroCACS 2010 - Conference on Computer Audit, Control and Security Copyright 2010 ISACA, Rolling Meadows, Illinois, USA ; 23-25 March 2010, Budapest, Hungary,Tutorial

[13] Szenes, K.: Supporting Applications Development and Operation Using IT Security and Audit Measures in: e-Informatica Software Engineering Journal, Volume 6, Issue 1, 2012, DOI 10.5277/e-Inf120102, http://www.e-informatyka.pl/wiki/e-Informatica, p. 27–37

Scopus: 84885130511

[14] Szenes, K.: Enterprise Governance Against Hacking. Procds. of the 3rd IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2011 August 25–27, 2011, Budapest, Hungary, ISBN: 978-1-4577-1840 DOI: 10.1109/LINDI.2011.6031153 © 2011 IEEE, IEEE Catalog Number: CFP1185C-CDR [CD-ROM], http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6026102, p. 229-233

Scopus: 80555154910

[15] Szenes, K.: Serving Strategy by Corporate Governance - Case Study: Outsourcing of Operational Activities in: Procds. of 17th International Business Information Management Association - IBIMA November 14-15, 2011, Milan, Italy, ed. Khalid S. Soliman, ISBN: 978-0-9821489-6-9, DOI: 10.5171/2011.903755, indexat BDI: Ebsco © 2011 IBIMA, [CD-ROM], p. 2387-2398

[16] Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására; Minőség és Megbízhatóság (Quality and Reliability); kiadó: European Organization for Quality (EOQ) Hungarian National Committee; HU ISSN0580-4485 editor: Pal Molnar; XLVI., 2012. / No 5 p. 252-257

[17] K. Szenes: Operational Security - Security Based Corporate Governance in: Procds. of IEEE 9th International Conference on Computational Cybernetics (ICCC); July 8-10, 2013 Tihany, Hungary; IEEE Catalog Number: CFP13575-USB (pendrive); CFP13575-PRT (printed); ISBN: 978-1-4799-0061-9 (pendrive); 978-1-4799-0060-2 (printed); Copyright @2013 by IEEE. p. 375-378

Scopus: 848868396260

## VIII. 25 független, és 2 belső hivatkozás a doktorjelölt tudományos közleményeire

Jelölt közleményeire a hivatkozások száma összesen:
25 független + 2 belső (a T-PROLOG-gal kapcsolatos cikk 2 társszerzőjétől).