Óbudai Egyetem

Doktori (PhD) értekezés

Biztonságos informatikai alkalmazás portfólió menedzselés

Kovácsné Mozsár Lívia Alice

Témavezető:

Dr.habil. Michelberger Pál

Biztonságtudományi Doktori Iskola

Budapest, 2019

Szigorlati Bizottság:

Elnök:

Prof. Dr. Berek Lajos egyetemi tanár

Tagok:

Dr. habil. Lazányi Kornélia egyetemi docens

Dr. Horváth Zsolt László

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Rajnai Zoltán egyetemi tanár, ÓE

Titkár:

Dr. Kiss Gábor adjunktus, ÓE

Tagok:

Dr. habil Farkas Szilveszter egyetemi docens, BGE

Dr. habil Kerti András, egyetemi docens, NKE

Dr. habil Szádeczky Tamás egyetemi docens, ÓE

Bírálók:

Dr. Beinschróth József egyetemi docens, ÓE

Prof. Dr. Nemeslaki András egyetemi tanár, BME

Nyilvános védés időpontja

……

TARTALOMJEGYZÉK

BEVEZETÉS

A vállalatok egyre nagyobb nyomás alatt állnak a versenypiacon. A költségcsökkentés a vállalati struktúrában sok területet érint. Nemcsak az üzleti terület képviselőinek, vezetőinek, hanem az informatikai menedzsereknek is napi szinten kell foglalkozni a rendelkezésre álló pénzügyi erőforrásokkal, költségallokációval. A költség monitorozás mellett elvárás az, hogy az informatikai terület magas színvonalú szolgáltatást nyújtson az üzleti szereplőknek. Az üzleti igényeknek is alkalmazkodni kell a folyamatosan változó piaci környezethez, ezt követi az informatikai szolgáltatás állandó változása. Napjainkban a vállalatoknál az egyik legfontosabb problémakör, a technológia nyomon követése mellett a folyamatos informatikai fejlesztések megvalósítása és az informatikai szolgáltatás színvonalának a javítása. Az informatika menedzsment egyik alterülete az informatikai alkalmazások életciklusának a nyomon követése, valamint az informatikai alkalmazások monitorozása. Az alkalmazás portfólió menedzsment feladatai közé tartozik az informatikai alkalmazások definiálása mellett a redundáns alkalmazások vizsgálata is. alkalmazások sebezhetőségének vizsgálata, az informatikai kockázatok kezelése, nyilvántartása is beépül a mindennapi informatikai szolgáltatás támogatás folyamataiba. Az informatikai kockázatmenedzsment és az alkalmazás portfólió menedzsment kapcsolatának a vizsgálata fontos szempont a szervezeteknek.

A tudományos probléma megfogalmazása

Értekezésemben az informatikai alkalmazás portfólió menedzsment problémakörét elemzem. Az alkalmazás portfólió menedzsmentre vonatkozó ajánlásokat a legtöbb vállalatnál nem veszik figyelembe, ezért a szervezetek saját megoldásokkal készítenek alkalmazás nyilvántartásokat. Az alkalmazások portfólió menedzselésének az ismertetésével párhuzamosan betekintést adok az informatikai alkalmazásokhoz tartozó pénzügyi információk nyilvántartásának a lehetőségeire és fontosságára. Az informatikai alkalmazás portfólió menedzsment lépéseinek a részletezése mellet megvizsgálom azt, hogy az Informatikai Infrastruktúra Könyvtár (Information Technology Infrastructure Library-ITIL) v3-ban hogyan jelenik meg az alkalmazás portfólió menedzselésre, költségekre és kockázatokra vonatkozó ajánlás.

Az informatikai rendszerek számának a növekedésével az informatikai folyamatokat érintő informatikai kockázatok száma is növekszik. A kockázatok definiálására, nyilvántartására, elemzésére, sok elfogadott nemzetközi keretrendszer, szabvány van érvényben. A kockázatmenedzsmentbe beletartozik az üzleti és az informatikai kockázatoknak a definiálása, nyilvántartása, számszerűsítése, monitorozása. A lehetséges kapcsolódási pontokat vázolom fel az alkalmazás portfólió és informatikai kockázatmenedzsment terület között. Hazai és nemzetközi szakirodalmakat, tudományos és iparági kutatási eredményeket, esettanulmányokat és a saját kutatásom alatt készített mélyinterjúk eredményeit használom fel a célkitűzéseim igazolására.

Hangsúlyt kap a kutatásomban az informatikai kockázatmenedzsment, ami az informatikai kockázatok definiálásával, csoportosításával, értékelésével és elemzésével foglalkozik. Áttekintést adok a kockázatmenedzsmentről, majd megvizsgálom, azt hogyan lehet beépíteni az informatikai kockázatok az informatikai alkalmazás portfólióba. Nem célom a különböző szabványok, ajánlások összehasonlító elemzése, valamint a különböző kockázati keretrendszerek, kockázati modellek összehasonlítása. A témához tartozó ITIL v3, mint nemzetközi informatikai szolgáltatástámogatás ajánlásban lévő alkalmazás portfólió menedzsmenthez, költséganalitikához és kockázatkezeléshez tartozó fejezetrészeket elemzem. Az informatikai irányítási és ellenőrzési keretrendszer, (Control Objectives for IT and Related Technology, COBIT) 5-ös verziónak az informatikai kockázatmenedzsmentre vonatkozó irányelveinek a vizsgálata jó alapot ad az informatikai kockázatmenedzsment megértéséhez.

Célkitűzések

A kutatás alapvető célja, hogy a primer és szekunder kutatási eredményekre alapozva hozzájáruljak az informatikai kockázatmenedzsment és az alkalmazás portfólió menedzsment kapcsolati rendszerének a bemutatásán keresztül az informatikai biztonság területének a fontosságára. Az informatikai alkalmazás portfólió menedzsment elméleti áttekintése után kutatási kérdéseket fogalmazok. Szekunder kutatást végezve elemzem egy lehetséges módját az informatikai kockázatoknak az alkalmazás portfólió menedzsmentbe való beépítését. Kutatásomban kiemelt kérdéskör az alkalmazás portfólió fontossága nagyvállalati körben, valamint az informatikai alkalmazások szintjén megjelenő költség- és informatikai kockázatok analitikája.

A hipotézisek és kutatási módszerek közötti kapcsolatot az 1. ábra illusztrálja.

Kutatási célkitűzéseim:

1. Bemutatni az alkalmazás portfólió menedzsment bevezetését és használatát akadályozó tényezőket.

2. Feltárni az informatikai alkalmazások rendszerszintű költségkezelésének hiányosságait.

3. Megvizsgálni az informatikai kockázatelemzés, -értékelés, és –kezelés beépítési lehetőségét az alkalmazás portfólió menedzsmentbe.

A téma kutatásának hipotézisei:

1. Hipotézis: Feltételezem, hogy a nagyvállalatoknak szüksége van az alkalmazás portfólió kialakítására.

2. Hipotézis: Feltételezem, hogy a nagyvállalatoknak szüksége van az informatikai alkalmazás szintjén megjelenő költséganalitikára.

3. Hipotézis: Feltételezem, hogy az informatikai kockázatok nyilvántartás rendszere beépíthető az alkalmazás portfólióba.

1. ábra Hipotézisek és kutatási módszerek
Forrás: Saját szerkesztés

Kutatási módszerek

- Kvalitatív kutatási módszerek: action research-akciókutatás, esettanulmány feldolgozása, mélyinterjúk készítése és elemzése Grounded Theory-megalapozott módszertan alapján.
- Szekunder szakirodalom feldolgozása: nemzetközi és hazai folyóiratcikkek, iparági elemzések eredményei, nemzetközileg elfogadott ajánlások, szabványok elemzése.

Kvalitatív kutatás

Az empirikus kutatásból a kvalitatív módszertant alkalmaztam arra, hogy igazolást kapjak a feltételezéseimre. Alkalmazott kutatásomban a cél az, hogy a problémakörök vizsgálata után a kutatási eredmények hasznosíthatóak legyen a vállalati életben. A kvalitatív feltáró jellegű módszer, a probléma természetének a megértését szolgálja, többnyire kis mintán végzik és strukturálatlan. Lehetőséget ad a folyamatok mélyebb, részletes megismerésére. Nem tartozik a célok közé statisztikailag igazolni a reprezentativitást. A rugalmasság, interaktivitás jellemzi. Esettanulmány, kísérlet, szakértői interjú, mélyinterjú, fókuszcsoportos interjú módszerekkel végezhető el a kutatás. A kvalitatív kutatás természetes környezetben történik, a kutató beszélgetés alatt megfigyeli a résztvevőket. A kutató nem kérdőívre hagyatkozik, hanem saját maga folyamatosan részt vesz a kutatásban és többféle adatforrást és módszert alkalmazva végez induktív adatelemzést. Lényegében egy interpretáló kutatás, ahol részletesen elemzi az adatokat, témákat, majd a kutatás végén egy holisztikus beszámolót készít. A vizsgálat lehetőséget ad egy komplexebb kép leírására, mivel különböző nézőpontokat vet össze. Adatgyűjtésre interjú, megfigyelés, kísérlet, esettanulmány jellemző. Mélyinterjúk készítésével a szervezetek működésére, folyamataira, problémáira kerestem a választ. Az interjú készítéssel ellentétben a kvantitatív kutatási módszerrel nem az adatok számszerűsítésére, hanem a személyes megkérdezés alapján a tapasztalatok, élmények összegyűjtésére irányul. Az interjú alatt kialakul egy bizalmi viszony a kérdező és a válaszadó között. Az interjúalanyok nem mintavétel alapján kerülnek kiválasztásra, hanem az elmélet alapján, célirányosan. Az interjú helyszíne fontos, hogy megfelelő, kényelmes legyen. Az interjú alatt fontos, hogy az interjúalany beszéljen többet, valamint

az is, hogy ezzel párhuzamosan irányítani is kell a beszélgetést. Jegyzet, hangfelvétel, videofelvétel készítésével lehet az elhangzott információkat rögzíteni. A rögzítés után az átirat készítése a következő lépés. Az átírt szöveg után a szöveg elemzése következik. Ez a legidőigényesebb és legnehezebb lépés. A kondenzáció során az interjút a kutató a saját szavaival összefoglalja. A kategorizáció alatt pedig azt érjük, hogy azonosságokat, eltéréseket keresve csoportokat kell képezni a szövegben. Narratívaalkotás során elbeszélést készít a kutató. Értelmezés, interpretáció során pedig a mély értelmezése történik meg az elhangzott véleményeknek. Az eseti elemzés alatt pedig több különböző eljárás kombinációját értjük [1], [2], [3].

A kutatási témám nagyvállalatok informatikai alkalmazás nyilvántartás megoldásaira, informatikai kockázatkezelésre, informatikai költségelemzésre terjed ki. A kvalitatív kutatás módszertana alkalmas arra, hogy jelenségek, folyamatok fokozatos megértésével természetes környezetben megfigyeléssel, résztvétellel alakítsa ki a kutató a véleményét. Aktuális problémák feltárása után az interjúk elemzéséhez a Grounded Theory-t alkalmaztam. A kapott kutatási eredményeket összevetettem a tanácsadói elemzésekkel, tudományos kutatási eredményekkel és megállapítottam, hogy a felvetett problémák és tézisek összhangban vannak egymással.

Action Research, cselekvéskutatás

Az Action Research-t, vagyis cselekvéskutatást alkalmazom, ami egy reflektív kutatási módszertan. A cselekvéskutatás célja, hogy a kutatásban résztvevők esettanulmányokon keresztül jelentésproblémákat határozzanak meg. A kutató alanya a kutatásnak és a folyamatokat elemzi, részletezi, valamint külső megfigyelő is, így kettős szerepet tölt be. A cselekvéskutatást vagy más szóval akciókutatást először 1946-ban Kurt Lewin körvonalazta. A kutató akkor ért meg valamit, ha megváltoztatja. Az akciókutatás definíciója: „Az akciókutatás célja, hogy együttműködésen keresztül pozitívan járuljon hozzá, mind az emberek valós gondjaihoz egy azonnali problémás szituációban, mind a társadalomtudomány céljaihoz egy mindkét fél által kölcsönösen elfogadható etikai keretben” [4]. Alkalmazásának az előnye, hogy a kutató, mint résztvevő, megérti, és folyamatosan figyelemmel kíséri a folyamatokat, eseményeket. A kutató mellett egy csapat van, aki részt vesz a változásokban. A kutató által létrehozott eredményeknek alkalmazhatónak kell lennie, hogy a szervezetben lévő vezetők adaptálni tudják a mindennapi folyamatokba. A kutató a meglévő ismereteit, tudásanyagát összekapcsolja

a megfigyelés és a részvétel során szerzett tapasztalatokkal, a szakemberek kutatják saját szakmai tevékenységüket, jellemzően a kutató szakmai tudása, értékei vannak a középpontban, nem a tudományos módszertanok.

Az informatika, információs rendszerek kutatási területén már az 1985-ös években használták az akciókutatást [5]. Jól használható az informatikai rendszer fejlesztésénél szerzett tapasztalatokra, hiszen a kutató olyan információkat gyűjt össze, amit a szervezet azonnal fel tud használni és beépíteni a mindennapi működésbe [6], [7], [8], [9], [10]. Az akciókutatás felhasználható szervezeti, emberi erőforrás fejlesztésre és alkalmas üzleti problémák kezelésére. Szervezeti átalakításra vonatkozó tervek kidolgozását támogatja, vagy segítséget nyújt ahhoz, hogy a felsővezetés jobban megértse a működési problémákat és a megoldási javaslatokat a szervezeti változtatásokra [11]. A projektmenedzsment területén lévő folyamatok feltérképezésére is használható kutatási módszer [12], [13].

Creswell 2015-ben az alábbi lépésekben határozta meg az akciókutatást:

1. meg kell határozni, hogy az akciókutatás a legjobb megoldás,
2. azonosítani kell a vizsgálandó problémát, erőforrásokat kell allokálni,
3. az információkat is azonosítani kell, amire szükség van a kutatáshoz,
4. az adatgyűjtés után elemezni kell az adatokat,
5. majd fejleszteni egy tervet az akcióra,
6. terv implementálása és reflektálás a tervre [14], [15].

Négy típusú akciókutatás van:

1. Diagnosztikai cselekvéskutatás (Diagnostic Action Research).
2. Részvételi cselekvéskutatás (Participant Action Research).
3. Empirikus cselekvéskutatás (Empirical Action Research).
4. Kísérleti cselekvéskutatás (Experimental Action Research) [16].

Az akciókutatás a minőségi kutatás módszertana. A hagyományos kutatásokkal összehasonlítva a megértés és cselekvés egyszerre történik, és fontos az érintettek szakmai véleménye is, nemcsak a kutatóé. A kutatásban a résztvevők és a kutató együtt vesznek részt, a probléma azonosítása is közösen történik. Az adatgyűjtés, elemzés, valamint a prezentálás pedig nemcsak a kutatók részére történik, hanem azonnal alkalmazható ismereteket tartalmaz, ami a gyakorlati, vállalati életben felhasználható.

Esettanulmány

Az esettanulmányban a kutató egy külső szemlélő, összegzi a tapasztalatokat, észrevételeket. Nem vesz aktívan részt a tevékenységekben, nem befolyásolja az eredményeket. A kockázatok azonosítására, elemzésére, priorozálására, monitorozására, valamint a kockázati keretrendszerek alkalmazásánál, bevezetésénél szerzett tapasztalatokra jól használható [17]. Informatikai projektekkel, informatikai kiszervezésékkel kapcsolatban felmerült kockázatokat, tapasztalatok összegyűjtésére, illetve az informatikai szoftverek bevezetésénél felmerült kockázatoknak, tényezőknek a vizsgálatára jó módszertan [18], [19], [20]. Az üzleti adatok integritásának a kockázatkezélési modelljére is készült esettanulmánnyal tudományos ajánlás [21]. Az esettanulmányal vizsgálható az informatikai menedzsment, valamint az informatikai stratégiai tényezői egyaránt [22]. Az informatikai szolgáltatás menedzsment területén az informatikai irányításra is készült esettanulmány [23]. Az ITIL implementálásánál szükséges tényezők összegyűjtéséhez jó lehetőség a kutatás során felmerült problémák és észrevételek összegyűjtésére. Az esettanulmányok lehetőséget adnak arra, hogy a szervezetekben történt változásokat részeletesen elemezze és összehasonlítsa a kutató [24], [25]. Informatikai alkalmazás portfólió elemzésére is készült már tudományos tanulmány esettanulmányok alapján [26], [27]. Az összegyűjtött esettanulmányok igazolják, hogy jól illeszthető ez a kutatási módszertan az akciókutatással együtt az értekezésemben.

Grounded Theory

A Grounded Theory (GT), magyar fordítása megalapozott elmélet [28]. Leggyakrabban a társadalomtudományi kutatásokban alkalmazzák. Emellett jól használható más tudományterületen is, ahol a kutatások félig strukturált interjúkra, vagy mélyinterjúkra épülnek. Nincsenek előre definiált kategóriák a fogalmak képzésénél. Nem kötelező a szakirodalmak feldolgozásával kezdeni a kutatási folyamatot. A kódolás, elemzés már az interjú készítése alatt elkezdődik. Az adatokból különböző szempontok alapján létrejött fogalomrendszer közötti kapcsolatrendszert lehet kialakítani. A leggyakrabban a félig strukturált interjúk, mélyinterjúk elemzésénél lehet használni. A GT alkalmas arra, hogy különböző véleményeket, meglátásokat együtt vizsgáljon a kutató Megjelentek kritikák is a Ground Theory alkalmazásával kapcsolatban. Lydar szerint nem jól érthető a módszertan leírása [29].

Két elemzési irányzat alakult ki a kilencvenes években. Glaser a valóságot modellezve, pozitivista megközelítést, Strauss és Corbin [30] pedig a deduktív, vagyis a szakirodalom alapján meghatározott törvényszerűségeket integrálja. A harmadik irányzatot, iskolát Charmaz [31] teremtette meg a munkásságával. 2002-ben továbbfejlesztette a Strauss-i iskolát és a konstruktivista felfogást támogatta. Véleménye szerint a kategóriák létrehozását jelentősen befolyásolja a kutató előzetes tudása, tehát az eredményeket is befolyásolja az előzetes feltevések, az elemzés intuitívabb. Az adatok már tartalmazzák a jelentést a megoldást, tehát a kutató feladata a már meglévő jelentéseknek az elemzése. Objektív és rugalmas felfogás Thronberg informed grounded theory-ja, tehát megalapozott grounded theory módszere tartalmazza a szakirodalmak feldolgozását és az elméleti ismereteket is [32].

2017-ben készült egy tanulmány, Grounded Theory in information system research címen. 43 cikk elemzése alapján a szerzők azt állapították meg, hogy az elemzések során nincs általánosan elfogadott eljárás a kódolásra, többnyire nincs előre létrehozott kutatási terv. A kutatóknak a 81%-a a Strauss-i megközelítés alapján elemezte a kutatási adatait [33]. A biztonságtudomány területén a GT alkalmas a munkavállalók biztonsági magatartásának a vizsgálatára is [34]. Készült tanulmány a GT-vel a kiber terrorizmus vizsgálatára [35], valamint az informatikai szolgáltatások fejlesztésének a lehetséges irányaira is [36]. A katonai-műszaki tudományok területén 2010-ben készült tanulmány katonai vezetők körében, akik részt vettek a 2004-es Tsunamiban a krízis menedzselésében [37]. Katonai szervezeteknél a dolgozók belső szociális internet használatával kapcsolatos vizsgálatánál készített interjúk elemzésénél és női katonáknak, a tapasztalatainak, küzdelmeinek az elemzésére is alkalmazták [38], [39]. Egy 2012-ben készült tanulmányban pedig a GT módszert arra használták, hogy katonai vezetők körben végzett mélyinterjúk alapján kiderüljön, hogyan befolyásolják a képzések átadását a hadsereg egységeiben [40].

A Grounded Theory elfogadásában nagy áttörést jelentett Glaser és Strauss 1967-ben megjelent könyve: A megalapozott elmélet felfedezése: stratégiák a kvalitatív kutatásban, The Discovery of Grounded Theory: Strategies for Qualitative Research [41]. Az elmélet jól alkalmazható a kvantitatív kutatásokban is. Intepretatív, tehát a vizsgált alanyoknak a nézőpontjait is figyelembe kell venni az elemzésnél. A GT módszernek főbb ismérvei közé tartozik az, hogy nyílt kódolással és folyamatos összehasonlítással keletkező új és új fogalmak összehasonlíthatóak. Lényegre koncentrálva, logikai

kapcsolatok, konzisztenciák mentén kell felépíteni az elméletet, az elmélet alapkövei pedig a fogalmak.

A vezetés- és szervezéstudomány területén [42], [43] kockázatmenedzsment és informatikai biztonság [44], informatika használata vállalati körben, informatikai menedzsment [45], [46], projektmenedzsment, szoftver folyamatok vizsgálatára jól adaptálható [47]. Az informatikai szolgáltatásmenedzsment, ITIL bevezetésénél a GT eljárással végzett elemzés segítséget, támpontot ad a vezetőknek arra, hogy a szervezeti stratégia kidolgozásánál milyen tényezőket vegyenek figyelembe [48], [49]. Szoftver folyamatfejlesztésre készített tanulmányban alkalmazták a szoftverfejlesztés gyakorlatának a bemutatására [50]. Az iteratív folyamat elemei: adatfelvétel, elemzés, kódolás, memóírás és a folyamatos összehasonlítás. Az elméleti kódok a terepmunka során feldolgozott adatokból jönnek létre és új elméletek a korábban létrehozott elméletekből állnak össze. A legfőbb eleme az összehasonlítás. Iteratív és ciklikus, mivel egyidőben történik az adatfelvétel, az elemzés és a kódolás.

Az értekezés koncepciója fejezetenként:

Az **első fejezetben** az alkalmazás portfólió menedzselés elméleti témakör kifejtésére szekunder kutatás alapján tudományos és iparági felméréseket használok fel. Az akciókutatás során szerzett tapasztalataimat, tudásomat, ismereteimet fejtem ki az első fejezetben. A nagyvállalatnál az akciókutatás részeként létrehozott application-compliance (alkalmazás-megfelelőség) mátrixot mutatom be.

A **második fejezetben a** mélyinterjúk GT kódolási eredmények körvonalazzák a további kutatási kérdésköröket. A kódolással létrejött fogalmi kategóriák képezik alapját a további elméleti kutatásomnak.

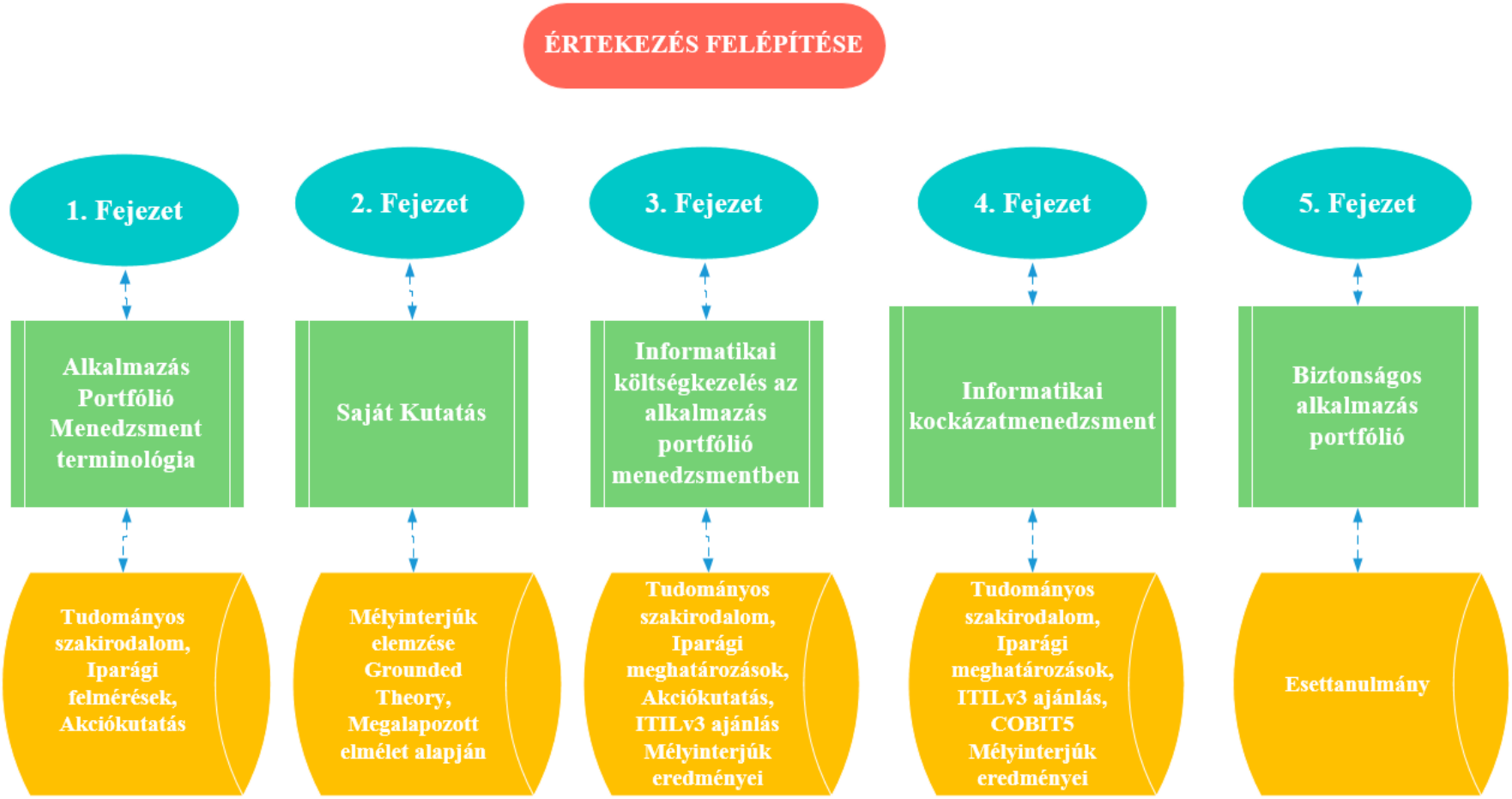
A kutatási problémakör egyik eleme az alkalmazás portfólió menedzsment létjogosultsága, szükségessége nagyvállalati körökben. A másik problémakör az informatikai alkalmazás költséganalitikának a fontossága. A harmadik pedig az alkalmazás portfólió menedzsment és az informatikai kockázatmenedzsment lehetséges kapcsolódási pontjainak a feltárása.

A **harmadik fejezetben** az informatikai szolgáltatások támogatására készült nemzetközi ajánlásnak, az ITILv3-at röviden ismertetetem. Az előnyök, hátrányok ismertetése után a mélyinterjúk eredményeivel támasztom alá a kutatási feltételezéseimet,

miszerint szükség van az alkalmazás portfólió képzésre vonatkozó ajánlásra a nagyvállalatoknak. Akciókutatás eredményét prezentálva mutatok be egy lehetséges megoldást az informatikai költséganalitikára és a nyilvántartásával felmerült problémákra.

A **negyedik fejezetben** az informatikai kockázatmenedzsment elméleti, megfogalmazását, valamint az informatikai kockázatok kategóriákat részletezem. Az ITILv3 és a COBIT5 releváns részeire kitérek.

Az **ötödik fejezetben** az első négy fejezetben felhasznált és összegyűjtött információk, ismeret alapján egy esettanulmányon keresztül igazolom a lehetőségét annak, hogy az informatikai kockázat analitika beépíthető az informatikai az alkalmazás portfólióba. A 2. ábra mutatja az értekezés felépítését fejezetenként, részletezve az alkalmazott kutatási módszereket.



2. ábra Értekezés felépítése
Forrás:Saját szerkesztés

1. AZ ALKALMAZÁS PORTFÓLIÓ MENEDZSMENT

A vállalat vezetése az alkalmazás portfólió menedzsment (APM-Application Portfolio Management) segítségével képes azonosítani azokat az informatikai alkalmazásokat, amelyek redundánsak. A globális nagyvállalatoknak jellemzően a több százezres komplex üzleti folyamatait, több ezer informatikai alkalmazás támogatja. Az alkalmazás portfólió menedzsment egyik előnye az, hogy információt gyűjt és monitoroz, valamint megoldási lehetőségeket dolgoz ki az alkalmazások kategorizálása révén az üzleti és informatikai folyamatok, valamint az alkalmazások optimalizálására. A racionalizáció mérhető előnye az informatikai költségmegtakarítás. A fejezetben akciókutatás eredményét rögzítem. Az alkalmazásoknak nemcsak a nyilvántartása a fontos, hanem a szervezet biztonsági politikájához igazodva a védelem biztosítása is. A akciókutatásomban részletezem azt, hogyan oldotta meg egy nagyvállalat a törvényi előírásoknak való megfelelőség figyelembevételével az alkalmazás portfólió bővítését. Tudományos megközelítés alapján az informatika, mint interdiszciplinális területen belül az információmenedzsmentben gyökerezik. Az informatikai portfólió menedzsment egy folyamatos tevékenység, ami magában foglalja az informatikai alkalmazásoknak a rendszerezését, kategórizálását, monitorozását. Az APM támogatja a vállalatot a versenyelőny megszerzésére az informatikai költségek számbavételén és menedzselésén keresztül. Adott portfólióba a hasonló funkcionalitású informatikai alkalmazások kerülnek, pénzügyi információkkal és alkalmazás jellemzőkkel együtt.

A portfólió megközelítéssel először 1952-ben H. M. Markowitz tanulmányában lehet találkozni. A pénzügyi modellezéshez adott támpontot, a diverzifikáció gyakorlatával foglalkozott, valamint a portfólió kialakításának az elveit is kidolgozta. A portfólió képzéssel különböző szempontok alapján halmazokat lehet képezni, ennek segítségével pedig az összehasonlítás és elemzés egyszerűbbé válik [51]. A pénzügyi portfólió képzés után az informatika területén is megjelenik a portfólió képzés fogalma. Az alkalmazások osztályozását és dimenzióba való sorolásával először McFarlan 1981-ben [52], Ward 1987-ben [53], illetve Kwan és West 2004-ben foglalkozott [54]. 2005-ben Maizlish és Handler definiálta a portfólió képzés lépéseit és előnyeit. Az informatikai portfóliókezelés biztosítja az eszközöket ahhoz, hogyan tud az informatika értéket

teremteni a folyamatok áttekintése mellett, az üzletileg redundáns funkciók kiszűrésével úgy, hogy az eredmény az üzleti terület képviselői, szakértői számára érthetőek legyenek. Az informatikai befektetési döntéseket is támogatja, így a vállalati stratégiához, tervezésekhez tud információkat adni [55]. Az alkalmazás portfólió menedzsment feladatai közé tartozik az informatikai alkalmazások definiálása különböző szempontok alapján. A definiálással párhuzamosan olyan információkat kell összegyűjteni és nyilvántartani az alkalmazásról, amelyek naprakészek, mérhetőek, összehasonlíthatóak a menedzsment részére. Az alkalmazás portfólió menedzsment lépéseit a 3. ábra mutatja. Az összes lépésnél fontos a megfelelő szakemberek, szakértők bevonása az alkalmazás portfólió menedzser koordinálása révén.

Alkalmazás portfólió menedzsment lépései:

1. Az üzleti folyamatok feltérképezése, informatikai alkalmazások regisztrálása.
2. Összes informatikai alkalmazásról nyilvántartást, listát készíteni.
3. Informatikai alkalmazás attribútumok vizsgálata, feltöltése a nyilvántartásba.
4. Portfólió elemzés, redundáns folyamatok, alkalamzás funkciók kiszűrése.
5. Döntések: alkalmazás kivezetés, funkciók integrációja.
6. Folyamatos portfólió monitorozás.

3. ábra Alkalmazás portfólió menedzsment lépései
Forrás: saját szerkesztés

A nagyvállalatoknak a digitális üzlet terjedésével párhuzamosan szükséges a meglévő informatikai alkalmazásoknak a funkcionalitását módosítani, vagy új alkalmazásokat fejleszteni. A nagyszervezetekben a vállalati architektúra menedzsment terület fogja össze az üzleti stratégia által létrehozott céloknak az informatikai

megvalósítását. Jó jel a nagyvállalatok számára, ha felismerik az APM-el elérhető előnyöket és beépítik az informatikai irányításba. Az APM tevékenységeibe beletartozik különböző metrikáknak a készítése az üzleti folyamatokról, technikai adataikról, költségekről. Üzleti folyamatgazdák, szakértők, üzemeltetők, pénzügyi szakemberek összehangolt együttműködésére van szükség az információk összegyűjtésére. Az alkalmazás nyilvántartások számbavételével párhuzamosan szükséges a vállalaton belül az IT biztonsági szempontokat figyelembe venni. Az informatikai kockázatok kezelésére az APM-től elkülönült szervezeti egységek, folyamatok, felelősök vannak. Az üzleti területeket kevésbé foglalkoztatja az informatikai kockázatok megléte egy adott alkalmazáshoz, sokkal fontosabb szempont az informatikai költségek nagysága. Az alkalmazásokhoz tartozó információk kezelése, valamint az informatikai kockázatok kezelése külön dimenzióban történik a nagyvállalatoknál. Az APM elősegíti a nagyvállalatok tevékenységét azzal, hogy a világszerte több ezer informatikai alkalmazást rendszerezetten vizsgálja. Az informatikai alkalmazás portfólió elemzés része az információ gyűjtés a technológiai elemekről, interfész kapcsolatokról, valamint a támogató, fejlesztői csapatról. Véleményem szerint a portfólió menedzsmentet össze kell az architekturális tervezéssel, alkalmazás fejlesztés lépéseivel, informatikai rendszerintegrációs projekt tervezésekkel, informatikai beruházási döntésekkel. Operatív szinten pedig az alkalmazás támogatók, üzemeltetők, pénzügyi elemzők, valamint alkalmazások törvényi megfelelésért felelős személyek bevonása a feltétele a folyamatos információk biztosításához. Az üzleti specifikáció készítésének a szakaszában, valamint a fejlesztés elkezdésénél meg kell határozni, hogy az adott alkalmazás melyik alkalmazás portfólióba fog kerülni. Az ésszerűsítés egyik látható eredménye, hogy átlátható a kapcsolat az informatikai alkalmazások között, és ezáltal az esetleges folyamat, vagy funkcionális redundanciák csökkenthetőek.

2014-ben, Hollandiában három kórházban készült egy empirikus kutatás az informatikai alkalmazások centralizált nyilvántartásáról. A három kórház közül egynek van folyamatosan szinkronizált, naprakész informatikai alkalmazás nyilvántartása. Az esettanulmányból kiderült, milyen akadályokba ütköznek a kórházak, amikor alkalmazás portfólió képzésről van szó. Problémák közé sorolják az informatikai menedzsment, valamint az emberi erőforrások hiányát, illetve kevés a támogatás a felsővezetéstől. A betegek adatainak a naprakész nyilvántartása az egész kórházban nehezen kivitelezhető, mivel több különböző funkcionális területekről kell az adatokat összegyűjteni. Nagy

mennyiségű megörökölt, elavult hardverekkel rendelkezik a kórház. Nehézkes az együttműködés külső speciális szervezetekkel, kórházi szervezeti egységekkel. Az esettanulmány igazolja, hogy van igény központosított informatikai alkalmazás nyilvántartásra [56]. Nagyvállalati körben végzett esettanulmány hasonló problémákat azonosított az informatikai alkalmazások kezelésére. Az autóipari cég, világszerte 7000 informatikai alkalmazást menedzsel. A gyökérokokra világít rá a kutatás eredménye. Az üzleti szereplőknek nincs elegendő információ az informatikai alkalmazásaikról. A vállalati architektek nehezen tudják teljesíteni a projekt határidőket. Kevés az idő a dokunentálásra, így a rendelkezésre álló adatok minősége sem megfelelő. Nem átláthatóak az interfész kapcsolatok az alkalmazások között, így az áramló adatok tartalma sem. A redundáns informatikai alkalmazásoknak a száma növekszik. Megoldásként javasolják az átláthatóbb informatikai irányítást, menedzsmentet, automatikusabb ellenőrzéseket. Adatmenedzsment támogatással, technikai fejlesztések, forráskódok ellenőrzésével, technikai szakértők bevonásával lehetne javítani az informatikai alkalmazás térképen. Az esettanulmány elvégzése után szakértői interjút folytattak a kutatók. Az informatikai alkalmazás portfólióra vonatkozó problémák hasonlóak más iparágban müködő nagyvállalati körökben. Az alkalmazások komplexitása miatt a strukturálásnak az igénye az állami szervezeteknél is megjelenik. Norvégiában végzett tudományos esettanulmány eredménye az, hogy a vállalati hogy az informatikai alkalmazások komplexek, ezen belül is az elavult rendszerek száma magas. A kihívások közé sorolják a szervezeti sajátosságokat, a funkcionális területek működése széttagolt. A bonyolult rendszerek átláthatatatlansága miatt nehéz az informatikai költségeket előre megbecsülni, az elavult rendszekre pedig sokat kell költeni [57]. Az informatikai alkalmazás portfólió menedzsment fontos, hiszen érthetőnek és menedzselhetőnek kell lennie az informatikai szoftverek fejlesztési és karbantartási költségeinek is. Egy informatikai alkalmazás, applikáció adatok és programok kombinációját jelenti. Az alkalmazás portfólió lényegében egy keretrendszer az alkalmazások, valamint az üzleti folyamatok, kockázatok, költségek, adat és információáramlások nyilvántartására és monitorozására.

Az alkalmazás portfólió menedzsment előnyei közé tartozik, hogy az alkalmazás költségek csökkenthetők. A költségcsökkentési lépések és intézkedések, költségek összetétel vizsgálatában adhat segítséget az alkalmazás portfólió menedzsment. Sok szempontból elemezhetőek az alkalmazások, amit egy alkalmazás portfólió

menedzsernek figyelembe kell venni: támogatott üzleti területek, folyamatok, stratégiai céljai a szervezetnek, informatikai alkalmazások életciklusai, meglévő és tervezett üzleti és informatikai projektek. A továbbiakban az alkalmazás tudományos és iparági meghatározásait gyüjtöttem össze.

1.1 Definíciók

Alkalmazás: „Olyan program, amelyet az alkalmazó saját igényei, céljai érdekében használ, és amely a hardver és az üzemi rendszer funkcióit használja” [58].

Alkalmazás (ITIL): egy IT szolgáltatás által megkövetelt funkciókat nyújtó szoftver. Minden alkalmazás egy, vagy több IT-szolgáltatásnak lehet része. Egy, vagy több szerver, kliensgépen futnak [59].

Az Informatikai Auditorok és Ellenőrök Szövetsége (Information System Audit and Control Association, ISACA): „Számítógépes program vagy programcsoport, amely az adatokat egy konkrét feladat végrehajtására dolgozza fel. (Megjegyzés: különbözik a rendszerprogramoktól, mint az operációs rendszer, vagy hálózati vezérlő program, és a rendszer segédprogramoktól, mint a másoló, vagy rendező programok.)” [60].

Vállalati alkalmazás: Integrálnak számítógépes rendszereket, amelyek a vállalat együttműködését és koordinálását könnyítik meg. Az alapvető célja, hogy integráljon alapvető üzleti folyamatokat, mint például értékesítés, könyvelés, pénzügy, készletek és gyártás stb. Az ideális vállalati rendszer képes az összes fontos üzleti folyamatot valós időben irányítani egyetlen szoftver architektúrán keresztül egy kliens szerver platformon. A vállalati szoftver kiterjeszti az alkalmazási körét arra, hogy összekapcsolja a vállalatot beszállítókkal, üzleti partnerekkel és az ügyfelekkel [61].

Alkalmazás portfólió meghatározásai:

ITILv3: „Olyan adatbázis, vagy strukturált dokumentum, amelyet az alkalmazások felügyeletére használnak teljes élettörténetükön keresztül. Az alkalmazás portfólió kiterjed az összes alkalmazás fő tulajdonságaira. Az alkalmazás portfóliót a szolgáltatás portfólió, vagy a konfigurációmenedzsment-rendszer részeként valósítják meg” [62]. A meghatározás arra tér ki, hogy egy nyilvántartást, listát kell készíteni az alkalmazásokról.

A portfólió képzésre vonatkozó lépéseket nem részletezi, így véleményem szerint a portfólió szóhasználat nem pontos.

ISO/IEC 16350: gyűjtemény az alkalmazásokra, melyet az alkalmazás menedzsment szervezet, vagy egy egység az alkalmazás menedzsment szervezeten belül menedzsel [63]. A második része a definíciónak nincs jól körülhatárolva, hiszen nem feltétlen van külön alkalmazás menedzsment egység a szervezeten belül. Az alkalmazás portfólió menedzsmentre pedig sem az ITIL, sem az ISO/IEC 16350 nem tér ki. Az alkalmazás menedzsmentet definiálják, aminek van relevanciája az alkalmazás portfólió menedzsmenttel, de nem ugyanaz. A következő kettő definíció részletesebben határozza meg ezt a területet.

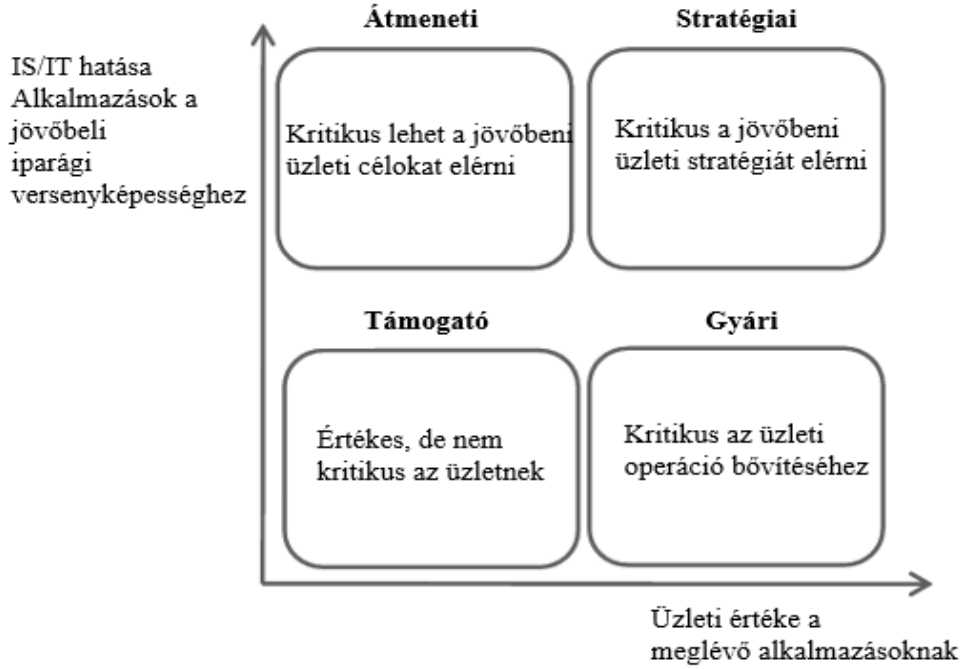
Az APM egy folyamatos szisztematikus és strukturált döntéshozatali folyamat ahhoz, hogy a szervezet különböző szempontok (üzleti és technikai) alapján az optimalizálás érdekében lépéseket tegyen. A megfelelő intézkedések végrehajtásával megoldja az azonosított feladatokat, amik megfelelnek a legfontosabb vállalati céloknak. Az APM elsősorban csökkenti a komplexitását az alkalmazás térképnek egy holisztikus megközelítésen keresztül [64].

Alkalmazás portfólió menedzsment: egy ismétlődő folyamat, amelynek eszköze az információk összegyűjtése és elemzések. Objektív és átláthatóak a döntések az alkalmazások beruházására, konszolidációjára, modernizálni, vagy helyettesíteni az alkalmazásokat [65].

1.2 Alkalmazás portfólió terminológia

Különböző javaslatok vannak az alkalmazás portfólió képzésre. Az egyik tipikus és legfontosabb szempont az üzleti folyamat. Egy globális nagyvállalatnál kevés egy szempont alapján képezni portfóliókat. Az értékesítés tekinthető egy üzleti folyamatnak. Ha egy nagyvállalat több üzleti területre fókuszál és ezek a területek szakmailag elkülönülnek egymástól, akkor az értékesítési elvek, módszerek, folyamatok, így a szükséges adatok, információk, támogató informatikai alkalmazásoknak a funkciói is eltérőek. McFarlan 1981-ben definiálta az alkalmazás portfóliót és négy kategóriát határozott meg az alkalmazásokra. Támogató (Support), gyári (Factory), stratégiai (Strategic), és az átmenetit (Turnaround). A 4. ábra mutatja az alkalmazás portfóliót az

üzleti érték és az informatika rendszer technológia hatásának kapcsolatán keresztül. A stratégiai alkalmazásoknak olyan funkciói vannak, melyek elengedhetetlen feltételei a hosszú távű működésnek, stratégiai célok megvalósításának. Az üzleti értéke magas ezeknek az alkalmazásoknak. Az átmenetieknek kevesebb az üzleti értéke. A támogató alkalmazások fontosak, de nem kritikusak az üzleti területeknek, akár kivezethetőek. A gyáriaknak magas az üzleti értéke, de alacsony a technológiai hatása [66].



4. ábra Alkalmazás portfólió: McFarlan ajánlása
Forrás: [66]

John Ward 1987-ben pedig hat különböző mátrix alapú alkalmazás menedzsment alapján egy új mátrixot hozott létre. John Ward and Joe Peppard [67] az alábbi négy kategóriát állapította meg:

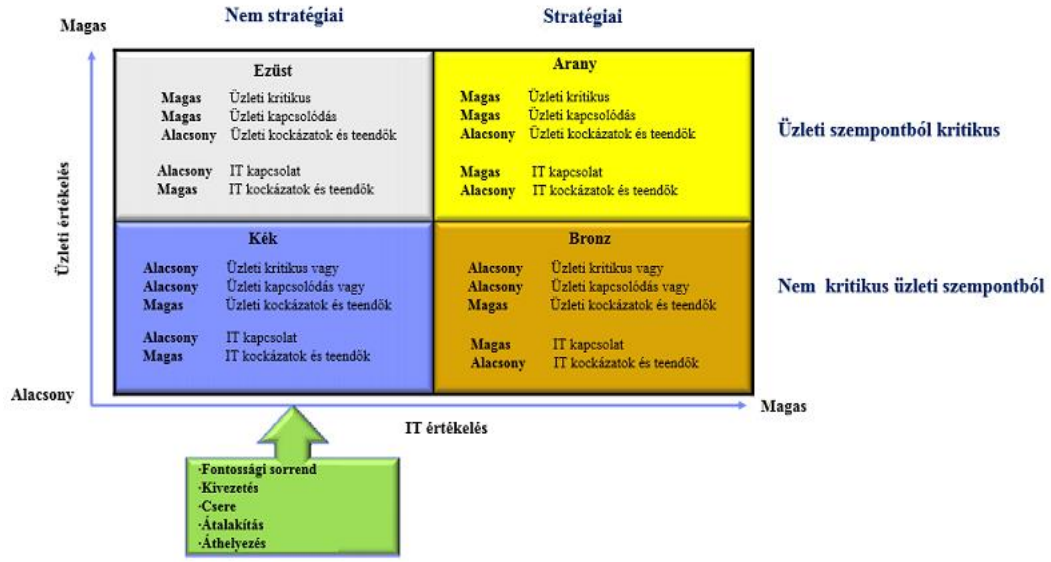
Első kategóriába a stratégiai alkalmazások tartoznak. A stratégiai alkalmazások korszerű technológiai háttérrel rendelkeznek. A legkritikusabb üzleti folyamatokat támogatják, mint például a pénzügyi eredménykimutatásokat és a mérleg összeállítását. Ezekre az alkalmazásokra költenek a legtöbbet a szervezetek, hiszen az üzleti értékek növeléséhez nagyban hozzájárulnak. Lekapcsolásukra, kivezetésükre nem dolgoznak ki akcióterveket. Ezekbe az alkalmazásokba integrálják az elavult alkalmazások funkcióit. A fejlesztésük, támogatásuk nagyon költségigényes.

Második kategóriába tartoznak a magas potenciálú alkalmazások, melyek a kutatási és fejlesztési területet támogatják. Nem integrálnak üzletileg kritikus funkciókat ezekbe az alkalmazásokba, de költségigényesek. Ha megfelelően támogatják az üzleti tevékenységeket, akkor a stratégiai csoportba kerülnek.

Harmadik kategóriába a kulcs operatív támogató alkalmazások sorolandók, tehát azok az alkalmazások, melyektől függ az üzletnek a sikeressége. Javítja a meglévő üzleti tevékenységeknek a teljesítményét. Ezek többnyire integrált rendszerek, melyek a legtöbb esetben elkerülik a duplikált funkciókat.

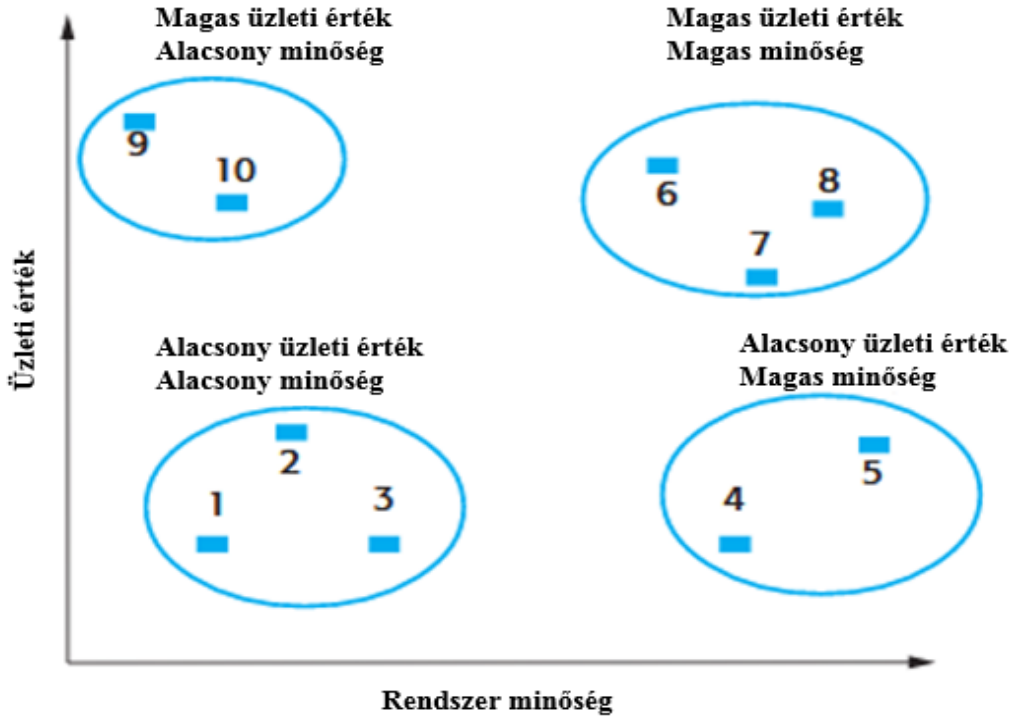
Negyedik kategória pedig a támogató alkalmazások halmaza. Ezek nem kritikusak az üzleti területeknek, de sok szempontból értékesek. Nem sokat költenek ezekre az alkalmazásokra. Minőségüket, technológiájukat tekintve sem kiemelkedőek.

A nagyvállalati, üzleti világban képzett portfólióra több elmélet is van. Az amerikai kongresszus 1996-ban fogadta el az informatikai beruházás portfólió képzére a Clinger-Cohen törvényt [68]. A rövid távú tervezések helyett, a hosszú távú stratégiát, célkitűzéseket támogatja. Az informatikai projektek, beruházások csoportosítása a kockázatok, vagy a megtérülés alapján történhet. Az informatikai eszközökben, a rendszerekben való komplexitást, valamint a kockázatokat tudják csökkenteni. A portfólió szintű elemzések lehetőséget adnak arra, hogy a vállalati felsővezetők lássák a kockázatok és megtérülések kapcsolatrendszerét. Az IBM globális nagyvállalat által kidolgozott besorolás lényege, hogy az alkalmazásokat négy kategóriába kell sorolni [69]. Eltérés a részletezett dimenzióktól, hogy színkategóriákat használva emeli ki az egyes csoportokat, illetve figyelembe veszi a kategóriák képzésénél az üzleti kockázatokat és az ebből eredő feladatokat. Az 5. ábra mutatja kék színnel jelölve azokat az alkalmazásokat, amelyeknek az üzleti értékelése és az IT értékelése is alacsony. Az IT kockázatok és az üzleti kockázatok magasak ebben a kategóriában. Valószínűsíthető, hogy olyan alkalmazások tartoznak ide, amiket ki kell vezetni, de nem lehet egyik napról a másikra lekapcsolni. A bronz színkategóriába olyanok tartoznak, amelyeknek az üzleti kritikussági szintje alacsony, de az üzleti és informatikai kockázatai magasak. A sárga színbe az üzletileg kritikusak vannak sorolva. Az informatikai és üzleti kockázatok alacsonyak. A szürkével jelöltek pedig magas informatikai kockázatokkal járnak, üzletileg alacsony kockázatúak, nem stratégiai alkalmazások.



5. ábra Alkalmazások kategórizálása informatikai érték és üzleti érték alapján
Forrás: [69]

A továbbiakban egy olyan alkalmazás kategóriát elemzek, amiről az eddigi portfólió képzési elméletek nem tettek említést. A „legacy” alkalmazások, más néven öreg alkalmazások, amelyek elavult technológiával rendelkeznek. A későbbiekben az elavult jelzőt fogom használni. Ezek az alkalmazások kockázatosak, költségigényesek, de gyakran előfordul, hogy a stratégiai alkalmazás kategóriába kell sorolni. A legtöbb globális nagyvállalat szakértői küzdenek azzal a feladattal, hogyan lehet lecserélni ezeket az alkalmazásokat, és ezzel párhuzamosan az interfészeket kiépíteni a modernebb technológiával készült alkalmazásokkal. Sommerville 2009-ben modellezett egy mátrixot az elavult alkalmazásokra [70]. A mátrixban a rendszer minőségét és az üzleti értéket mérve négy kategóriát különböztet meg. A kutató meglátása az, hogy az elavult rendszereket teljesen le kell kapcsolni, vagy minimális szintre kell csökkenteni a fejlesztést rajtuk. Az utolsó opció a teljes kivezetés, lecserélés. Az alacsony minőségű és költségű rendszereket mindenképpen érdemes lekapcsolni. A magas üzleti értéket képviselő alkalmazások nagyon drágák, de érdemes a fejlesztésükre pénzt allokálni. A magas minőségű, de alacsony üzleti értéket képviselő alkalmazásokat pedig célszerű lekapcsolni. A magas minőségű és magas üzleti értéket hordozó alkalmazásokat folyamatosan támogatni, fejleszteni kell. A négy kategóriát a 6. ábra szemlélteti



6. ábra A rendszer minősége és üzleti érték alapján alkalmazáscsoportok
Forrás: [70]

Tudományos körökben készített esettanulmányok igazolják az APM-nek az előnyeit. Az architektúrális szinten jelen lévő tervezésnek egyik eleme az alkalmazások életútjának a tervezése. Az informatikai stratégia támogatása az informatikai architektúra és üzleti architektúra közös együttműködésén alapszik [71], [72], [73]. Célszerű az alkalmazás portfólió képzésnél az összes interfészről, támogatott üzleti folyamatokról képet, ábrát készíteni. Sokkal könnyebb az összehasonlítás, elemzés, ha vizualizálva vannak a folyamatok, interfész kapcsolatok az alkalmazások között. A rendszerek funkcionalitása közötti kapcsolatok, a támogatott üzleti folyamatok leírása, illetve költségek, kockázatokok felsorolása tartozik a portfólió képzés lépéseibe [74]. 2010-ben készült egy esettanulmány arról, hogyan csökkentsék az alkalmazás fenntartási és fejlesztési költségeit. A kihívás egy integrált adatbázis létrehozása volt. A megoldásban azonosították a redundáns alkalmazásokat, osztályozták a stratégiai értékük alapján, illetve minőségi besorolás alapján. Lehetőség volt a fejlesztési feladatok összevonására, így a portfólió képzés után az alkalmazások száma 70%-al csökkent. A Szolgáltatási Szint Megállapodás (Service Level Agreement, SLA) az üzleti priorítás alapján lettek kötve, valamint a fejlesztési költségeket 20% -al csökkentették [75]. Egy autóipari vállalatnál készített esettanulmány emprikus elemzésen keresztül mutatja be, hogy 3656 informatikai

alkalmazás menedzselésénél már fontos szempont az, hogy az egyes költségelemek mihez rendelhetőek. A támogatott interfészek száma, üzleti folyamatok szoros kapcsolatban vannak a működési költségekkel és az incidensek számával [76]. 2015-ben 112 szövetségi kormányzati taggal készítettek egy felmérést. A válaszadóknak csupán a 12.5%-a állította azt, hogy van megfelelő alkalmazás portfólió elemzés a szervezeteknél. Általánosságban hiányosak az ismereteik az informatikai alkalmazásukról. 77.7%-a válaszolta, hogy nem biztosak abban, hogy a régi alkalmazásokat le kell kapcsoln [77].

A továbbiakban néhány iparági felmérés eredményét összegzem az alkalmazás portfólió szükségessének a fontosságára. 2014-ben a CENTRIX Software vállalat 100 angol informatikai vezérigazgatóval készített felmérét. Az informatikai vezetők 75%-a válaszolta azt, hogy kulcsfontosságú az alkalmazások teljes portfóliójának a megértése. A válaszadók 74%-a nyilatkozott arról, hogy az egyik legnagyobb kihívás a szervezetben megérteni azt, hogy mi történik az alkalmazásokkal. A vezetőség 69%-a közölte, hogy a céljaik között szerepel menedzselni, tervezni, racionalizálni és optimalizálni az alkalmazás portfóliójukat, hogy illeszkedjenek az üzleti igényekhez. Ugyanilyen arányban válaszolták a vezetők, hogy a racionalizáció eredményeképpen a futtatási költségek csökkentésével erőforrások, tehát informatikai eszközök, személyek tudnak felszabadulni. 38%-a a szervezeteknek manuálisan menedzseli azt, hogy mennyire hasznosak az alkalmazások. A szervezetek, akik ebben a felmérésben részt vettek felfigyeltek az alkalmazás portfólió a fontosságára. Azonban nincsenek felkészülve a felügyeletére és nincs kialakítva egy különálló szervezeti egység az alkalmazások menedzselésére [78].

Néhány idézet az informatika menedzsmentjétől, mely a Mega cég 2012-es felmérésében szerepel:

„Az összes előírásoknak kialakított technológiákat, amit az idő felhalmozott, nagyon drága fenntartani.”

„A fúziók és felvásárlások után túl sok a redundancia az alkalmazások között”

„Nem tudjuk mennyi alkalmazásunk van, körülbelül 10000”.

„Az informatikai költségvetés csökkentésével a célunk az, hogy a támogatott alkalmazások száma 800-ról 500-ra csökkenjen.” [79].

Az alkalmazás portfóliók folyamatos monitorozásával a következő szervezeti változások, folyamatok támogathatóak:

- Fúziók és felvásárlások

Bármilyen szervezeti átalakulásnál naprakész és pontos lista van részletes információkkal az alkalmazásokról.

- Üzleti folyamat menedzsment

Az alkalmazás racionalizáció segít abban, hogy az üzleti folyamat redundanciák kiszűrhetőek legyenek, valamint kockázatokat lehet csökkenteni hosszú távon. Az üzleti és informatikai területek közötti kommunikációt támogatja, ha a folyamatok átalakításánál rendelkezésre állnak és naprakészek az információk.

- Törvényi megfelelősség biztosítása, auditok

Ha tudja a szervezet, hogy mely folyamataik, alkalmazásaik támogatnak üzletileg és technikailag kritikus üzleti folyamatokat, akkor a törvényi előírásoknak könnyebb megfelelni. Az APM-nek a része lehet az alkalmazásokhoz rendelhető dokumentációk meglétének az ellenőrzése, monitorozása. A dokumentációk meglétével jobban ellenőrizhetők az alkalmazáshoz kapcsolódó folyamatok, tevékenységek. A nagyvállalatoknál ennek a tevékenységnek a megszervezése és koordinálása komplex feladat. Különböző területeknek a szakértőit kell bevonni.

- Vállalati architektúra, informatikai stratégia

Új folyamatok integrálása, interfészek kiépítésénél támogatja az alkalmazás nyilvántartás a mindennapi működést. Nagyvállalatoknál jellemző, hogy az üzleti, informatikai tervezők (IT architect) együtt dolgoznak az alkalmazás portfólió menedzserrel. A technikai tudás az informatikai tervezők birtokában van, a költség adatok és részeletes információk az alkalmazásokról pedig az alkalmazás portfólió menedzsereknél.

- Vendor menedzsment, kiszervezés

A vendormenedzsmenttel foglalkozó területeknek támogatást ad az alkalmazás portfólió a naprakész és precíz információkkal. A külső szállítok kezelése sok kockázattal jár. Az informatikai folyamatok, tevékenységének kiszervezését kellően megkönnyíti, támogatja, hisz a tárgyalásoknál, átadás-átvétel folyamatában a szervezet azonnal biztosítani tudja a szükséges adatokat. A tárgyalások után nem kell időt, pénzt fordítani

arra, hogy a szervezet összegyűjtse az információkat, dokumentációkat az alkalmazásokról. A jogi keretek létrehozásánál előny az, ha az alkalmazás nyilvántartás aktuális és transzparens.

- Kockázatmenedzsment

Az előforduló alkalmazás hibák számának a csökkentése és a kockázatok kezelése is részét képezheti az alkalmazás portfólió menedzsmentnek. A hibák kapcsolódhatnak technikai elvárásokhoz, készségek hiányához, kiber támadásokkal szembeni sebezhetőséghez.

- Költségcsökkentés

A fejlesztési, futtatási költségek csökkentése az IT összköltségek csökkentését eredményezi. Új alkalmazások bevezetésénél, meglévő alkalmazások kivezetésénél, illetve élesben működő alkalmazások költségvizsgálatánál nyújt konzisztens információkat. Megkönnyíti a következő, új technológiával fejlesztett informatikai alkalmazások migrációját. Proaktív megközelítést is ad a problémák megoldására [80].

Az informatikai osztályoknak a feladata az üzleti folyamatok folyamatos kiszolgálása. Az üzleti életben sok olyan eset fordul elő, amikor szükség van az informatikai alkalmazások pénzügyi vizsgálatára, elemzésére különböző szempontok szerint. Egy globális nagyvállalatnál, ahol az informatikai alkalmazások száma a több ezért is meghaladja, a pénzügyi elemzések az alkalmazásokra nemcsak a mindennapi folyamat részei, de a stratégiai döntések részét is képezik. Ha a vállalatok igényét elemezzük a felhő alapú megoldásokra, akkor azt látni, hogy az adatok, információk integrációjára szüksége van a szervezeteknek, ehhez pedig az informatikai alkalmazásokat felül kell vizsgálni. Az alkalmazás portfólió képzés első lépése az információk összegyűjtése, strukturálása, elemzése az informatikai alkalmazásokról. A következő lépés a racionalizáció. Az ésszerűsítésnél figyelembe kell venni a szervezeti felépítést, struktúrát, vállalati architektúrális keretrendszert. A vállalati architektúra magában foglalja az üzleti folyamatok, adatmodellek, infrastruktúra közötti kapcsolatrendszert. Fontos tényező még az informatikai szolgáltatások minősége, komplexitása, vállalati kultúra, az üzleti és informatikai terület kommunikációja. Egy európai bankban, ahol 273 informatikai alkalmazás van, a szervezeti felépítés, elkülönült funkcionális területek miatt a folyamatok is összetettek [81], [82], [83]. Alkalmazás

portfólióba valamilyen szempontrendszer alapján kell az alkalmazásokat sorolni. A szempontrendszer kialakításának alapja az üzleti folyamatok csoportosítása. A racionalizáció azt jelenti, hogy átlátható, transzparens tényezők mentén a duplikált üzleti funkciók kiszűrhetőek, tervet lehet kidolgozni az egyes alkalmazások kivezetésére, lekapcsolására. A következő fejezetben egy akciókutatáson keresztül mutatom be az alkalmazás portfólió menedzsment létjogosultságát, fontosságát egy nagyvállalati környezetben.

1.3 Akciókutatás

A részvételi akciókutatásom egy nagyvállalatnál zajlott. A probléma feltárásánal aktívan közreműködtem, szakmai tudásomra is szükség volt a projekt során. A projektben a döntéseket közösen hoztuk a csapat tagjaival. A multinacionális nagyvállalat, több mint 300.000 alkalmazottat foglalkoztat és több, mint 100 országban van jelen világszerte. Termékei közé tartozik az elemzés, felhő alapú megoldások, értékesítő megoldások, szoftvergyártás. Szolgáltatásai közé pedig az üzleti tanácsadás, technológiai szolgáltatások. Szervezeti felépítését tekintve globálisan széttagoltan vannak az üzleti egységek, folyamatok. A széttagoltság miatt az informatikai szolgáltatások nincsenek központosítva. A digitális átalakítás miatt a szervezetben a technológiák megújítása mellett, az informatikai alkalmazások felülvizsgálatára, részletes nyilvántartás elemzésére szükség volt. A digitális átalakításhoz nélkülözhetetlen a rugalmasság, gyors változtatási alternatívák az informatikai alkalmazásokban. A korábbi technológia megoldások elavultak, és az agilis informatikai szolgáltatások, valamint a felhő alapú megoldások irányába terőlödött a transzformáció. Az agilis integrációs architektúra részeként a hibrid integrációs platform keretrendszerre való átállás miatt kiemelten fontos volt az informatikai alkalmazás térkép, nyilvántartás. A zökkenőmentes automatizálás és a professzionális szolgáltatás nyújtása a vállalat számára az elsődleges cél. A nagyvállalatnak saját belső keretrendszere volt arra vonatkozóan hogyan kezeli az informatikai alkalmazásoknak a törvényi megfelelőségét. Egy belső audit több hónapig is eltartott. A külső auditot a KPMG és PWC nagyvállalat végezte. A különböző jogszabályokban és nemzetközi szabványokban lefektetett követelményeket figyelembe véve kellett megfelelően működnie az informatikai alkalmazásoknak. Az információk összegyűjtésére interjúkat alkalmaztam és részt vettem a heti projektmegbeszéléseken.

Vállalati adatokat, szervezeti diagramm, technikai dokumentációkat nem hozhatok nyilvánosságra. Arra kerestem a választ, miért alkalmaz a nagyvállalat alkalmazás portfóliót, hogyan képez portfóliókat és a nagyvállalatban milyen szereplők, hogyan vesznek részt ebben a menedzselési folyamatban. A következő kérdéskör arra irányult, miért szükséges az informatikai alkalmazásokhoz tartozó dokumentációk listájának a megléte, és ez hogyan függ össze a törvényi előírásokkal. Az akciókutatás lépéseit rögzítettem. Az előzmények, kiindulási helyzet leírása után a célokat, kihívásokat részleteztem, végül a létrehozott application- compliance mátrixot szemléltetem. A felmerült problémákat, jövőbeni fejlesztési lehetőségeket összegeztem a vállalati tapasztalatok után.

Az első fázisban összegyűjtöttem az információkat arról, hogyan történik az alkalmazás portfólió menedzselés. A folyamatok megismerésével párhuzamosan az akciókutatásban résztevők egy köre változott. Az APM a nagyvállalatnál, már több évtizede jelen van az informatikai architektúra menedzsment részeként. Szervezeti felépítést tekintve, az architektúrális menedzsmenttel egy szinten helyezkedik el az alkalmazás portfólió menedzsment. Az üzleti folyamatok modellezése és a hozzájuk rendelhető informatikai alkalmazások definiálása az informatikai tervezők feladatai. Az APM kialakításnál, a legnehezebb feladata az volt a felső vezetésnek, hogy mi alapján csoportosítják az alkalmazásokat, tehát mi a vezérfonala a portfólió képzésnek. A bevált és gyakorlott módszer üzleti folyamatokat, szervezeti egységeket figyelembe venni. Annak eldöntése, hogy pontosan milyen alkalmazás kerülhet az adott alkalmazás portfólióba nagyon komplex. Az üzleti és informatikai közép és felsővezetőknek, alkalmazás portfólió menedzsereknek, üzleti és informatikai tervezőknek kell együttműködni. Az alappillérek felállítása után a precíz, mindenki számára érthető dokumentálás, adminisztrálás a feladat. Az alkalmazás portfólió menedzsment tevékenységei közé tartozik az alkalmazás portfóliók rendszeres felülvizsgálata, a portfólióban lévő alkalmazások részletes, analitikus nyilvántartása mellett, az alkalmazás portfóliók között az alkalmazások áthelyezése. A nyilvántartások folyamatos karbantartásának a része az volt, hogy felülvizsgáltuk, hogy az alkalmazások tényleg az adott portfólióba kell, hogy legyenek.

A kiinduló helyzet: Minden informatikai alkalmazást, ami részt vesz a nagyvállalatnak az informatikai szolgáltatási tevékenységében egy alkalmazás portfólióba kell sorolni. Adott portfólióba kerülnek olyan informatikai alkalmazások,

melyek földrajzilag eltérő helyen vannak, különböző a technológiai megoldás, platform, programnyelv, végfelhasználók száma. A lényeg, hogy egy adott alkalmazás portfóliót egységként kezeljen a felső menedzsment a stratégiai tervezéseknél, mint például a költség allokáció. A portfólióban lévő alkalmazásokról ugyanazt kell nyilvántartani. Az alkalmazás portfólió képzést meghatározza az, hogy milyen iparágban van az adott nagyvállalat, milyen termékeket állít elő, milyen szolgáltatásokat nyújt a piacon. A nagyvállalatnak, ahol az akciókutatást végeztem, 12 alkalmazás portfóliója van. A 12 portfólió felsorolása nem lehetséges titoktartási okok miatt, de egy portfólió bemutatása részletesen igen. A portfólió angol megnevezése: Order to Cash, vagyis „Fizetési Alkalmazások" portfóliója. 864 informatikai alkalmazás van a portfólióban. A portfólióban szereplő informatikai alkalmazások támogatják az üzleti folyamatnak azt a részét, amikor beérkezik egy megrendelés a vevőtől és megtörténik a feldolgozása. A partnerekkel kötött szerződéseknek a menedzselése, hardverrel, szoftverrel kapcsolatos pénzügyi információk, liszensz kezeléssel, logisztikával kapcsolatos információk, számlák kezelése, pénzügyi számlázési üzleti folyamatokat támogató informatikai alkalmazások vannak besorolva. Integrált adatbázis támogatja az információk tárolhatóságát. Az adatbázisból Cognos szoftverrel lehet riportokat, kimutatásokat lekérni. Az APM bevezetése a Chief Information Officer (CIO) szervezetébe több részletben történt. A projekt első részében 55%-kal csökkentette az alkalmazásuk számát és 40%-kal a karbantartási költségeket. A folyamatos modernizációval párhuzamosan a hardver, karbantartási és liszensz költségek csökkentése mellett, az új technológiák alkalmazásával új üzleti lehetőségek nyíltak meg. Az alkalmazások kritikus szintjének a besorolásával az SLA összehangolásával elkerülte a magas SLA hozzárendelését az üzletileg kevésbé kritikus alkalmazásokhoz.

Az alkalmazásokról az attríbutum egy informatikai rendszerben található, amelyből kinyerhetőek adatok Excelben. Az exportált Excel adatból készítettem néhány kimutatást, amit szemléltetek. A 7. ábra egy megoszlást mutat a 6. számú portfólióra. A kördiagramm alapján jól látható, hogy magas az arány az elavult rendszerekre vonatkozóan. Ez egy olyan portfólió, ahol régi technológiai megoldásokkal támogatnak ügyfél szerződésekhez, megrendelésekhez üzleti folyamatokat. A kihívások az APM-ben: **Szervezeti felépítés, kultúra, hierarchia:** a lehető legtöbb információt szükséges összegyűjteni az alkalmazásokról. Mivel komplexebbek a folyamatok, annál nehezebb a pontos adatok konszolidációja. Az információk összegyűjtése sok időt vesz igénybe a

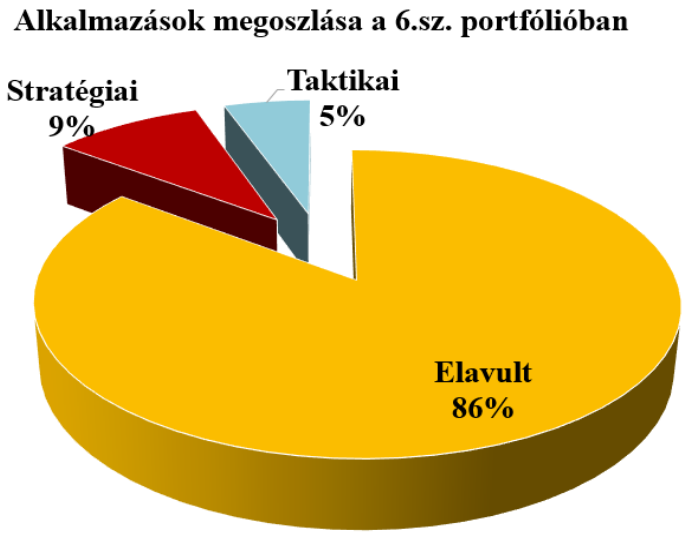
szervezeti felépítés miatt. Eltérő időzónában lévő szakemberek, hozzáértők idejének az összehangolására van szükség.

Duplikációkat, átfedéseket nehéz azonosítani: a legtöbb esetben lehetetlen eldönteni, hogy mely folyamatok, funkciók duplikáltak a különböző alkalmazásokban. Gyakran előfordul, hogy ugyanazt az üzleti folyamatot támogatja két különböző alkalmazás, elkülönülten, különböző régiókban. Mivel a törvényi előírások, szabályok mások két országban, ezért nem lehetséges az, hogy egy alkalmazás támogassa ugyanazokat az üzleti folyamatokat.

Felsővezetői támogatás hiánya: A több hónapos, vagy éves projektek eredménye után sikerült karbantartási, működtetési költségeket csökkenteni. A felmérés előrejelzései alapján a felsővezetés nehezen látja és érti meg az APM előnyét a szervezeti működésben.

Az 1. táblázat a portfólió analitikát szemlélteti. A 6-os számú, úgynevezett Order to Cash portfólióban üzleti folyamat alapján csoportosítják az alkalmazásokat. 3 típusú alkalmazás van, és 10 alkategória a portfólión belül. Az alkalmazás portfólió menedzsernek elsősorban azzal az alkalmazásokkal kell kezdenie a portfólió elemzést, ahol az 'ismeretlen' jelölés van az alcsoportban. Ebben az esetben az alkalmazás leírása, archtektúrális ábrából kiindulva egyeztet az alkalmazás tulajdonossal és az üzleti terület képviselőivel. A 2-5. táblázat részletezi azt, hogy milyen attríbutumok vannak a szoftverben, amelyik nyilvántartja az alkalmazásokat. Az ismeretlen alkalmazásokra a portfólió menedzser egy riportot készít és megpróbálja megérteni, miért nincs alkategóriája ezeknek az alkalmazásoknak. Az akciókutatásomban tapasztaltam, hogy bizonyos esetekben alkalmazás transzfert kell végrehajtani. Ez azt jelenti, hogy adott portfólióból, a példán szemléltetve, a 6. sz. portfólióból egy másik portfólióba helyezni az alkalmazást. Ehhez a másik portfólió menedzserrel, üzleti és technikai tervezőkkel szükséges egyeztetni. A döntésig az egyeztetések több hónapot is igénybe vettek. Az alkalmazáshoz tartozó költségek is a másik portfólióba kerülnek ilyen esetekben.

Az application- compliance mátrix létrehozásának a fő célja a portfólió átláthatóságával a belső és külső ellenőrzések támogatása, az auditok sikerességének a támogatása. Megfogalmaztuk a lista készítés lépéseit, idejét, a felelősöket, illetve a nyilvántartásra vonatkozó követelményeket. A dokumentációkra vonatkozó előírásokat egy külső szabályzat határozta, vagy a szervezetnek a belső, saját ellenőrzési szabályrendszere.



7. ábra Alkalmazások típusának megoszlása az alkalmazás portfólióban
Forrás: saját szerkesztés

Definiálva van a dokumentációk létrehozására, karbantartására, monitorozására vonatkozó részletes lépések és a szabályrendszerek a felelősökkel együtt. A compliance terület szakértői együtt működnek az alkalmazás támogató csapattal. Az alkalmazáshoz rendelhető dokumentációk: adatvédelem, vagy a folyamatok, információk dokumentálása, adatok kategorizálása, üzletmenet folytonossági tervek (Business Continuity Plan, BCP), adatvédelem ellenőrzési pontok az üzleti és informatikai folyamatokban. A nyilvántartás kezelése, folyamatos frissítése is komoly szervezést igényelt.

Típus	Üzleti szerződések menedzselése	Globális logisztika menedzselése	Hardver eszközök menedzselése	Igény tervezés	Ismeretlen	Szoftver eszközök menedzselése	Szoftver liszenszek menedszelése	Ügyfél és hardver szoftver megrendelések	Ügyfél számla menedzselése	Ügyfél szerződések kezelése	Összesen
Elavult	385	85	7	50	17	3	6	146	37	2	**738**
Stratégiai	17	3	2	42	0	1	0	13	0	2	**80**
Taktikai	27	2	0	2	0	0	0	12	2	1	**46**
Összesen	**429**	**90**	**9**	**94**	**17**	**4**	**6**	**171**	**39**	**5**	**864**

1. táblázat ’Orderto Cash’, 6.számú portfólió összetétele
(Forrás: saját szerkesztés)

Egységes Azonosító (Unique ID): A rendszer által generált egyedi azonosító.	Üzleti tulajdonos (Business Owner): Az üzleti területnek a felelőse, aki jóváhagyási, döntési jogkörrel rendelkezik az alkalmazást illetően. Többnyire annak a területnek a vezetője, ahol az alkalmazás által támogatott üzleti folyamatok vannak.
Név (Name): Azonosítja az informatikai alkalmazást.	Üzleti tulajdonos delegáltja (Business Owner Delegate): Az a személy, aki ugyanazzal a jogkörrel rendelkezik, mint az üzleti tulajdonos. Jóváhagyási folyamatoknál fontos.
Rövidítés (Acronym): rövíditett informatikai alkalmazás név.	Üzleti egység (Business Unit Name): Annak a szervezeti egységnek a megnevezése, ahol használják az informatikia alkalmazást, illetve az üzleti folyamatok támogatottak valamilyen módon az alkalmazással.
Verzió szám (Version number): A nagyvállalati folyamatban, meghatározott előírás alapján az utolsó verzió, ami éles környezetben van.	Ország neve (Country): Azok az országok, ahol az alkalmazást használják, tehát van felhasználói interfésze.
Leírás (Description): Pár mondatban leírja az alkalmazás által támogatott üzleti folyamatokat.	Régió besorolás (Region): ahol az alkalmazást használják.
Státusz (Status): A nyilvántartásban több kategória van meghatározva. Tervezett (Planned), Fejlesztés alatt álló (Development), éles környezetben futó (Production/Deployed), kivezetés alatt lévő (decommissioning) kivezetett (Retired).	Fejlesztés támogatása (Development Team): melyik csapat végzi az alkalmazás fejlesztését.
Alkalmazás portfolió menedzser (Application portfolio manager): annak a személynek a neve, aki fele azért a portfólióért, amelyben az adott informatikai alkalmazás be van sorolva.	Harmadik fél neve (Vendor name): A kiszervezett cég neve, vagy a kapcsolattartó elérhetősége. Ennél az attribútúmnál nem belső fejlesztésű, vagy akár támogatású alkalmazásokról ad leíró információt.
Felhasználók száma (Number of users): Az adatbázis nyilvántartás alapján a felhasználónévvel és jelszóval rendelkező végfelhasználók száma, akik éles környezetben hozzáférnek az alkalmazáshoz.	Alkalmazás besorolása (Application status): Stratégiai, taktikai, “legacy”, tehát elavult.
Alkalmazás tulajdonos (Application Owner): Az alkalmazásnak a felelőse, vagy a delegáltja, aki döntéseket hoz az informatikai alkalmazások életútján keresztül. Legtöbb esetben az alkalmazáshoz kapcsólódó informatikai projekteken részt vesz.	Üzleti folyamat (Business Process): Fő kategória arra vonatkozóan, milyen üzleti folyamatot támogat az alkalmazás.

2. táblázat Informatikai alkalmazás attríbutum
(Forrás: Saját szerkesztés)

Üzleti funkció (Business Function): Üzleti funkcionális terület, amit támogat az alkalmazás.
Vállalati stratégiai támogatottsági szint (Enterprise Strategy Level): Az alkalmazásnak a besorolása az alapján, mennyire támogatja az üzleti célok elérését stratégiai szinten.
Üzleti kritikussági besorolás (Business Criticality): 1-5 ig terjedő skálán az üzlet határozza meg, mennyire kritikus az alkalmazás számára.

3. táblázat Alkalmazás kritikussági besorolás
Forrás: Saját szerkesztés

Alkalmazás ellenőrző tulajdonos (Application Control Owner): Az a személy, aki az alkalmazásokhoz tartozó törvényi előírásokat nyomon követi, informatikai auditokban részt vesz, a dokumentációkra vonatkozó előírásokat betartja.	Belső Audit (Internal Audit). Belső audit időpontja, részletei, audit riport.
Tárolt adatok besorolása (Stored data categorization): Itt a nagyvállalat által meghatározott adatbesorolási kategória szerepel. Például: személyes adatokat tárol.	Tervezett audit időpontja (Time of Planned Audit): Az előre kommunikált külső/belső audit időpontja.
SOX (Sarbanes Oxley) alkalmazás (SOX, Yes/No): SOX alkalmazásoknál itt az igen kerül kiválasztásra. Ez azt jelenti, hogy az alkalmazásnak követnie kell a SOX törvényi előírásokat.	Tervezett audit típusa (Type of planned audit): Külső vagy belső audit van az audit tervben szerepeltetve.
Külső Audit (External Auditor): Itt kerül részletezésre, ha az adott alkalmazást auditálta külső auditor	Dokumentumok listája (List of documents): BCP (Business Continuity Plan), Üzletmenetfolytonosági Terv, DRP (Disaster Recovery Plan), Katasztrófahelyreállítási Terv, Folyamatábra, Architektúrális ábra, változáskezelés dokumentációja, problémakezelés dokumentációja, SOD (Separation of Duties) mátrix-Szerepkör-Funkció mátrix, Folyamatleírás a manuális és automatikus kontrollra, Rekord visszaállítási terv, Alkalmazás minőségi riport, Audit logok, hozzáférési folyamat leírása.

4. táblázat Törvényi előírásoknak való megfelelési attríbutum
Forrás: Saját szerkesztés

Fejlesztési költségek (Development Costs): alkalmazás fejlesztésére fordított összköltség. Tartalmazza a fejlesztők bérköltségét, technikai, fejlesztői környezet kialakításának a költségeit is.
Támogatási költségek (Maintenance Costs): A mindennapi, operatív működéshez szükségek költségek sorolandók ide.
Szolgáltatási költségek (Service Delivery): szolgáltatás támogatási, hardver (pl.: CPU használat) költségek tartoznak ide.
Egyéb költségek (Other Costs): Minden olyan költség, ami nem sorolható az előző 3 kategóriába.

5. táblázat Alkalmazás költségei attríbutum
Forrás: Saját szerkesztés

A projektben informatikai alkalmazás tulajdonosok, informatikai alkalmazás támogatók, compliance szakértők, valamint üzleti folyamatgazdák vettek részt. A résztvevők munkaidejükben foglalkoztak a projektfeladatokkal. Az információk összegyűjtésére alkalmazásonként került sor. Az információk összegyűjtésében részt vettem. A mátrix létrehozása Excelben történt és készült javaslat arra, hogy ezek a leíró tulajdonságok, dokumentációk meglétére, állapotársa kerüljenek bele a központi informatikai alkalmazás nyilvántartó szoftverbe is. A továbbiakban a 6. táblázatban a létrehozott mátrixot szemléltetem. Színkódók értelmezése az alkalmazás portfólió-compliance mátrixban a következő.

A **piros szín** azt jelenti, hogy egyáltalán nem áll rendelkezésre az alkalmazáshoz tartozó előírt dokumentáció. A zölddel jelölt rekordoknál a dokumentáció megvan, elérhető és jóvá van hagyva a kijelölt felelősökkel. A **sárga szín** a dokumentáció meglétére utal. Azonban jóváhagyás nélkül nem érvényes, ezért ezeket külön kell jelölni. Az utolsó színkategóriába a **szürkével** jelölt rekordok tartoznak. A törvényi előírások nem minden informatikai alkalmazásra ugyanazok, ezért előfordul, hogy nem előírás valamelyik dokumentáció.

A mátrix elkészítésekor a közép- és felsővezetés támogatással fogadta a projektet. Javasoltuk, hogy az összes alkalmazás portfólióra elkészüljön a mátrix, így az auditokra könnyebb lesz a felkészülés. Nem kell majd időt tölteni a dokumentációk feülvizsgálatával az auditok előtt. A projekt során felmerült az a probléma, hogyan lehet naprakészen tartani a létrehozott mátrixot. Belső, vállalati hálóra való rendszeres feltöltés után, felelősöket kell rendelni a rekordokhoz. A mátrix egy jó alapot ad az informatikai auditok előkészítéséhez, így akár a sikerességhez. A szervezetben végzett kutatásom során kiderült az, hogy a nagyvállalat nem tudja megállapítani azt, milyen informatikai kockázatokat tartalmaz az alkalmazás, milyen a kockázati profilja az adott alkamazásnak.

A kockázatmenedzsment önálló szervezeti egységként működik a vállalatnál és nincs kommunikáció a compliance, illetve az alkalmazás portfólió menedzserrel. További kutatási kérdésként fogalmazodott meg bennem, milyen lehetséges módszertanok, eszközök használhatók arra, hogy az alkalmazás portfólióban az informatikai kockázatok listája is szerepeljen.

Az akciókutatás részeként mélyinterjút készítettem a szervezetben egy alkalmazás portfólió menedszerrel. Az interjúalany véleményét összegzem. Az alkalmazás portfólió menedzsment mindenkor egy fontos hajtóerőt képvisel az alkalmazást menedzselő csapatok számára saját fejlesztési tervük kiépítésében. Emellett bizonyos iránymutatást is ad, hogy vállalati szinten milyen irányelvek (technológiai, pénzügyi) mentén kell ezt a csapatoknak elvégezniük. A jelenlegi mérési rendszerek főleg pénzügyi jellegűek. Az IT elkerülhetetlen eleme minden vállalat létezésének. Minden hosszútávú alkalmazás fejlesztési tervének végső célja az üzemeltetési költségek csökkentése így érthető, hogy a mérőszámok adják a mérési rendszer gerincét. Emellett természetesen készülnek mérések, melyek a portfólióban lévő alkalmazások különböző tulajdonságait vizsgálja, mint például a felhasználók száma, az újonnan létrehozott alkalmazások száma, a lekapcsolt alkalmazások száma, vagy a szolgáltatási szintek. Ezek mind segítenek pontosabb képet kapni, hogy az alkalmazások a rájuk fordított erőforrások tükrében milyen szintű szolgáltatást, értéket nyújtanak a felhasználói oldalnak. Mint minden fejlesztés úgy a portfólió menedzselés sikere is néhány alapvető tényezőn nyugszik: Megfelelő pénzügyi erőforrások és IT technológiáknak rendelkezésre kell állni, hogy vállalati szinten a technológiák homogének tudjanak maradni. A jelenlegi állapotokat helyesen és alaposan felmérve realisztikus, szakmailag megalapozott célokat kell kitűzni. Elengedhetetlen, hogy az IT és az üzleti oldal teljes összhangban legyen azt illetően, hogy a kitűzött célok mind a vállalat, mind pedig a felhasználói réteg céljait is szolgálja. Az interjúalany véleménye az, hogy fejlesztendő terület a portfólió menedzser szerepkört közelíteni az üzleti tulajdonos szerephez. Tehát, az üzleti területet jobban megismertetni az alkalmazás portfólió menedzsment tevékenységekkel. Az akciókutatásban sok tudást és tapasztalatot gyűjtöttem az informatikai szabályzatokról, előírásokról, illetve informatikai auditok követelményrendszeréről. A nagyvállalati sajátossága volt, hogy sok időt vett igénybe az erőforrások allokálása, illetve az információk összegyűjtése.

Alkalmazás neve	Azonosító	Üzleti kritikusság	BCP (Business Continuity Plan)	Adatvédelmi előírás	Architektúrális ábra	Változás kezelés	Probléma kezelés	SOD (Separation of Duties)	Audit logok elérhetősége	Folyamatábra manuális, automatikus kontrollokkal	DRP (Disaster Recovery Plan)	RRP (Record Retention Plan), (Adatvisszaállítási terv)	Érzékeny programok	DOU/SLA	Folyamatleírás a manuális és automatikus kontrollokra	Adatmigrációs tervek	Tesztelési jegyzőkönyvek	Oktatási anyag
Dolgozói nyilvántartás	R51-1973680	3	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Hiányzik	Nem szükséges	Rendben	Rendben	Hiányzik	Hiányzik	Jóváhagyásra vár	Hiányzik
Környezeti incidens riportálás	TORL-KL6712	5	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Hiányzik	Hiányzik	Rendben	Rendben	Hiányzik	Hiányzik	Hiányzik	Hiányzik
Szabályzatok	JGO-981746	4	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Rendben	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Jóváhagyásra vár	Nem szükséges	Hiányzik
Utazási költségtérítés	CWH-2519389	3	Rendben	Hiányzik	Rendben	Hiányzik	Hiányzik	Rendben	Hiányzik	Rendben	Hiányzik	Hiányzik	Rendben	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik
Liszensz nyilvántartás	ORZ-1401987	4	Rendben	Rendben	Hiányzik	Lejárt	Lejárt	Rendben	Rendben	Rendben	Hiányzik	Nem szükséges	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik
Szakértői ellenőrzés	RDL-0297402	4	Rendben	Hiányzik	Rendben	Lejárt	Rendben	Rendben	Rendben	Rendben	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik	Hiányzik
UK vakáció tervező	SSE-036087	5	Rendben	Rendben	Lejárt	Rendben	Rendben	Hiányzik	Rendben	Rendben	Hiányzik	Nem szükséges	Rendben	em szüksége	Hiányzik	Hiányzik	Hiányzik	Hiányzik
Riportálás	CAL-0618418	1	Rendben	Rendben	Lejárt	Rendben	Rendben	Rendben	Rendben	Rendben	Hiányzik	Hiányzik	Rendben	em szüksége	Hiányzik	Jóváhagyásra vár	Jóváhagyásra vár	Hiányzik
Üzletkötői támogatás	MHT-L196439	3	Rendben	Rendben	Lejárt	Rendben	Rendben	Hiányzik	Rendben	Rendben	Rendben	Rendben	Rendben	em szüksége	Nem szükséges	Nem szükséges	Hiányzik	Rendben

6. táblázat Informatikai application-compliance mátrix
Forrás: Esettanulmány alapján saját szerkesztés

Az akciókutatás után megállapítottam, hogy hasznos az, ha az informatikai alkalmazásokról portfólió készül és azon belül pedig analitikus részletezés a dokumentációkra. Az informatikai auditok nemcsak a dokumentációk vizsgálatára terjedhet ki, hanem a folyamatok elemzésére és kockázati tényezők feltárására. A dokumentációk pontossága és naprakészen tartása mellett, az alkalmazásokra költött költségek és informatikai kockázati lista megléte a portfóliókban további kutatási kérdéseket vetett fel. Mivel a nagyvállalatnál volt kezdeményezés az informatikai kockázati analitikára és a portfólió képzés része volt a költséganalitika, kíváncsi voltam, hogy más nagyszervezetek milyen megoldásokat használnak.

1.4 Összefoglalás

Az első fejezetben az alkalmazás portfólió menedzsment fogalmi keretét, a portfólió képzés lépéseit, alkalmazásával nyerhető előnyöket fejtettem ki. Áttekintettem az alkalmazás portfólió képzésre lévő szakirodalmi ajánlásokat. Amennyiben az alkalmazás portfólió menedzsment beépült a vállalati informatikai stratégiába, akkor a nyilvántartás miatt az informatikai alkalmazásoknak a száma, minősége, illetve a költség, amit a fejlesztésére, támogatására fordítanak, mérhetővé válik. Azoknál a globális nagyvállalatoknál, ahol alkalmaznak alkalmazás portfólió menedzsmentet, az jellemző, hogy az alkalmazás térképet használva objektív és elérhető célokat tudnak kitűzni az alkalmazások életútjára vonatkozóan. Az informatikai alkalmazás portfólió menedzsment meglétével mérhetővé válik az informatikai szoftverek fejlesztési-, és karbantartási költségei is. Akciókutatásomban bemutattam, hogyan épül fel egy alkalmazás nyilvántartó rendszer. A projekt eredményeképpen az alkalmazás portfólióba beépítettük a törvényi előírások által meghatározott alkalmazás dokumentáció követelmények aktuális helyzetét. A létrehozott mátrix egy jó elemzési lehetőséget ad az informatikai auditok előkészítéséhez, akár az auditok során feltárt hiányosságok csökkentéséhez.

2. SZAKÉRTŐI INTERJÚK, PROBLÉMAFELVETÉS

Ebben a fejezetben a kutatási kérdések megfogalmazása utána, a szakértői interjúk értékelését fogom részletezni. Kitérek a nagyvállalati körben használt ajánlásokra, előírásokra, szabványokra és kapcsolatrendszerre az informatikai alkalmazás portfólió menedzsmenttel. Az interjúk kivonatát a függelékben szerepeltetem. A táblázatokban dőlt betűvel vannak a nyers interjú szövegek. Nem módosítottam az interjúalanyok véleményén, így előfordulhatnak az idézetekben fogalmazásból eredő pontatlanságok.

Az informatika területén elismert szakemberekkel készítettem mélyinterjút. A szakértőknek a szakmai háttere, tapasztalata és képesítése igazolja azt, hogy ért a kutatási témámhoz. Az interjúalanyok kiválasztásánál figyelembe vettem, hogy főleg nagyvállalati körben legyen munkatapasztalatuk, tehát nem kis- és középvállalati körben vagy állami szektorban. Az interjúalanyok legalább 15 év szakmai tapasztalattal rendelkeznek. Az első célcsoportba multinacionális vállalatoknál az informatikai területen dolgozó szakértő személyek. Nemzetközileg elismert képesítéssel rendelkeznek. A másik csoportba olyan interjúalanyok kerültek, akik szintén rendelkeznek az informatikai szolgáltatástámogatáshoz tartozó nemzetközi képesítésekkel. Ezek a személyek legalább 4 nagyvállalatnál szereztek tapasztalatot az informatika területén. Különböző pozícióban dolgoztak az informatika területén. A csoportképzésem azért fontos, mert így több, eltérő szempontrendszert összevetve tudtam elemzést végezni. Mélyinterjút 7 személlyel készítettem el 2017. december és 2018. január között. Az interjú készítés során elértem a Grounded Theory alapján a telítettséget. Ez azt jelenti, hogy további interjúalanyok megkérdezése, nem járt volna a kutatási kérdésem igazolásához több információval. A továbbiakban röviden ismertetem az interjúalanyok szakmai hátterét.

Az első interjúalany képesített informatikai ellenőr, (Certified Information System Auditor, CISA). Jelenleg több, mint 2000 főt foglalkoztató szervezetben az informatikai osztálynak az egyik vezetője. Szakmai múltját tekintve közel 15 éves tapasztalata van az IT területen. IT auditért, valamint csalásfelderítésért felelős szervezeti egységet vezetett. IT auditorként 2 évet dolgozott. Jelenleg a mindennapi munkájának része az informatikai

szabályzatok és folyamatok menedzsmentje, törvényi megfelelőségének biztosítása, fejlesztési igények, illetve az ezekhez szükséges erőforrások kezelése, IT tesztelési, kiadáskezelési és változási folyamatok felügyelete. Az interjút 2017. december 13.-án készítettem. A második interjúalanynak ITIL v3 képesítése van és képesített informatikai menedzser (Certified Information System Management, CISM). 25 éves tapasztalata van az informatika területén. Különböző állami és nem állami szervezetekben vett részt informatikai szolgáltatástámogatás fejlesztésében. Az interjút 2017. december 21-én készítettem. A harmadik interjúalanynak ITIL v2 és v3 képesítése van, 15 éve dolgozik informatikai területén. Az interjú készítésekor szolgáltatásmenedzsment vezető egy olyan szervezetben, ahol az alkalmazottak létszáma 3000 fő. Részt vett a szervezetben, a szolgáltatásmenedzsment kialakításán ITIL alapján. Az interjút 2017.december 28.-án készítettem. A negyedik interjúalanynak 22 éves tapasztalata van az informatika területén. 16 különböző képesítéssel rendelkezik: MCSA (Microsoft Certified Solutions Associate), MCPS (Microsoft Certified Professional Certification), MCTS (Microsoft Certified Technology Specialist). 16 különböző informatikai projektben dolgozott külföldön is. Solutions Architektként, tehát megoldás tervezőként pedig 10 éves tapasztalattal rendelkezik. Jelenleg egy 7000 fős vállalatnak, amelyik 16 országban van jelen, az informatikai osztályának az egyik vezetője. Az interjút 2018.január 4.-én készítettem. Az ötödik interjúalany, Klotz Tamás volt, aki jelenleg az SAP Hungary Kft. Kormányzati üzletfejlesztésen dolgozik. Tamás hozzájárult ahhoz, hogy a nevét szerepeltessem az értekezésemben. Szakmai múltját tekintve, a Számítástechnikai kutatóintézetnél dolgozott 3 évet, majd az IQSYS Informatikai és Tanácsadó Zrt.-nél, mint projektmenedzser. Az Oracle Hungary Kft.-nél pedig, mint üzletfejlesztési menedzser, marketingigazgató. A Magyar Posta Zrt.-nél informatikai igazgató volt. A HOUG (Magyarországi Oracle felhasználók) egyesületének az elnökhelyettese volt 8 évig, jelenleg a Neumann János Számítástechnikai Társaság (NJSZT) tagja. Az interjút Tamással 2018.január 10-én készítettem. A hatodik interjúalany, Kerékfy Pál, aki szintén hozzájárult, hogy a nevét szerepeltessem. Az MTA SZTAKI vezetője volt 1986-1991 között, utána konzultánsként dolgozott, majd 1997-től 2014-ig a Deloitte CIO-ja volt. Jelenleg több különböző helyen is oktat. A budapesti Metropolitan Egyetemen ITIL-t oktat. 6 éve pedig a Vezető Informatikus Országos Szövetségének a tagja. Az interjút 2018.január 10-én készítettem. A hetedik interjúalany 15 éves tapasztalattal rendelkezik az informatikai területén. Képesítései: CISM, ITIL expert, ISO27001 vezető auditor. Több globális nagyvállalatnál dolgozott informatikai biztonsági területen. Egy biztonsági

keretrendszert dolgozott ki informatikai alkalmazások menedzselésére vonatkozóan az egyik multinacionális vállalat informatikai osztályán. Az interjút 2018. január 20-án készítettem. Az interjúkérdések összeállításánál figyelembe vettem azt, hogy általánosan kérdezzek, az elméleti tudásom iránytűként szolgált. Az interjúk készítésével párhuzamosan megtörtént az iratok elkészítése és elemzése. Az interjúalanyok kiválasztása meglévő kapcsolati tőkémen keresztül történt. Az interjúk készítéséhez előkészítettem egy kérdőív vázlatot. Az interjúk félig strukturáltak voltak, néhány kérdés mentén haladtak az interjúk. Az interjúk alatt megfogalmazódtak új kérdések is. A mélyinterjúk időtartama átlagosan 1.5 óra volt. Az interjúk készítésével párhuzamosan az elméleti kategóriákat is meghatároztam a GT módszertan alapján. Voltak feltételezéseim, ami alapján kérdeztem, de további elméleti kategóriákat is képeztem. A mélyinterjúk készítése hasznos volt és külön élménnyel töltött el a vállalati körben dolgozókkal, szakértőkkel eszmecserét folytatni. A kutatás eszköze a saját telefonom és egy diktafon volt. Az interjúkészítésnél és elemzésnél az objektivitásra törekedtem.

2.1 Manuális kódolás eredményei

A GT módszertan lényege a kódolás. A kódolás a rögzített mélyinterjúk alapján történhet meg. Az első lépés a mélyinterjúk kivonata készítése után az adatelemzés. Az adatgyűjtés alatt a mélyinterjúk készítését és rögzítését értjük. Az elemzés alatt, pedig az interjúban használt kifejezések értelmezése történik meg. Az adatelemzés után fogalmakat (concept), majd a fogalmakból kategóriákat kell képezni, az utolsó lépés az elméletalkotás. A nyers adatok konceptualizálása folyamatosan történik meg. A hasonló fogalmakat kell egy kategóriába képezni. Az elméleti mintavétel (theoretical sampling) azon alapszik, honnan és hogyan gyűjtsön adatokat a kutató. Az adatok elemzésével párhuzamosan új kérdések, új fogalmak, kategóriák képződnek. Az elméleti telítettség (theoretical saturation) akkor következik be, amikor a kutató meggyőződik arról, hogy a kategóriák telítettek, nem tud újabb csoportokat képezni.

Nyitott kódolás (open coding) esetén az adatokhoz valamilyen koncepciót rendelek. A kifejezések között azonosságokat, hasonlóságokat, illetve eltéréseket keresek, majd ez alapján építem fel a koncepcióját. Ezt sokszor pár interjú elvégzése után megtettem, mivel az előzményekből leszűrhetttem, hogy mire kell később fókuszálni a következő kérdezés alkalmával. Az axiális (axial coding) szakaszban kategóriákat határoztam meg a

koncepció mentén és az egyes fogalom és kategóriák rendezése után kapcsolatokat teremtettem. A szelektív (selective coding) szakaszban meghatároztam, kiemeltem a kategóriákat azzal, hogy összefűztem az axiális szakaszban létrehozott kategóriákat. A kódolás után következett az elmélet kialakítása, Itt a strauss-i modellt követtem, tehát a felhasznált szakirodalmi tudásanyag és az interjú memo alapján csoportokat alkottam. A kódolásra kétféle lehetőség van. Manuális és automatikus. A manuális, tehát a nyílt kódolás előnye az, hogy a kutató magyarázza a kódolás eredményét. Az adatokat osztályoztam, kategorizáltam. A nyílt kódolással az volt a célom, hogy a leggyakrabban használt kifejezések alapján kategóriákat hozzak létre.

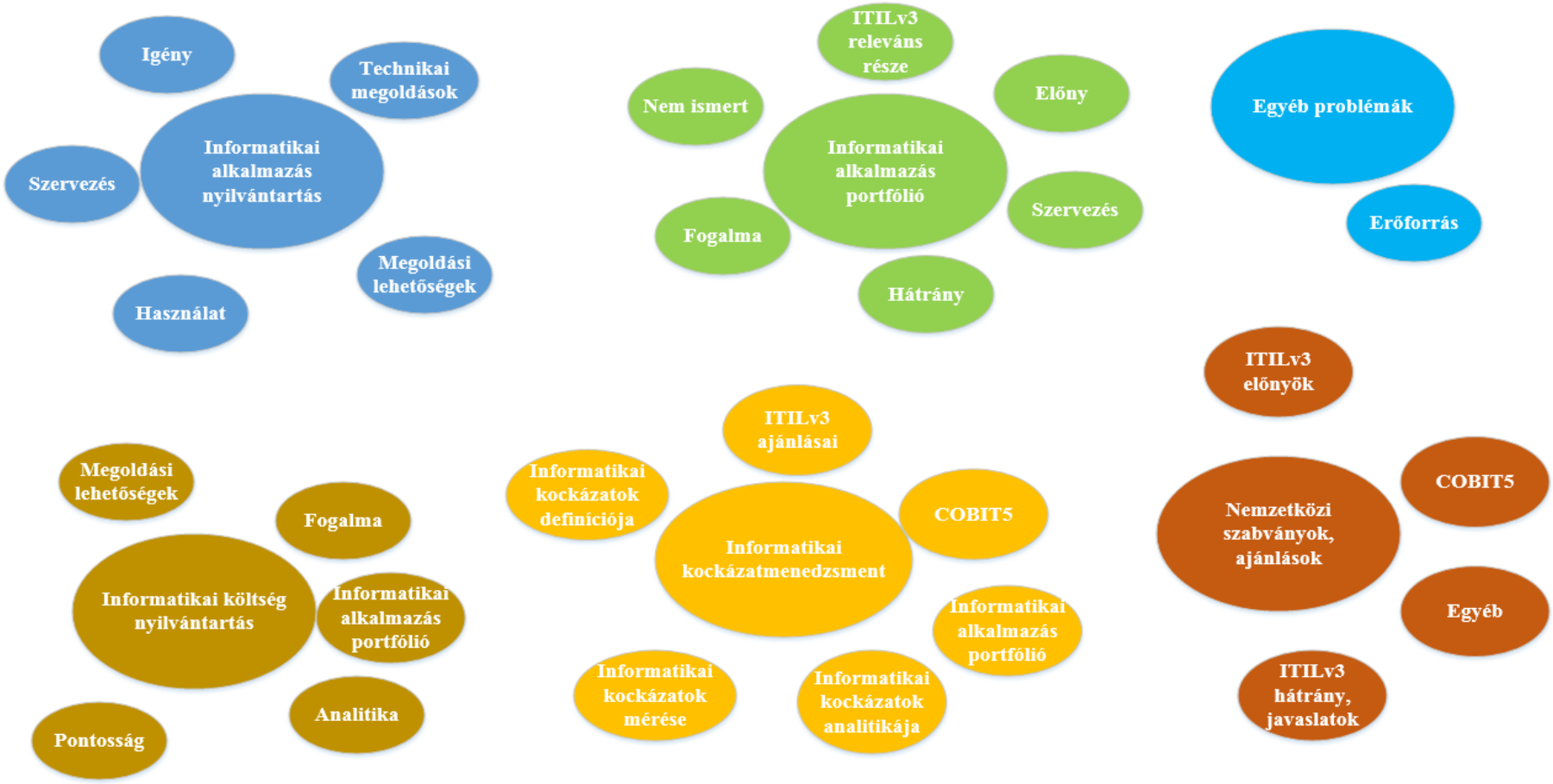
A tartalomelemzés lépései:

1. Adatok rögzítése, rendszerezése, szűrése.

2. Manuális, nyílt kódolás. Többszöri tartalom elolvasása után fogalomtérkép létrehozása, majd Excelben kódolás. A kódolás többszöri ellenőrzése.

3. Elemzés Excel segítségével.

Kétféle módszerrel lehet kódolni. Az első módszer alapja az, hogy a kutató már meglévő hipotézisekkel dolgozik, és a hipotézisekhez keres fogalmakat, elméletet. A másik módszer alapja az, hogy a kutató nem rendelkezik semmilyen feltételezéssel és a kódolás eredménye adja a kutatás gerincvonalát. Értekezésemben alapvetően már rendelkeztem feltételezésekkel, de a kódolás során új elméletek is körvonalazódtak. A 8. ábrán szemléltetem a fogalomtérképet, amit használtam a kódoláshoz. Az informatikai alkalmazás nyilvántartás, informatikai költség nyilvántartás, analitika, informatikai alkalmazás portfólió képzés, informatikai költség analitika és a fogalmakhoz rendelhető szabványok, ajánlások képezték a fogalmi keretét az interjúknak. Az informatikai alkalmazás nyilvántartásra vonatkozó kérdések arra vonatkoztak, hogy van-e bármilyen alkalmazás nyilvántartás a szervezetben. A 7. táblázatban az informatikai alkalmazás nyilvántartás elméleti kategóriának a kódolási egységei láthatóak. A szervezetekben van valamilyen nyilvántartás, vagy láttak különböző megoldásokat, de jól működő folyamatot nem. Két nagyvállalatnál is CMDB (Content Management Database System)-ben vannak nyilvántartva az informatikai alkalmazások.



8. ábra Fogalomtérkép az interjúk előkészítéséhez
Forrás:saját szerkesztés

A CMDB szoftver az alkalmazások listázására, a felvitt attribútumoknak a tárolására használják. Az egyik szervezetben informatikai folyamatot is tudnak az informatikai alkalmazások mögé rendelni, de üzleti folyamatot már nem. Ezáltal komplex, leképezhető interfész, architektúrális ábra nem nyerhető ki a rendszerből. A CMDB logikai struktúrájának kialakítása nem függ össze az ITIL ajánlásaival. Ha az elavult alkalmazás listára kíváncsi egy szervezet, akkor annak meghatározása a központi nyilvántartás nélkül nehezen megoldható. A CMDB-ből nem nyerhető ki információ az üzleti területekre. Az elavult rendszereket a nagyvállalatok figyelemmel kísérik, de a kivezetésük, cseréjük költségigényes. A listázása az elavult alkalmazásoknak külön van kezelve a többi alkalmazásoktól. Az egyik nagyvállalatnál a költségcsökkentési kezdeményezések vezettek oda, hogy készítettek egy központi nyilvántartást. A nyilvántartás után áttértem a portfólió képzés kérdéseire. A legtöbb cég látja a problémakört, hogy túl sok alkalmazás van és túl sok rendszert kell menedzselni. A következő szintig is eljutnak, hogy konszolidálni kell ezeket az alkalmazásokat. A konszolidáláshoz azonban nyilvántartást kellene készíteni az alkalmazásokról, funkciókról. Az igény a konszolidálásra sokszor az auditok után is felmerült. Az auditok alatt előkerültek olyan kérdések, amik az üzleti folyamatokra és informatikai alkalmazásokra irányultak. Az informatikai alkalmazásokhoz tartozó dokumentumkezelés nem megoldott. Összeségében megállapítom, hogy a nagyvállalatoknál van alkalmazás nyilvántartás, de nagyon hiányos és nincsenek üzleti és informatikai folyamatok az alkalmazásokhoz rendelve. Portfólió képzésről két szakember hallott, de jól működő megoldást nem. A nyilvántartás készítése is nehézségekbe ütközik.

A következő elméleti kategória, amit a 8. táblázat mutat a használt keretrendszerekre, ajánlásokra, szabványokra vonatkozik. Az ITIL v3-ban lévő utalás az alkalmazás portfólióra minden interjúalanynak ismeretlen volt. Azt feltételeztem, hogy nemzetközi ajánlás, szabvány alapján képeznek nyilvántartást a szervezetek, de ezt nem igazolták az interjúválaszok. A kérdések a nemzetközi ajánlások, szabványok használatára vonatkoznak. A legtöbb nagyvállalatnak különböző ajánlásokat és sztenderdeket kell párhuzamosan figyelembe venni, ez erőforrás igényes. Egyik ajánlás, szabvány sem alkalmazható teljes körűen és nehezen kezelhetőek, érthetőek. A kutatási témámhoz nem tartozik a szabványok, ajánlások összehasonlítása, vagy akár az összevonási lehetőségeknek a feltárása, de úgy gondolom jövőbeni kutatásokhoz jó alapot adhat ez az elméleti kategória.

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„A másik és már kapcsolódik az alkalmazás nyilvántartáshoz, egyáltalán a nyilvántartásoknak az a fajta filozófiája, hogy ne csak egy katalógusom legyen a polcon, egy statikus leltár. … annyi leltárat láttam már, hogy azt el nem tudom mondani… egyetlen szervezeten belül .."	statikus leltár	kezelhetetlen	Igény	**Nincs központosított informatikai alkalmazás portfólió, de igény van rá**
„Így bontjuk le az üzleti szolgáltatásokat, mögöttük futó IT szolgáltatásokra, alkalmazásokra, hardver elemekre, infrastruktúra elemekre és az összes köztük lévő kapcsolatrendszerre, amitől kialakul egy üzleti szolgáltatás mögött futó IT szolgáltatás pókháló."	átláthatatlan IT szolgáltatások	kezelhetetlen	Igény	
„Na, most ezeknek a rendszereknek a nyilvántartását kétféleképpen csináltuk. Nem volt olyan szerencsénk, hogy ezt a cég maga nyilvántartotta. Hát, hogy miben? Egy Excel táblában.."	Excel nyilvántartás	nehezen karbantartható	Igény	
„És igazából nem volt semmilyen nyilvántartásunk arról, hogy hol milyen rendszerek vannak, hanem igazából csak folyamatosan dolgoztuk fel Szerverről szerverre haladtunk, hogy azon milyen komponensek vannak, milyen szolgáltatások tartozhatnak, milyen termékek tartozhatnak.."	Ad-hoc megoldások	sok meghatározás	Igény	
„Igen, igény az van rá, és általában ez ott szokott elhalni, hogy a mátrixban megvannak a sorok, tehát megvannak a figyelt configuration item-ek , még akár .."	nincs megoldás	nem érthető	Igény	
„..sokszor nem is lehet tudni, meg nem is lehet egyértelműen dokumentáltan bizonyítani az auditoroknak, hogy itt most azon az alkalmazáson megy keresztül az üzleti folyamat és kontrollálható, ellenőrizhető módon megy keresztül az üzleti folyamat.."	sok folyamat, sok alkalmazás, átláthatatlan	átláthatatlan	Igény	
„Sok kezdeményezést már láttam, de jól működő rendszert nem--"	sok különböző kezdeményezés	kezdeményezés	Igény	
„Azért van még Excel táblánk eszközökről, mert bár meg tudnánk csinálni, hogy a CMDB-ben benne legyen és meg is van, de van, amiért nem tudjuk eldobatni velük a régi nyilvántartásukat, mert ott le van rajzolva pl. egy rack szekrénybe mi található, amit nem tudunk felvinni."	sok nyilvántartás, lehetne	különböző	Igény	

7. táblázat Interjú elemzés: Központosított alkalmazás nyilvántartás
Forrás: saját szerkesztés

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„Nem véletlen, hogy két szabványt használunk. Ha mind a kettő teljes lenne, akkor vagy az egyiket, vagy a másikat használnánk.”	két szabvány	két szabvány	sok ajánlás, szabvány	**Sok keretredszer, szabvány, ajánlás**
„Mi kettőt használunk, ergó nekünk meg van az igényünk az integráltra, mi úgy oldjuk meg, hogy fogunk így kettőt, azt így össze ragasztjuk, és máris van egy sokkal teljesebb körünk. Tehát nekünk megvan az igényünk.”	kettő használata	kezelhetetlen	sok ajánlás, szabvány	
„Alkalmazott szabványok hiányosak.”	hiányos	nem teljes körű	sok ajánlás, szabvány	
„Két oka van, ami miatt nem tudjuk használni. Az egyik az, hogy nincsen erőforrás, aki az ezzel kapcsolatos dokumentációt el tudná végezni....de korábban dolgoztam már olyan cégeknél, ahol akkor kezdtünk el ezzel igazából foglalkozni , és utána szerezték meg az ISO 31.000-res minősítést is, miután valami nagyon nagy baj volt...”	nincs rá erőforrás	sok meghatározás	sok ajánlás, szabvány	
"ami szerintem fontos, hogy ha az ITIL nem teljes körűen, vagy közel sem teljes körűen alkalmazott a nagyvállalatoknál, akkor a COBIT még annyira sem.."	nem teljes körű	nem érthető	sok ajánlás, szabvány	

8. táblázat Interjú elemzés: Sok keretrendszer,ajánlás
Forrás: saját szerkesztés

A következő elméleti kategória az előzőből alakult ki. A keretrendszerek, ajánlások közül az ITIL-t választottam ki. Az ITIL-t az informatikai üzemeltetésen használják, ahol az informatikai alkalmazás támogatók, üzemeltetők, adatbázisszakértők dolgoznak. Az informatikai szolgáltatásmenedzsmentre a legtöbb nagyvállalat már használja az ITIL-t. Az interjúalanyok nagyon részletesen kifejtették véleményüket az ITIL-ről. A következő elméleti kategóriák, az ITIL előnyeiről és hátrányairól a kutatásom alatt körvonalazódott. A kódolási eredményeket a 9-11. táblázat szemlélteti. Mivel túl bonyolult egy szervezetnek teljes körűen bevezetni, ezért csak egy-két részt alkalmaznak az ITIL ajánlásból. A folyamatok definiálása felelősökkel nagy előny. Nehezen érthető a nyelvezete, sok benne a definició és teljes körű bevezetésére még egy nagyvállalat sem lenne képes. Az ITIL implementálásánal felmerülő problémák hasonlóak a nagyvállalatoknál. Fontos lenne az informatikai szolgáltatások dokumentálása, folyamatgazdákkal, felelősökkel, de a menedzsment támogatás nincs meg ehhez. Az ITIL implementálásába ütköző nehézségek miatt, inkább a saját megoldásukat választják a szervezetek az informatikai folyamatok figyelemmel kísérésére. Azokban a szervezetekben, ahol nincsenek dokumentálva az informatikai folyamatok, az ITIL szemlélete, ajánlása beépíthető a működésbe. Az erőforrásigényessége miatt nem implementálják teljes körűen a nagyvállalatok. Az előnyét az incidenskezelésnél látját.

Két új elméleti kategóriát képeztem a kódolás során. Az egyik a folyamatok, a másik a menedzsment támogatásról alkotott véleményeket összegzi. Összefüggésben van a szervezetekben az, hogy az ajánlásokat mennyire tudják kiterjeszteni azzal, hogy milyen a felső vezetés támogatottsága és mi a prioritás a szervezetben. A menedzsment támogatottság hiánya, illetve a folyamatok komplexitása. Ezek a problémák minden nagyvállalatnál jelen vannak. Nem szerepeltetem a kódolási táblázatot, mert nem tartozik a kutatási kérdéseimhez a menedzsment és a folyamatok összetettségének a vizsgálata. Van összefüggés az eddig kialakított elméleti kategóriákkal, de a hangsúlyt a továbbiakban a költséganalitikára és informatikai kockázatkezelésre helyezem.

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„Nincs bevezetve az ITIL, de használjuk, nem formálisan használjuk, tudjuk, hogy mi az ITIL meg elküldjük az IT-sokat ITIL tanfolyamra, bizonyos szintig használjuk."	formális használat, nincs bevezetve	bizonyos szintig használat	használat	**ITIL –ről vélemény**
„Amióta a V3 létezik, azt gondolom, hogy amellett, hogy jó ötletek vannak benne, amellett ez a stratégia kezelhetetlen.",	a stratégia kezelhetetlen	kezelhetetlen	használat	
„a v3 az túlságosan akadémikus… szofisztikált, olyan érzésem van, hogy azt akarták, hogy tényleg ne hagyjunk ki belőle semmit és minden le legyen fedve. Inkább azt mondanám, hogy túlságosan bő és kivennék belőle."	túlságosan akadémikus, túlságosan bő	nehezen érthető	használat	
„Az pedig nagyon szépen működött…… mindig valamilyen ITIL fogalommal kezdődött."	minden definiált	sok meghatározás	használat	
„..hogy egy nagyon jó segédmutató tudna lenni az ITIL. Időnként túlságosan bonyolult volt ahhoz képest, vagy túl generalista volt ahhoz képest, amit az adott szervezet szeretett volna. "	túl bonyolult	nem érthető	használat	

9. táblázat Interjú elemzés: ITIL általános vélemények
Forrás: saját szerkesztés

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„Összességében helyzettől függően vannak hasznosítható részei."	hasznosítható részek	alkalmazható részek	Előny	**ITIL alkalmazásával keletkezett előnyök**
„ITIL a kezdetektől nagyon jól és nagyon erősen hangsúlyozott, az pont az a szemléletváltás, hogy az informatikai szolgáltatások nem önmagukban valók."	szemléletváltás a szolgáltatásokban	szemléletváltás	Előny	
„ITILben nagyon erős fejlődés, hogy vannak olyan technológiák, vannak olyan rendszerek, amelyek tényleg képesek úgy ezt a dinamikus mondjuk CMDB-t megvalósítani, ami már épp ésszel követhető kapcsolatokat mutatnak. "	követi a technológiai fejlődést	fejlődés	Előny	
„Olyan szolgáltatás irányítási területeket fed le és ír elő, ami nagyon kézzelfogható, tipikusan a service desk, az incidens, a probléma menedzsment, vagy magasabb szinten a continuity menedzsment, availability, mert nagyon jól megfogható tevékenységek vannak, amit csinálni kell."	tevékenységeket konkretizál	kézzelfogható részek	Előny	
„ITIL-t úgy kezeltük itt a szervezetben, hogy ez egy jó támpontot ad, avagy egy jó lehetőség arra, hogy megismerjünk legjobb gyakorlatokat."	jó lehetőség	támpont	Előny	
„.azokat a folyamatokat használtuk belőle, ami nekünk a mindennapokban olyan segítséget nyújt, vagy akkora hatékonyságjavítás látható mögötte, amitől mi azt reméljük, hogy az egész IT szervezet jobban és hatékonyabban fog dolgozni."	mindennapi munkához kell	segítség	Előny	
„Én dolgoztam az Európai Bizottságnak, ami viszont akkora egy hatalmas szervezet, hogy egy normálisan vezetett ITIL nélkül egyszerűen működésképtelen lett volna. Az pedig nagyon szépen működött."	átláthatóbb a szervezet	működést támogat	Előny	

10. táblázat Interjú elemzés:ITIL alkalmazásával keletkezett előnyök
Forrás: saját szerkesztés

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„..hogy miért nem vezetjük be holnap, azért mert egy komoly befektetés lenne..	formális használat, nincs bevezetve	erőforrásigény	Hátrány	**ITIL alkalmazása során észlelt hiányosságok**
„Amióta a V3 létezik, azt gondolom, hogy amellett, hogy jó ötletek vannak benne, amellett ez a stratégia kezelhetetlen, szerintem."	a stratégia kezelhetetlen	kezelhetetlen	Hátrány	
„ITIL keretrendszerre érzem problémának, hanem inkább az interpretálásában, hogy az ITIL megfogalmaz egy csomó olyan követelményt, folyamatot, aminek van menedzsere, végrehajtási rendje stb.… hogy sokszor azaz ember képe, hogy ha ezt mind megcsinálom, akkor csináltam egy 200 fős szolgáltató szervezetet és ott „még ember nem dolgozik".	nehezen implementálható	erőforrásigény	Hátrány	
„A másik, hogy azt látjuk, hogy azok a folyamatok működnek jól, amelyiknek dedikált folyamatgazdát tudunk biztosítani, azt mutatta a gyakorlat, hogy minden olyan folyamat, ahol nem így volt előbb utóbb elkezdett sorvadni és nem tudtunk olyan fókuszt tenni rá, hogy a létjogosultságát így betenni egy ember figyelmébe, egy dedikált folyamat gazdához."	minden definiált	sok meghatározás	Hátrány	
."…. 2008-ban a költségeken kellett vágni és az összes folyamatot, amiben nem volt meg a meggyőződés, hogy haszna van azt gyakorlatilag a cég lefejezte és az ITIL itt egy óriási sérülést szenvedett ez látszik a konferenciáik minőségén is."	túl bonyolult	nem érthető	Hátrány	
„És azon a mérlegen vannak megmérve, hogy akkor ez mennyit fog hozni a konyhára, és ezek mellé betolni egy ITIL szerinti folyamat átalakítást… good luck, győzd meg a menedzsmentet."	nem támogatott	erőforrásigény	Hátrány	
„..én ezt úgy érzem, hogy az ITIL még azt tükrözi, amikor van egy felhasználója egy szoftvernek és a felhasználó használja a szoftvert és úgy állít elő üzleti értéket. És most ugye kezd ez a mesterséges robotok meg mindenféle dolgok, kezd eljutni odáig, hogy nincs a végén a felhasználó, aki használja, amivel most foglalkozni kéne az ITIL fejlesztése során, hogy nincs ott a felhasználó a végén a dolognak, hanem már magától működik."	nem követi az automatizálást	Fejlesztésre szorul	Hátrány	

11. táblázat Interjú elemzés: ITIL alkalmazásával észlelt hiányosságok
Forrás: saját szerkesztés

Az alkalmazás szintű költséganalitika készítéséhez nem veszik figyelembe az ITIL ajánlásat. Az analitikához szükséges a megfelelő stratégia, szakmai tudás, erőforrás, jó modell és egy támogató szoftver. A költségelemek megvannak és elszámolásra kerülnek a pénzügyi folyamatokon keresztül Excelekben, vagy pénzügyi szoftverekben. Tőkekiadásokra és beruházási kiadásokra osztják fel a költségeket. Nem elemzik részletesen a fejlesztési, vagy akár a támogatási költségeget alkalmazásonként. Az összerendelés nem történik meg az informatikai alkalmazásokkal. Az igénynek a részletesebb kimutatáshoz a menedzsment részéről kellene megfogalmazódnia. Persze az operatív szinten dolgozók is készíthetnének javaslatokat, bemutatva az előnyöket. Van olyan szervezet, amelyik már projektet indított a nyilvántartás létrehozására, persze a kezdeti nehézségek már körvonalazódnak a projekt indításakor. A továbbiakban arra kerestem a választ, mennyire alkalmazható, használható az ITIL-nek a pénzügyi nyilvántartásra vonatkozó fejezete. Mivel az informatikai szolgáltatások dokumentáltságát, az üzemeltetés folyamatának az egyszerűsítését szolgálja az ITIL ajánlás, ezért az informatikai szolgáltatásokhoz tartozó költséganalitika is fontos. Az elemzés eredményét a 12. és a 13. táblázat mutatja. A legtöbb vállalatnál lenne igény az alkalmazás portfólióra és benne lévő költséganalitikára. A 14. táblázatban az informatikai kockázatkezelésre vonatkozó kódolási egységeket lehet látni. Az interjúk alatt kiderült, hogy az informatikai kockázatokra nincs elkülönítve szervezeti egység, szakértőkkel. Az IT incidenskezelésben jelenik meg valamennyire az informatikai kockázatok kezelése. Ahol van kockázat elemzés, ott a működési kockázatokat mérik, elemzik. Üzleti, technológiai, szervezeti kockázatokról nincs részletes lista. Az üzletileg kritikus alkalmazásokat figyelemmel kísérik, de ez kevés. A különböző keretrendszerek, ajánlások értelmezése sok erőforrást köt le. Szóban, elméleti úton vázoltam az interjúalanyoknak az informatikai kockázati analitika beépítésének a lehetőségét az alkalmazás portfólióba. Tény, hogy erőforrás igényes a kialakítása és menedzsment támogatás szükséges hozzá, de az összegzett vélemény az, hogy megállná a helyét a nagyvállalati környezetben.

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„…a költségeket mi az SAP-ben és Excelekben tartjuk számon.	több nyilvántartás	széttagolt	fejlesztés	**Informatikai költséganalitika nem kellően kidolgozott**
„Ezzel kapcsolatban beszélgetünk az anyavállalat kapcsolattartójával, hogy érdemes lenne elgondolkodni, hogy gyakorlatilag ezekhez az információkhoz hozzákapcsolni a pénzügyi információkat, nagyon sok dimenziót be tudnánk hozni, ahol költségeket tudnánk megjeleníteni..."	igény az analitikára	széttagolt	fejlesztés	
„.. hogy vannak e rejtett költségek, akkor abban az a megközelítés sokkal többet segíthetne, hogy ha valaki analitikusan végig gondolná, hogy milyen elemekből áll az én IT szolgáltatás környezetemnek a költség összetétele. Van OPEX és CAPEX, hát már ott problémák vannak, hogy melyik elem micsoda."	tudáshiány a költségelemekre	tudáshiány	fejlesztés	
„…de tegyük fel, hogy van egy jól működő kapacitás menedzsment egy cégnél és még azt is meg tudjuk nézni, hogy melyik alkalmazás, milyen időszakban, mennyit fogyaszt az egyébként közös használatú vasakból. Ennek a költségallokációnak sok dimenziója van, és hogy mi mentén osztjuk az egy dolog, a használati része egy másik dolog. Ha nincs ilyen kapacitás menedzsment mérésünk, akkor más módszerrel kell megállapítani, hogy hogy lehet leosztani ezeket a költségeket…	van megoldás, több dimenziós	nem alkalmazás szinten	fejlesztés	
„Az informatikai költségeket nem CMDB-ben hanem Excelben tartjuk nyilván. Van egy költségallokációs modellünk és minden évben készül egy hozzárendelés…"	Több nyilvántartás	széttagolt	fejlesztés	
„Például régen az egy évvel ezelőtt a cég, ahol dolgozom, teljesen más módszer alapján sorolta be azt, hogy mi az, ami az operációs költség, mint például ebbe az évben. Holott a rendszerek nem változtak, a rájuk költött pénz nem változott csak annak a besorolása, kategorizálása	fogalomzavar	tudáshiány	fejlesztés	
„És most nekünk van egy olyan projektünk, hogy megpróbáljuk az összes informatikai költséget egy rendszer alá tenni."	futó projekt	igény	fejlesztés	
„Nagyon sok helyen azt csinálják, hogy egyszerűen azokat az alapszoftvereket, sokszor alap hardware-ket, amiket vettek ez a rendszer, ennek a rendszernek a működtetéséhez arra a rendszerre teszik rá pénzügyileg és aktiválják rá a fejlesztési költségeket is. Innentől kezdve szakmailag is hibás, nem csak pénzügyi szakmailag, hanem informatikai szakmailag is hibás.."	helytelen költségallokáció	tudáshiány	fejlesztés	
„Annyit csinálnak, hogy vagy beruházás, vagy OPEX vagy CAPEX szinten fogják és megbontják.	helytelen költségallokáció	tudáshiány	fejlesztés	
„hanem két helyen is láttam azt, hogy a pénzügyön két profi kontrollinges összeállt egy nagyon jó IT-sal, akinek volt pénzügyi vénája és összeraktak egy olyan Excelbe valamiket. Aminek az a baja, hogy egyszer összerakják és maximum 2 frissítés után szétesett az egész. Ha lehet automatizálni ezeknek, a például egy CMDB és egy műszaki eszközök gazdasági nyilvántartását, ha jól össze vannak kötve, akkor ott az átmenet teljes mértékben automatikus tud lenni. De ez csak egy aspektus..."	Fogalomzavar	széttagolt	fejlesztés	

12. táblázat Interjú elemzés: Informatikai költséganalitika kidolgozottsága
Forrás:saját szerkesztés

Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„Ha van egy szituáció és az ITIL-t be akarnánk vezetni, mint standard, és jelenleg a CMDB-nkben hiányoznak bizonyos dolgok, mint a cost is, mögé egy business case-t kell tolni, ez az önmagában frankó dolog lenne, de marha drága."	bonyolult a kivitelezés	széttagolt	nehézkes	**Informatikai költséganalitika és ITIL nehezen összeegyeztethető**
„..az ITIL ad támpontot, hogy mik azok a költségelemek, amikre figyelni kell, licenszingre, amortizáció, stb. Van ajánlás, de nem kielégítő és ez szerintem a legnehezebben megfogható téma."	nem elég részletes	széttagolt	nehézkes	
„..az ITIL pénzügyi menedzsment folyamata felé mozdulni, hogy abban a pillanatban, hogy ha ezt a kérdést arról az oldalról nézzük, hogy van e ennek létjogosultsága, az én véleményem hogy van. "	van létjogosultsága	igény	nehézkes	
„.Tehát igazából jött egy igény, megbecsültük, elfogadták, implementálták költségkereten kívül vagy belül és az ITIL módszerből semmit nem használtunk. Annyira nem, hogy ha itt egy szolgáltatást bevezettünk, az nem úgy került át a szolgáltatás portfólióra vagy a termék portfólióba, hogy ez ennek a projektnek az eredménye."	más megoldásokkal	nem alkalmazható	nehézkes	
„Az ITIL ezt nem tudja követni."	nem elég részletes	széttagolt	nehézkes	
„. Kicsit az volt az érzésem, hogy másfél év után eljutottunk volna oda, hogy már alkalmazás szinten is lehetett volna ezt csinálni, de akkor ott még az a szervezet az alacsony szinten tartott az ITIL-nek ezen implementálásában."	fogalomzavar	tudáshiány	nehézkes	
„Hát, ugye lehet használni csak pont az vele a probléma, mint amit az előbb mondtam, hogy az ITIL-nek a filozófiáját követni akarjuk, akkor a költségeket az értékkel össze kéne tudni hozni valahol."	költség-érték összerendelés	értéke	nehézkes	

13. táblázat Interjú elemzés: Informatikai költséganalitika és ITIL kapcsolata
Forrás:saját szerkesztés

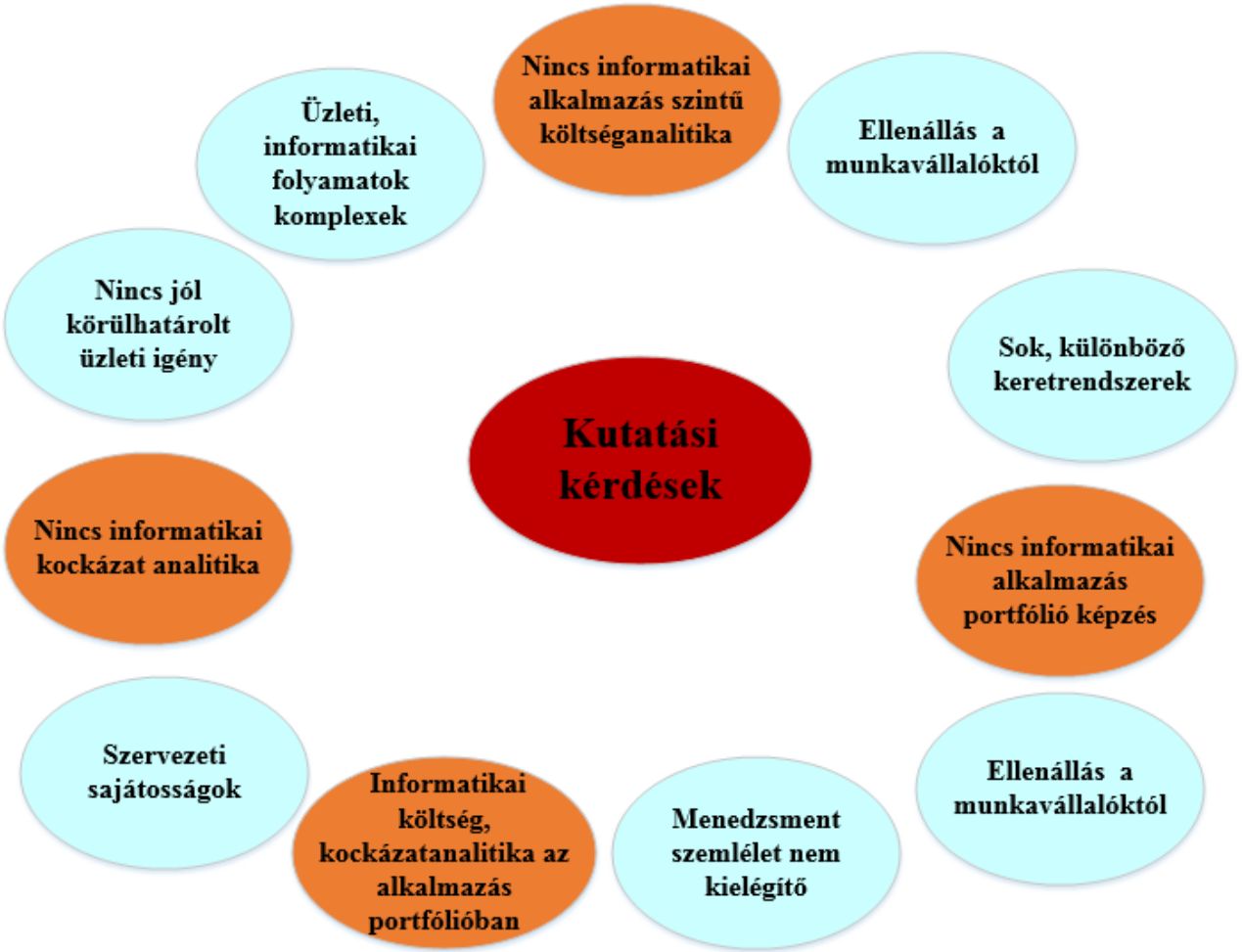
Iniciális, nyitott kód	Tematizált	Axiális	Szelektív	Elmélet
„Nálunk az IT kockázatkezelés formális process, két központja van: üzleti folyamatok és rendszerek. Az üzleti folyamatoknak felmérik a folytonossági kockázatát… Az informatikai alkalmazások milyen folyamatokat támogatnak, ott öröklik az RTO-t például és ebből származik a kockázat is, az availability kockázat az üzleti folyamatokból jön direktbe. Informatikai kockázatoknál."	bonyolult kapcsolatrendszer az üzleti folyamattal	átláthatatlan	Nyilvántartás hézagos	**Informatikai kockázatok nincsenek nyilvántartva, nem körvonalazódik pontosan az igény rá**
„Nagyon régóta tudjuk azt, hogy a kockázat menedzsment az egy feladat, mindamellett, hogy ez egy külön szakma informatikától függetlenül.."	fontosság és igény felismerés	fontos	Nyilvántartás hézagos	
„Tehát nekünk megvan az igényünk. Amennyire emlékszem nem tehát amennyire az informatikai kockázatkezelésbe beleértjük az elemi szintű kockázatokat. Ez a szint ez nem jelenik meg sem egy COBIT-ban sem egy ITIL-ben.	vannak már közelítések	felismerés	Nyilvántartás hézagos	
„az incidensek hoznak működési kockázatokat, ezeknek vannak fórumai, van compliance commitee ahova beviszünk ilyet… Közvetve részt vesznek a folyamataink az IT kockázat menedzsmentben, de dedikáltan nem. CMDB-ben nincs kockázatra vonatkozólag nyilvántartás, azt tudjuk megnézni, hogy a rendszerek között mi az, ami üzletileg kritikus."	dedikált kockázat menedzsment nincs	közvetett kapcsolat	Nyilvántartás hézagos	
..hogy a kockázat kezeléssel foglalkozó osztályoknál külön van IT kockázat kezeléssel foglalkozó egy-két ember és ők tipikusan az alkalmazások működési kockázatának irányából közelítettek. A klasszikus IT szervezetek viszont az alap infrastruktúrák működési kockázataiból szoktak kiindulni és azt szokták elemezgetni.."	néhány szakember	szaktudás kevés	Nyilvántartás hézagos	

14. táblázat Interjú elemzés:Informatikai kockázatkezelésre helyzetkép
Forrás:saját szerkesztés

2.2 Kutatási kérdések körvonalazása

A kéziratok soronkénti elemzése után, nyitott kódolási technikát alkalmazva meghatároztam a fogalmakat és csoportokba képeztem. Eltérő vélemények, nem fordultak elő, így azokra újabb kategóriát nem kellett képeznem. Többször végeztem kódolást, mire eljutottam az elméleti eredményekhez. Meglévő problémák feltárására, illetve megoldási, fejlesztési lehetőségekre irányul az eredményem bemutatása. Az iniciálás után a tematizált kódolást végeztem el. Az iniciális kódoknál a nyers szöveget vettem alapul, nem a kéziratot, kivonatot. Az interjúk olvasása közben többször is értelmeztem a szövegeket. Az iniciális kódolásnál szakkifejezésekre is fókuszáltam, mint pl.: ITIL, költség, probléma, ajánlás, szabvány. A nyitott kódolásnál figyelembe vettem a kérdésköröket, kérdéseket, ami elhangzott az interjú alatt. A tematikus kódok létrehozásánál figyeltem arra, hogy ne legyenek átfedések a tematikus kódok között. Az axiális kódolásnál figyelembe vettem a nyílt és a tematikus kódokat, valamint a közöttük lévő kapcsolatrendszert. A szelektív kódolásnál már figyeltem arra is, hogy a kategóriák kiemelésével párhuzamosan rávilágítsak az elméletre. Olyan elméletet is alkottak a kategóriák, melyek nem voltak a feltételezéseim között. Az eredmények érdekes képet alkotnak. A kódolások alapján létrejöttek olyan elméletek, melyek mögött nem volt semmilyen feltételezésem. Ezek az elméleti eredmények lehetőséget adnak egy további kutatás folytatására, elemzésére. Természetesen ezek az elméletek szorosan kapcsolódnak a többi elmélethez, amik mögött valamilyen előzmény van.

Az első feltárt probléma az, hogy az informatikai alkalmazásokról a legtöbb nagyvállalatnál nincs nyilvántartás. Azoknál a szervezeteknél, ahol volt bármilyen nyilvántartás ott listázhatók, riportálhatók az alkalmazásoknak az attribútumai. Azonban az informatikai és üzleti folyamatok térképe, hálója már nincs fejlesztve a rendszerben. Az első kutatás kérdésköröm az informatikai alkalmazás portfólió nyilvántartás szükségességének a vizsgálatára irányult. Az első fejezetben egy esettanulmányon keresztül bemutattam, hogyan tud működni egy nagyvállalati környezetben a menedzselése az alkalmazásoknak. A kiinduló pont az volt, hogy láttam az akciókutatás során, milyen problémákba ütközik a szervezet, ha szeretne részletesebb információt az informatikai alkalmazásokról. A 9. ábra szemléltetem narancssárgával azokat a kérdésköröket, amivela továbbiakban foglalkozom.



9. ábra Feltárt problémák a mélyinterjú alapján
Forrás: saját szerkesztés

A kék színnel jelölt halmazokban a feltárt fogalmi kategóriák vannak. A második kérdéskör, ami kapcsolódik a feltételezéseimhez az informatikai költséganalitika a nagyvállalatoknál. A rendszerekhez tartozó költségek besorolása aggregáltan történik meg. Bonyolultnak találják a szervezetek szétszedni elemeire az egyes költségkategóriákat. Az informatikai projektek költségkeretei is sokszor túllépik a tervezetet és hatásvizsgálat nem készül utána. A legfontosabb a gyorsaság, ami nem jár együtt a pontos informatikai költséganalitikával. Informatikai alkalmazás szintre való lebontásra lenne igény, de erőforrás, vagy szaktudás hiánya miatt, ennek a megvalósítása elmarad.

A harmadik problémakör, az informatikai kockázatok kezelése. Az üzleti területek nem kezdeményezik a nyilvántartást, a hozzáadott értékét nem tudják egyelőre mérni. A sok ajánlás, szabvány mellett bármilyen szintű kockázat nyilvántartás Excelekben van. Egy-két szakértő foglalkozik operatív, vagy infrastruktúrához tartozó informatikai kockázatokkal. Az üzleti folyamatok komplexitása miatt az informatikai szolgáltatások menedzselése is széttagolt. Ez az egyik tényezője annak, hogy a kockázatokat nehezen tudják meghatározni.

2.3 Összefoglalás

A második fejezetben a kutatás lépéseit, elemzéseit és az eredményeket mutattam be. A nagyvállalatnál végzett interjúk eredményéből az derült ki, hogy sok különböző ajánlást, szabványt kell figyelembe venni az informatikai szolgáltatások területén, ami jelentős erőforrásokat köt le a szervezetben. Több nagyvállalat rendelkezik valamilyen alkalmazás nyilvántartásra alkalmas szoftverrel, de folyamatosan problémát jelent az alkalmazások nyilvántartására vonatkozó attributomok egységesítése, illetve az információk karbantartása. A legtöbb helyen a portfólió képzés fogalma nem ismert, így nem is alkalmazzák. Az ITIIL v3. nemzetközi ajánlás iránymutatást és jó alapnak tekintik az interjúalanyok, de a folyamatos szervezeti transzformációk, megkövetelne egy könnyen és gyorsan bevezethető alkalmazás portfólió képzésre vonatkozó irányelvet, ajánlást, összefoglaló gyűjteményt. Az informatikai alkalmazás költséganalitikának a nyilvántartására nincs megfelelően alkalmazható és használható modell, iránymutatás. Az informatikai szolgáltatások szintjén megjelenő költségek definiálása nem megoldott. Az informatikai szolgáltatások bonyolultsága és komplexitása miatt a szolgáltatásokhoz

nem rendelhető egyértelműen költség. A legtöbb nagyvállaltnál szervezeti szinten nincsen kialakítva IT controlling, így az informatikai pénzügyi analitika nem központosított. Az informatikai kockázatok alkalmazás szinten való kimutatása nem megoldott és az informatikai kockázatok kezelését külön szervezeti egységek végzik, elkülönülve az informatikai szolgáltatásmenedzsment területétől. Több szervezetnél az az informatikai kockázatok pontos definiálását és az elemi kockázatoknak az elemzését, monitorozását nem végzik el, de az interjúk véleménye alapján kiderült, hogy lenne rá igény. Az igénynek felsővezetői szinten kell megfogalmazódnia.

3. INFORMATIKAI KÖLTSÉGKEZELÉS AZ ALKALMAZÁS PORTFÓLIÓ MENEDZSMENTBEN

Az interjúvélemények és az elemzések körvonalazták az ITIL v3 használatával kapcsolatos tapasztalatokat. A fejezet első részében az ITIL v3 nemzetközi ajánlást vizsgálom meg, használatának előnyét és hátrányát összegezve. Az informatikai alkalmazás portfólió kezelésére és az informatikai költség analitikára vonatkozó részt mutatom be. A tudományos és iparági felmérések után a szakértői interjúk elemzéséből levont következtetéseket részletezem az alkalmazás portfólió menedzsment, informatikai költség és ITIL kapcsolatánál. A fejezet második részében az informatikai alkalmazás költséganalitikára vonatkozó problémákat elemzem egy esettanulmányon keresztül.

3.1 ITIL terminológia

Az interjúkból körvonalazódott egy probléma, miszerint az ITIL használatával párhuzamosan, nem tudják a nagyvállalatokban központosítani az informatikai alkalmazás nyilvántartást. A CMDB informatikai rendszer alkalmas katalógus készítésére és alkalmazás attribútumok nyilvántartására, de nem támogatja a portfólió képzést. Az ITIL lényegében egy keretrendszer az informatikai szolgáltatások minőségének a javítására, az üzemeltetés szabályozásán keresztül. Az informatikai szolgáltatásmenedzsment komponense [84]. Az ITIL-t a Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunication Agency, CCTA) fejlesztette az 1980-as években. Jól körülhatárolt nemzetközi ajánlás, oktatásokon, kurzusokon lehet elsajátítani az ajánlás tartalmát, tudásanyagát. Az ITIL használatával a szervezetek azonosíthatják az informatikai folyamataikat.

Az ITIL v3, melyet 2011-ben publikálták, az alábbi öt fejezetre tagolódik:

1. Szolgáltatásstratégia (Service Strategy)

A szolgáltatás stratégia fejezetben van részletezve, hogyan tud az informatika értéket teremteni az üzleti és az IT stratégia kapcsolódásán keresztül. Főbb

témakörei: gazdasági hatása a szolgáltatásnyújtásnak, pénzügyi menedzsment, kockázatok, valamint kritikus sikertényezők, szervezetfejlesztés [85].

2. Szolgáltatástervezés (Service Design)

A szolgáltatástervezés feladatai, vagyis a tervezéskoordinálás, szolgáltatáskatalógus, szolgáltatásszint, rendelkezése állás, kapacitás és IT-szolgáltatásfolytonosság, információbiztonság és szállítómenedzsment kerül kifejtésre [86].

3. Szolgáltatásátadás (Service Transition)

A változáskezelésre, szolgáltatáseszköz és konfiguráció menedzsmentre, átadás és telepítési menedzsmentre, átadás tervezésére és támogatására, értékelés és tudásmenedzsmentre vannak ajánlások [87].

4. Szolgáltatásüzemeltetés (Service Operation)

Esemény, incidens, probléma és hozzáférés menedzsment, valamint a kérésteljesítés funkciói vannak kifejtve. Új architektúrákat és modelleket ajánl a szolgáltatásüzemeltetés támogatására [88].

5. Folyamatos szolgáltatás fejlesztés (Continual Service Improvement)

Az utolsó fejezetben pedig a folyamatos, rendszeres szolgáltatásfejlesztés gyakorlatait részletezi. A tervezés- végrehajtás- ellenőrzés- beavatkozás (Plan Do Control Act, PDCA) ciklusra építi a visszacsatolási rendszer lényegét [89].

Az ITIL v4-et 2019. februárban publikálták. Az utolsó verzióban már az agilis fejlesztés, a digitális transzformáció is szerepel. Az ITIL aktuális a mostani informatikai környezetekben, főleg a globális nagyvállalatoknál. Az informatikai szolgáltatásoknak, rugalmasnak, dinamikusnak és gyorsan adaptálhatónak kell lennie. Az útmutatás kiterjed a folyamatokra, emberekre, tevékenységekre, technológiákra, kockázatokra. Az informatikai szolgáltatásokra építi az ajánlást. Informatikai szolgáltatásra néhány példa: telefonos ügyféltámogatás, hibaelhárítás, szoftver, hardver telepítések, nyomtatási lehetőségek, E-mail használat biztosítása, felhasználói adminisztráció. A Service Desk, vagy helpdesk feladata a felhasználók támogatása hibajegyek nyilvántartásán keresztül. A helpdesk tevékenység nyomon követhető, mérhető. Az ITIL második összetevője az

úgynevezett SLA. Tartalmazza a szolgáltatási szint biztosításának feltételeit, felelősökkel, határidőkkel. Az incidenskezelés része körvonalazza az informatikai szolgáltatások normál működési feltételeit. A problémakezelés során történik a felismert problémák, incidensek kezelése, illetve a monitorozás segítségével a lehetséges problémák megelőzése. A változáskezelésnek több oka lehet. Üzleti igények módosulása, rendszerfejlesztések, patchek telepítése, törvényi, vagy szervezeti változás. Természetesen a változáskezelési folyamatban is dedikált szerepkörök, felelősségek vannak, így biztosítható a változtatások ellenőrzése. Az utolsó összetevő a release (kiadás) kezelése, menedzselése. A tesztelésen jóváhagyott, hardver csomagok éles környezetbe való bevezetését támogatja. Az élesítés után fellépő hibák, üzemzavarok száma csökkenthető a release menedzsmenttel. Az informatikai szolgáltatásokkal szemben alapvető elvárás, hogy költséghatékony, értékteremtő, minőségi és mérhető legyen. Az IT szolgáltatáshoz szükséges adatok nyilvántartására a CMDB ajánlja. A továbbiakban az ITIL portfólió megközelítését figyelembe véve, az alkalmazás portfólióra tett ajánlásokat vizsgálom meg. A szolgáltatás portfólió nem ugyanaz, mint az alkalmazás portfólió. Több alkalmazás, illetve alkalmazás portfólióban lévő alkalmazás együtt is adhat egy szolgáltatást, a szolgáltatás portfólióban. Az ITIL előnye, hogy dokumentált keretrendszer, az informatikai szolgáltatásokat struktúrába helyezi, ajánlásokat ad az informatikai folyamatok dokumentálására.

2005-ben készült egy tudományos tanulmány az ITIL bevezetéséről. Nagyvállalati körökben az egyik legnagyobb és legfontosabb előnynek azt tartották a szervezetek, hogy sokkal transzparensebben, hatékonyabban tudtak működni, mivel a folyamatok megfelelően voltak dokumentálva. Ebben a tanulmányban az ITIL v2-es verzióhoz kapcsolódtak a tapasztalatok [90]. 2009-ben készült esettanulmányok összegzése alapján az ITIL alkalmazásával az infrastruktúra kiszámíthatóbb, a felelősségek és szerepek tisztázottabbak. Az incidensek naplózása a nyomon követhetőség miatt növelte az üzlet, vevők elégedettségét [91]. Egyéb tudományos kutatások eredménye alapján megállapítható, hogy az informatikai változtatásokon az ellenőrzés nagyobb, hatékonyabb. A szolgáltatás szintről való megállapodás dokumentálása, konzultáció az üzleti terület és informatika között is javult, illetve az incidensek adminisztrálása [92], [93]. 2011-ben készült empirikus kutatás eredményéből az derült ki, hogy az ITIL implementálási nehézségeivel párhuzamosan, nő a használatával elérhető előny. A szolgáltatás minőségének a javítása, egyszerűsített folyamatok, jobb kommunikáció az informatikai és üzleti szereplők között a legnagyobb előnyök közé sorolandók [94]. 2014-

ben készült egy tanulmány Finn, Svéd, Német és Dán vállalatokkal. Az ITIL bevezetésének a hatékonysága nagymértékben függ a szervezet rendelkezésre álló erőforrásaitól, a folyamatok dokumentáltságától, illetve attól is, hogy mennyire van a felső vezetés bevonva. Az ITIL bevezetésének a száma arányosan növekszik a vállalat méretével, tehát a nagyvállalatok szélesebb körben használják. A legtöbb vállalat nem teljes körűen adoptálta a folyamataiba a szolgáltatásmenedzsmentet és operatív szinten nagyobb arányban alkalmazzák az ajánlás egyes fejezetrészeit, mint stratégiai szinten [95], [96]. Az informatikai szolgáltatásmenedzsment szervezet (IT Service Management Forum, itSMF) 2013-ban 49 országban 738 válaszadóval készített egy felmérést. Az ITIL használatának a legnagyobb előnye az informatikai szolgáltatás minőségének és hatékonyságának növelése, valamint a költségeknek és a kockázatoknak a csökkentése. Az ITIL-ből a legtöbb vállalat az incidenskezelést, változtatáskezelést, kéréskezelést és problémamenedzsment folyamatokat tudta majdnem teljes egészében adaptálni a szervezet folyamataiba [97]. Iparági felmérések más aspektusokat is mutatnak. 2009-ben készített a GARTNER cég 156 vállalattal felmérést. Az eredmény azt mutatja, hogy az informatikai szolgáltatás minőségének a növelése, valamint az agilitás növelése miatt implementálják a szervezetek a folyamataikba az ITIL-t. A válaszadóknak 13%-a költségcsökkentés, 9%-a pedig kockázat csökkentése céljából vezette be [98]. 2018-ban az Equinor, norvég energia vállalat, Globális Üzleti Szolgáltató (Global Business Service, GBS) ágazatába implementálta az ITIL egyes részeit. 35%-os költségcsökkentést tudtak kimutatni, illetve hatékonyabb működést a vevők kiszolgálásában [99].

A vállalat méretétől, tevékenyégétől és rendelkezésre álló kapacitásától függ, hogy mennyire tudja alkalmazni az ajánlásokat. Összességében elmondható előnynek, hogy a folyamatok átláthatóbbá válnak, de az ajánlást teljes egészében alkalmazni, bevezetni kivitelezhetetlen. A nagyvállalatnak nincs annyi erőforrása, hogy minden egyes folyamatához folyamatgazdát jelöljön ki. Kapacitás, erőforrások hiányában a legtöbb nagyvállalat nem tudja az ajánlást teljes egészében alkalmazni. A kódolási egységekből az alábbi gondolatokat, idézeteket emeltem ki:

„Összességében helyzettől függően vannak hasznosítható részei”,

„ITIL a kezdetektől nagyon jól és nagyon erősen hangsúlyozott, az pont az a szemléletváltás, hogy az informatikai szolgáltatások nem önmagukban valók.”

„ITIL-t úgy kezeltük itt a szervezetben, hogy ez egy jó támpontot ad, avagy egy jó lehetőség arra, hogy megismerjünk legjobb gyakorlatokat.”

„..azokat a folyamatokat használtuk belőle, ami nekünk a mindennapokban olyan segítséget nyújt, vagy akkora hatékonyságjavítás látható mögötte, amitől mi azt reméljük, hogy az egész IT szervezet jobban és hatékonyabban fog dolgozni.”

„Én dolgoztam az Európai Bizottságnak, ami viszont akkora egy hatalmas szervezet, hogy egy normálisan vezetett ITIL nélkül egyszerűen működésképtelen lett volna. Az pedig nagyon szépen működött. Ha én oda bejelentkeztem, akkor azt egy incidensként azonosította. Ha kértem valamit, hogy állítsanak nekem át az máris egy request-ként jelent meg a rendszerben és nem működött, hogy valakitől azt személyesen kértem volna, hogy állítsa be, csak ezen a rendszeren keresztül és ezzel biztosítottuk azt, hogy folyamatosan adminisztrálva volt minden tevékenység, tehát auditálható volt. Arra nagyon jó volt, hogy a vezetőnek pontos rálátása volt arra, hogy mi történt, milyen állapotban van, mekkora a backlog-ja az informatikai szervezetnek.”

Az ITIL implementálásánál sok probléma léphet fel. A probléma mértéke függ a szervezet méretétől, illetve a szakértők számától. Problémák közé sorolandó az, hogy túl sok időt kell eltölteni a folyamatok, ábrák megértésével, folyamatfelelősök kijelölésével. A menedzsment támogatása is szükséges a megfelelő implementáláshoz. Nagy szervezetek esetében könnyebb az alkalmazása, mert rendelkezésre áll a szükséges költségkeret, azonban ez a kis és közepes vállalatokra, illetve az állami szektorra nem, vagy kevésbé igaz [100].

2017-ben készült itSMF tanulmány megállapítása, hogy az ITIL-nek a frissítésére, új területek kiegészítésére van szükség, mint például az Agile, Lean IT, felhőszolgáltatások. Egyre jobban nő a kereslet a szakemberek iránt ezen a területen [101]. Egy Ausztráliában készített tudományos vizsgálat 110 válaszadó alapján összegyűjtötte azokat a faktorokat, ami szükséges ahhoz, hogy az ITIL implementálása hatékony, gyors és sikeres legyen. Fontos a magas szintű és minőségű a kommunikáció a felső vezetésben, az oktatás megszervezése. Az üzleti folyamatok, ezáltal az informatikai folyamatok priorizálása, valamint az elemzés mellett a riportálási struktúra beépítése a vállalati környezetbe. Kritikus sikerfaktor még az, hogy az egész változásra mennyire nyitottak a munkavállalók. A különböző sikerességi tényezőket dokumentálni és mérni kell [102]. A Budapesti Corvinus Egyetem Informatikai Intézetének egyik kutatása azt

állapította meg, hogy az informatikai szolgáltatásmenedzsment projektek népszerűsége csökken. A felmérésben állami, külföldi és belföldi tulajdonú szervezetek vettek részt. Míg 2011-ben a szervezeteknek az 51%-a, addig 2016-ban már csak 28%-a tervez valamilyen fejlesztést az informatikai szolgáltatásmenedzsment területén. Az új technológiai irányok, mint például a felhő alapú szolgáltatástámogatás, illetve a mobil informatikai megoldások is sok időt és költséget követelnek a szervezetekben, így ezeknek az integrálása a napi munkába az elsődleges feladatok közé került. Az újonnan induló projektek, programok a digitális kommunikációt támogatják [103]. FORBES Insight, iparági 2017-es felmérése, melyet 261 szakértővel készítettek, azt mutatja, hogy a szervezeteknél az ITIL -t használják túlnyomó többségében az informatikai szolgáltatás menedzsmentre. Persze emellett még a COBIT és a Microsoft Operációs Keretrendszer (Microsoft Operations Framework, MOF) is népszerű [104]. Az arányokat a 10. ábra mutatja.

10. ábra Szervezetek aránya a szolgáltatásmenedzsment fejlesztésre
Forrás:[104]

A mélyinterjúk alatt felsorolt tényezőket foglalom össze, melyek az ITIL alkalmazásával járó fejlesztési lehetőségeket összegzi. A nagyvállalatok egyre kevesebb erőforrást biztosítanak arra, hogy az informatikai szolgáltatást javítsák. A hangsúlyt a költségcsökkentésre, technológiai újításokra, mobil vagy felhő alapú megoldásokra helyezik. Az interjúalanyok véleménye a témához kapcsolódoan:

„ITIL keretrendszerre érzem problémának, hanem inkább az interpretálásában, hogy az ITIL megfogalmaz egy csomó olyan követelményt, folyamatot, aminek van menedzsere, végrehajtási rendje stb… hogy sokszor, azaz ember képe, hogy ha ezt mind megcsinálom, akkor csináltam egy 200 fős szolgáltató szervezetet és ott „még ember nem dolgozik”.

„Az, hogy miért nem vezetjük be holnap, azért, mert egy komoly befektetés lenne.”

„A másik, hogy azt látjuk, hogy azok a folyamatok működnek jól, amelyiknek dedikált folyamatgazdát tudunk biztosítani, azt mutatta a gyakorlat, hogy minden olyan folyamat, ahol nem így volt előbb utóbb elkezdett sorvadni.”

Az informatikai szolgáltatásokhoz folyamatgazdát rendel az ajánlás. Tehát nem elég a folyamatoknak a feltérképezése, dokumentálása, hanem dedikált felelőst is hozzá kell rendelni. Az ITIL teljes körű alkalmazása drága, egyes fejezetei nehezen érthetőek, implementálhatóak a gyakorlatba. Az interjúk kódolásából az egyik elméleti fogalom az, hogy az ITIL nem eléggé részletesen fejti ki az alkalmazás portfólió nyilvántartásra vonatkozó ajánlást. Az ITIL ajánlást ad az alkalmazások nyilvántartásának a fontosságára az életútjuk alatt. Defíniálja, hogy mi az alkalmazás portfólió, valamint egy példát tartalmaz arra vonatkozóan, hogy mit kell tartalmaznia az alkalmazás portfóliónak. Azonban nem tér ki a portfólió képzés lépéseire, vagy akár kapcsolati rendszerére az informatikai szolgáltatásmenedzsment többi területével.

Az interjúk alatt elhangzottak alapján a katalógus menedzsment, ami az ITIL-ben szerepel, azt a CMDB nevű szoftver használatával próbálják megoldani. A CMDB bevezetése során defíniálják a szervezetek, mit értenek egyáltalán informatikai alkalmazás alatt. A CMDB már nemcsak alkalmazás nyilvántartásra alkalmas, hanem folyamatok nyilvántartására, illetve a folyamatok státuszkezelésére is. A CMDB a változáskezelési folyamattal is összevan kötve. A Konfigurációs Elem, (Configuration Item, CI), az egy attríbutum a CMDB-ben. A CMDB-t több nagyvállalat szeretné lecserélni, kivezetni.

A 15. táblázat ITIL v3-ban szerepel, a szolgáltatás tervezés, alkalmazás menedzsment részben. A szakmai jelentések mögötti egységes értelmezés pedig az egyik legfontosabb tényező a sikeres informatikai szolgáltatásmenedzsmentben. A táblázat egy jó alapnak tekinthető, de nem fedi le teljes körűen azt, mit is kellene tartalmazni az alkalmazás portfóliónak. A kategóriák nincsenek pontosan definiálva, körülírva. Konkrét

kérdés merül fel, hogy mit jelent pontosan a felhasználói interfész, vagy a product metric, lefordítva termék metrika [86].

Alkalmazás neve	Informatikai működés tulajdonos	Fejlesztési költség
Alkalmazás azonosító	Informatikai fejlesztés tulajdonos	Éves működési költség
Alkalmazás leírása	Támogatói kontaktok	Éves támogatási költség
Támogatott üzleti folyamat	Adatbázis technológia	Éves fejlesztési költség
Informatikai szolgáltatás támogatás	Függő alkalmazások	Kiszervezett komponensek
Felső támogató	Támogatott informatikai rendszer	Kiszervezett partnerek
Támogatott földrajzi egység	Felhasználói interfész	Termék metrikák
Kritikus üzlet	IT Architektúra hálózati topológiával	OLA link
SLA link	Használt alkalmazás technológia	Támogatott metrikák
Üzleti tulajdonos	Felhasználók száma	

15. táblázat Alkalmazás portfólió az ITIL ajánlása szerint
Forrás: [86]

A nagyvállalatok egy része elkülönülten dolgozza ki az alkalmazás portfólió képzés lépéseit. A vállalatok egy része az alkalmazás portfólióra vonatkozó adataikat a CMDB ben tárolják. A harmadik kategóriába esnek azok a nagyvállalatok, melyek kombinálják az alkalmazás portfóliót és a szolgáltatás portfóliót. Természetesen van kapcsolat az alkalmazás portfólió és a szolgáltatás támogatás között, hiszen az összes alkalmazásokhoz kapcsolódó információkat, mint például a támogatott szolgáltatásokat, valamint az üzemeltetéshez kapcsolódó információkat összesítve kell nyilvántartani.

Az interjúalanyok meglátása a témát illetően:

„ITIL-ben leginkább IT folyamatok vannak összegyűjtve, amennyire én tudom…… Sok olyan része van az ITIL ajánlásnak, amely nincs benne a CMDB alkalmazás nyilvántartó részében.”

„Egy kiindulási alap és jó ötlet kell, de hogy pl. a user interfaces alatt mit értenek így, hogy ez nincs tovább kifejtve, az ember szinte arra gondol amire akar.”

„..alkalmazások karbantartásánál, vagy szerver nyilvántartásánál nagyon sok olyan szempont van, amit az ITIL felsorol, hogy ezekre figyelj, de hogy hogyan azt nem mondja meg.”

A résztvevők, felelősök meghatározása fontos. Az ITIL informatikai szolgáltatás megközelítésű, ezért használja és részletezi a ’service portfolio’-t, vagyis a szolgáltatás

portfóliót. Az architektúrális tervezésekben segítséget adhat az ITIL [105]. Vannak olyan nagyvállalatok, ahol az ITIL mellett külön szervezeti egységek személyek, felelősök vannak, arra, hogy az alkalmazás életútjához tartozó folyamatokat koordinálják, felügyeljék. Az alkalmazás portfólió nem ugyanaz, mint a szervíz portfólió. Az alkalmazás portfólió képzés és menedzsment elkülönül a szolgáltatás portfóliótól. Megállapítom, hogy a szervezeteknek van alkalmazás nyilvántartása, de a szolgáltatás portfólió részeként. Az alkalmazás portfólió képzésről kevés információval rendelkeznek, de az interjúk alatt kiderült, hogy hasznos lenne, ha a szervezetbe különböző szempontrendszerek alapján lenne kategorizálva az informatikai alkalmazás.

3.2 Informatikai költség

Az informatikai költségeket két kategóriába lehet sorolni. Az egyik az úgynevezett Tőkekiadások, **CAPEX** (Capital Expensive) a másik az Operációs költségek **OPEX** (Operating Expense). A tudományos kutatások alapján nem jelenthető ki konkrétan, hogy az informatikai beruházási költségek pozítiv hatással vannak a vállalat termelékenységére, bevétel növekedésére. Egyes tanulmányok szerint nincs kapcsolat az informatikai tőkekiadások és az eladott termékek növekedése között a szolgáltatás szektorban [106], [107], [108], [109]. A 2000-es évek után készültek olyan tanulmányok, amelyek azt igazolják, hogy pozítiv a kapcsolat a tőkekiadások és a termelékenység között [110], [111]. A CapEx, tehát a vállalati tőkekiadással kapcsolatos döntések hatással vannak a vállalat pénzügyi teljesítményére, így a piaci értékére [112]. Egy 2014-ben készült tanulmány a CAPEX és OPEX hatását vizsgálta az informatikai minőségre. Alapvetően nem jelenthető ki, hogy pozítiv hatással van a kiadás növekedés az adatok integritására [113].

A másik megközelítés az informatikai költségek csoportosítására az ún.: tulajdonosa a költségnek (Total Cost of Ownership, **TCO**). A modell koncepcióját 1994-ben körvonalazták. A modell azon alapszik, hogy meg kell érteni egy adott költségnek a tulajdonosát. A keretrendszer lényege, hogy a külső beszállítótól vásárolt terméknek, vagy szolgáltatásnak az értékének az allokációjából kiindulva lássa a szervezet analitikusan a költségelemeket. Teljesítménymérést, döntéseket támogatva a folyamatos fejlesztés mellett költségmegtakarítási lépések tervezésére is alkalmas. Részletes adatokra alapozva történhet meg a beszállítókkal a tárgyalás. Az implementálása hosszú

és időigényes folyamat, sok szakértelmet igényel [114], [115], [116]. Használata az informatikai szolgáltatások területén is elterjedt. Az informatikai szolgáltatások kiszervezése megköveteli a költségek TCO koncepció alapján való költség elemzését. Az informatikai szolgáltatás nyújtója lehet külső cég, beszállító. Informatikai rendszerek tervezését, fejlesztését, élesítését, üzemeltetését, vagy akár informatikai projektek vezetését végezhetik. Elég széles körű a kiszervezett tevékenység lista az informatikai területén. Az informatikai költségek összetevője a TCO modell alapján: hardver, informatikai alkalmazás költségek, adminisztratív támogatási költségek, rejtett költségek és a nem adminisztrált költségek. Az utolsó kategóriába a képzési költségek, megnövekedett fejlesztési igények, rendszertervezési költségek tartoznak. A Gartner Group által fejlesztett TCO modell lényege, hogy minden direkt és nem direkt informatikai költséget nyilvántart a szervezet és hozzárendeli informatikai eszközhöz. Az informatikai költségelemek az alábbiak: kliens, szerver, hardver költségek, fejlesztési, hálózati, támogatási költségek [117]. Egy másik megközelítés alapján öt kategóriába sorolja: bevezetési, működési, támogatási, fejlesztési, kiterjesztési és kivezetési.

A következő költségelszámolási megközelítés az informatikai költségek összetevőinek a vizsgálatára az úgynevezett: **ABC**, vagyis Activity Based Cost, Tevékenység alapú költségelszámolási ajánlás. Az ABC alkalmazásával kimutatható a szevezet teljesítményének és az informatikai területeknek a kapcsolatrendszere [118], [119]. A szolgáltatási szektorban jól alkalmazható és hozzájárul a vállalati teljesítmény növeléséhez [120], [121]. Az ABC méri a tevékenységeknek a költségét és teljesítményét. Az erőforrások tevékenységekhez vannak rendelve, majd a tevékenységek költségobjektumok alá vannak sorolva [122].

Egy gyártóvállalatnál végzett informatikai költségek elemzés eredménye az volt, hogy a vállalat költségeinek 82%-a működésre, 12%-ot pedig tőkekiadásokra költ. Olyan iparágban volt jelen, ahol a versenytársak 33%-ot költöttek befektetésekre, így a vállalat versenyhátrányban volt. Az informatikai vezetés nem fordított figyelmet arra, hogy az informatikai költségeik nagyobb része olyan informatikai alkalmazásokra költötte, amelyek nem gyakoroltak nagy hatást az üzleti tevékenységre, így bevétel, üzleti profit generálásra sem [123]. A Forrester cég 2011-ben készült felmérése azt mutatja, hogy a nagyvállalatok az informatikai költségeik 65%-át költik a mindennapi működés támogatására, valamint informatikai fejlesztésekre [124]. A Computer Economics IT spending and staffing Benchmarks, 2017 májusában készült 202 US és Kanadai vállalattal

felmérése azt mutatja, hogy az informatikai költségeken belül jelentősen megnövekedett a biztonságra, felhő alapú alkalmazásokra, infrastruktúrára fordított költségeknek az aránya [125]. A KPMG CIO felmérése, 4498 CIO szervezettel, 80 különböző országban készült 2016 december és 2017 április között. A felmérésben a negyedik helyen szerepel, vagyis a válaszadók 54%-nak prioritás a költségmegtakarítás. A felhő alapú megoldások, technológiai újítások, folyamatok optimalizálása, üzleti intelligencia (Business Intelligence, BI) egyre jobban előtérbe kerül. Ehhez pedig a folyamatos magas szintű informatikai szolgáltatás biztosításához szükséges. Az informatikai költségeknek a részletesebb, analitikusabb nyilvántartására, kimutatására alkalmazás szinten szükség van [126].

Az alkalmazásokhoz tartozó költségeknek kétféle megközelítése van. Az egyik alapján az informatikai projekt összköltségéből vetítődik le a költség. A másik megközelítés alapja a költség-elosztás. A személyi jellegű költségek, tőkeköltségek, dokumentációs költségek, fejlesztési, támogatási és egyéb kategóriájú költségek tartoznak ide. A továbbiakban a második megközelítést fogom használni. A fejlesztési (development) költségekbe tartoznak azok a komponensek, ami egy új alkalmazás fejlesztéséhez tartoznak, vagy meglévő funkció bővítéséhez. Dokumentált követelményspecifikáció alapján a programkódban, vagy akár dokumentációban történt fejlesztési költségek. A fejlesztések dokumentálása is költséggel jár. A specifikációk írása, javítása, levelezés, riportok, kimutatások készítése. A személyi jellegű kiadásokba a fejlesztők és egyéb technikai szakemberek bérköltsége sorolható. A támogatás (maintenance) költségekbe a napi működés fenntartásához szükséges költségelemek tartoznak [127]. A nagyvállalati körben ’support’ költségként emlegetik a támogatási költségeket.

Az idézetek és a kódolási eredmény megerősíti a feltételezést, hogy az informatikai alkalmazás szintű költséganalitikára szükség van.

„Például a költségeket mi az SAP-ben és excelekben tartjuk számon. Releváns információk lehetnek, ha egy helyen vannak ezek az információk és könnyedén lekérdezhetünk adott alkalmazásokról mindent egyszerre, anélkül, hogy több helyről csipkednénk össze az infókat, mint pl. a cost.”

„*El tudok képzelni olyan érettségi szintet, ahol a pénzügyi döntéseknél ez egy szempont lehet.”*

„többet segíthetne, hogy ha valaki analitikusan végig gondolná, hogy milyen elemekből áll az én IT szolgáltatás környezetemnek a költség összetétele. Van OPEX, CAPEX, hát már ott problémák vannak, hogy melyik elem micsoda. A szervezetek nem tudják önmagukról, hogy mit mennyiért csinálnak és ebben egyébként az ITIL ad támpontot, hogy mik azok a költségelemek, amikre figyelni kell, liszenszekre, amortizáció, stb. Van ajánlás, de nem kielégítő és ez szerintem a legnehezebben megfogható téma, mint a facility menedzsment…"

„megpróbálok eltávolodni a gyakorlattól és az ITIL pénzügyi menedzsment folyamata felé mozdulni, hogy abban a pillanatban, hogy ha ezt a kérdést arról az oldalról nézzük, hogy van-e ennek létjogosultsága, az én véleményem hogy van.."

„Tehát, aki látta a javasolt összes szolgáltatást, összes ilyen pénzügyi információ gyűjtése és kezelése, ez nincsen meg. Egyáltalán nincsen meg."

„Tehát igazából jött egy igény, megbecsültük, elfogadták, implementálták költségkereten kívül vagy belül és az ITIL módszerből semmit nem használtunk. Annyira nem, hogy ha itt egy szolgáltatást bevezettünk, az nem úgy került át a szolgáltatás portfólióra vagy a termék portfólióba, hogy ez ennek a projektnek az eredménye, hanem hogyha volt egy projekt, ami például bevezet egy SAP-t, nálunk nem SAP van, tehát bevezetünk egy olyat."

A portfólió képzésnél, az alkalmazások besorolásánál az informatikai alkalmazások költségviselőjének a meghatározása az első lépés. Azt kell meghatározni, hogy melyik üzleti terület fizeti az alkalmazáshoz költségeket. Ez nagyvállalati körben, ahol ugyanaz az informatikai alkalmazás több üzleti területet is támogat nehéz a költségviselőknek a hozzárendelése a költségekhez. A résztvevők meghatározása a döntési folyamatban, valamint a megfelelő adminisztrálása és nyomon követése a döntésnek elengedhetetlen. A pénzügyi menedzsment része az ITIL v3-ajánlásnak jó alapot ad a nagyvállalatoknak. A folyamataik komplexitása révén bonyolult költség elszámolási szabályokkal, rendszerekkel rendelkeznek.

Az **ITIL, Financial Management**, tehát a pénzügyi menedzsment rész a szolgáltatás stratégia fejezetben található. ABC (Accounting, Budgeting, Charging), vagyis számvitel, költségtervezés és költségterhelés, számlázásra építi az informatikai szolgáltatás elszámolását. A szolgáltatásértékelés, igény modellezés, portfólió kezelés, optimális szolgáltatás nyújtás, bizalom tervezés, költség-haszon elemzés, költségvetés,

számvitel, pénzügyi törvényi megfelelést, valamint fix és változó költségmodellt tartalmaz az ajánlás. Az informatikai szolgáltatásokra fordított költségek folyamatos monitorozása és értelmezésére tesz ajánlást. Az ITIL megközelítése az, hogy adott szolgáltatáshoz kell rendelni a költséget. Az informatikai szolgáltatások priorizálásával, valamint a hozzájuk rendelt költségekkel transzparens képet kapnak az informatikára költött költségekről a vezetők. Költség-haszon elemzéssel pedig láthatóvá válik egy összetett, bonyolult informatikai architektúrában az egyes informatikai szolgáltatások értéke. A szolgáltatásban pedig egy, vagy több szerver, alkalmazáscsoport, támogató emberi erőforrások költsége szerepel. A nagyvállalatoknak van igénye arra, hogy nem csak szolgáltatás alapú megközelítés, hanem alkalmazás szintű költséganalitika is legyen. Ez jelenleg a legtöbb vállalatnál nincs megvalósítva. A fenti lista mellett, ezzel párhuzamosan az ITIL v3-ban a pénzügyi információk kezelése az informatikai szolgáltatások terén nem kiforrott [128]. Részlegesen vezetik be az ITIL fejezeteit és a költségmenedzsment fejezetrész használata nem jellemző. Ezzel szemben a szakértők tudják, hogy fontos lenne nyilvántartani alkalmazás szinten az informatikai költségeket. Egy új szerver vásárlása, vagy interfész kiépítésénél adott informatikai alkalmazáshoz már részletesebb analitikára lenne szükség. Ad-hoc jelleggel készítenek elemzéseket. A következő alfejezetben egy akciókutatás során keletkezett projekt eredményeit vázolom fel. Az akciókutatás egy jó példa arra, hogy a költségnyilvántartás elemzése milyen problémákba ütközik, illetve az analitikus nyilvántartással milyen előnyöket generálhat egy szervezet.

3.3 Akciókutatás

Akciókutatásom során arra kerestem a választ, hogy az alkalmazás portfólió menedzsment részeként hogyan történik a szervezetben az alkalmazásokhoz tartozó informatikai költséganalitika. A költségelszámoláshoz nem vettek figyelembe nemzetközi ajánlást. A költséganalitikába beleértem a költségek eredetét, nyilvántartási módját, frissítését, ellenőrzését, monitorozását, értékelését. Az akciókutatásban a szakmai tudásomat és tapasztalataimat felhasználva vettem részt. Az előzmények, kiindulási helyzet leírása után a célokat, kihívásokat részleteztem, végül az alkalmazás költség analitika portfolió kialakításának a menetét, a tervezéstől az elkészítéséig vázoltam. A felmerült problémákat, jövőbeni fejlesztési lehetőségeket összegeztem a vállalati

tapasztalatok alapján. Az akciókutatás során az észrevételeimet folyamatosan rögzítettem. A rögzített tanulságok alapján készültem fel arra, hogy mit fogok jobban megvizsgálni. Az adatokat, amit felhasználtam az eredmény prezentálásához, folyamatosan gyűjtöttem össze. A kutatás időtartama 6 hónap volt. A projekt, amiben részt vettem a nagyvállalatnak az egyik informatikai alkalmazás portfólió költségcsökkentéséhez kapcsolódott. Az APM a globális nagyvállalatnál, már több évtizede jelen van az informatikai architektúra menedzsment részeként. Az alkalmazás portfólió menedzser hatáskörébe tartozik a költségek nyomon követése az informatikai alkalmazások szintjén. Négy fő kategóriára van osztva a költség alkalmazás szinten: Fejlesztési, támogatási, bérköltségek és egyéb. Az alkalmazás portfólió nyilvántartásban alkalmazásonként egy érték szerepel. A folyamatos alkalmazás portfólió menedzselés része a költségarányok figyelemmel kísérése a portfólión belül. Az alkalmazás fejlesztés és támogatás kiszervezett tevékenység. A költségek értéke, amik a központi nyilvántartásban szerepelnek, tartalmazzák az alkalmazások fejlesztéséhez tartozó projekt költségeket is. A projekt költségeknek a monitorozása a projektvezetők hatáskörébe tartozik, ezzel a költségelemmel nem foglalkoztunk az akciókutatásban. A költséganalitika nem látható a nyilvántartásban, az információkat, adatokat több különböző forrásból kellett összegyűjteni. A költségcsökkentés fontos volt a felső vezetésnek ezért a támogatást is megkaptuk a projekthez. A projekt igénye 3 hét alatt körvonalazódott. Csökkentenünk kellett a költségeket, részletesen megvizsgálva, milyen szolgáltatások állnak az egyes költség elemek mögött. A projekt időtartama 6 hónap volt. 12 dedikált tagja volt a projektnek. A célja a projektnek az informatikai alkalmazás költségek csökkentése 10%-al a kiválasztott 6-os számú alkalmazás portfólióban. Az informatikai alkalmazások a nagyvállalat gyártási egységéhez tartozó üzleti folyamatokat támogatták. A portfólióban az egyik gyártási részel üzleti folyamatait támogató informatikai alkalmazások voltak.

Helyzetfelméréssel kezdődött a projekt. Listázva lettek a portfólióban szereplő alkalmazások, költségelemekkel. Utána megvizsgáltuk, melyek a legmagasabb költségelemek. A következő lépésben, a portfólióban szereplő rekordok, tételek szét lettek osztva a projekt tagjainak. Egy rövid pár órás oktatás történt számunkra, hogy szakmai ismereteket szerezzünk az alkalmazás költségekről. A csapat tagjai lokálisan nem egy helyen voltak, így az információk összegyűjtése, kommunikáció is virtuálisan történt. A 16. táblázat mutatja, hogy milyen információ állt rendelkezésre a költségekről

A táblázat nem valós pénzügyi adatokat tartalmaz, a portfólió analitikának a struktúráját szemlélteti. A költségeknek az elemzése mellett, meghatározása került az is, hogy jogos elszámolás történik-e az adott alkalmazásokra. Az információ összegyűjtésében, pénzügyi kapcsolattartó lista frissítése sok időt vett igénybe.

Év	Hónap	Alkalmazás egyedi azonosító	Alkalmazás neve	Éves fejlesztési ktg.	Éves támogatási ktg	Éves szolgáltatás ktg	Éves ktg Egyéb kategória	Éves Összes költség	Üzleti kritikusság besorolás	Portfólió	Alkalmazás besorolás
2017	12	ANG-0111	Alk_1	$20,419.10	$52,963.45	$210,514.57	$0.00	$283,897.12	4	6	Stratégiai
2017	12	BCD-1234	Alk_2	$4,326.00	$0.00	$129,308.93	$0.00	$133,634.93	5	6	Elavult
2017	12	CDF-8973	Alk_3	$134,567.43	$348,358.74	$32,988.00	$5,181.00	$521,095.17	4	6	Elavult
2017	12	BHA--3278	Alk_4	$4,396.00	$108,214.86	$0.00	$0.00	$112,610.86	4	6	Elavult
2017	12	EVD-3291	Alk_5	$67,010.00	$11,189.24	$25,645.72	$0.00	$103,844.96	5	6	Stratégiai
2017	12	FTR-4567	Alk_6	$212,900.00	$3,498.54	$721,645.72	$0.00	$938,044.26	5	6	Taktikai
2017	12	GCL-6781	Alk_7	$55,080.00	$391,156.20	$134,845.72	$17,919.00	$599,000.92	5	6	Stratégiai
2017	12	PRTS-9810	Alk_8	$350,200.00	$33,156.20	$33,682.13	$0.00	$417,038.33	5	6	Stratégiai
2017	12	COL-3245	Alk_9	$25,000.00	$31,056.20	$6,798.34	$0.00	$62,854.54	5	6	Elavult

16. táblázat Informatikai költségek alkalmazásonként
Forrás: saját szerkesztés

A 17. táblázat a mérlegkészítéshez használt informatikai rendszerből kinyert információkat szemlélteti. A dívizó és a mérlegfő kód a pénzügyi mérlegben szereplő azonosító. Számunkra nem jelentett addicionális információt az elemzéshez. A számla leírása, vagy akár a szervízeknek, szolgáltatásoknak a rövid ismertetése kevés információ ahhoz, hogy pontosan azonosítani lehessen a költségelemet. A szolgáltatás tulajdonosoknak (Service Owner) a megkeresése több hetet vett igénybe. Ők tudtak tovább irányítani minket a pénzügyi kapcsolattartókhoz. Az egyéb kategóriában lévő: LBR jelentése, Labor, tehát személyi jellegű költség. Szerverekhez, processzor használathoz tartozó költségek analitikáját kértük be. Itt egy összeget látni. A részletezéshez a megfelelő támogató csapat tudott további adatokat biztosítani. A kommunikáció e-maileken keresztül történt. Gyakran előfordult, hogy az E-mailekre nem válaszoltak a kollégák, így a belső céges chat hálózaton keresztül történt a megkeresés és kommunikáció. A végleges döntést, adatokat E-mailen bekértük, hogy visszakereshetőek legyenek az információk. Meetingekre, találkozókra hetente volt szükség. A szolgáltatás tulajdonos azonosítása után, sikerült részletesebb riportokat nyerni a pénzügyi elszámoló rendszerekből, amik az elemzéshez sok segítséget adtak. Megvizsgáltuk mennyi volt a CPU (Central Processor Unit), használat és az ehhez tartozó költség. Elemzésünkhöz megnéztük, hogy havonta hogyan változik a CPU használat alkalmazásonként. A változás mögötti okok kiderítésére a technikai szakemberektől nyertünk információt. A személyi jellegű költségek elemzése több időt vett igénybe, akár több hónapot is. Előfordult, hogy ugyanarra a költségkódra, több fejlesztő regisztrálta a munkaóráit. Ez azért volt probléma, mert nem láttuk fejlesztőnként a munkaórát, fejlesztési órákat, így a költséget sem. Az elszámolásnak a javítását kezdeményeztük, de a javítás több hónapot vett igénybe. A projekt végére több, mint 10%-os költségcsökkentést sikerült elérnünk. A nagyvállalat felső vezetése észlelte azt a problémát, hogy nem megfelelő az informatikai költségek nyilvántartása, az elszámoláson nincs megfelelő kontroll. Automatikus elszámolások futnak, manuális jóváhagyás nélkül olyan számlaszámokon, ahol szükség lenne pénzügyi jóváhagyó bevonására. Olyan költségek is elszámolásra kerültek a vállalatnál adott számlaszámra, melyeket az adott terület vezetői nem tartottak jogosnak. Adott esetben szükség volt a költségeknek a transzferálása egyik számlaszámról a másikra. A számla nyitás és számlazárási folyamat több hónapot vett igénybe.

Év	Hónap	Alkalmazás egyedi azonosító	Dívizió	Mérleg fő kód	Osztály kód	Számlaszám	Számla leírása	Szervíz 1	Szervíz 2	Egyéb	Éves Összes költség
2017	12	ANG-0111	1G	9975	536	12KZ	Implementáció	SD	Egyéb szolgáltatás	LBR	$283 897,12
2017	12	BCD-1234	1G	9975	536	12KZ	Beszerzés	SD	Egyéb szolgáltatás	AHE	$133 634,93
2017	12	CDF-8973	1G	9975	536	12MZ	Implementáció	SD	Egyéb szolgáltatás	LBR	$521 095,17
2017	12	BHA--3278	1G	9975	536	12MZ	Támogatás	SD	Egyéb szolgáltatás	AHE	$112 610,86
2017	12	EVD-3291	1G	9975	536	12PP	Beszerzés	SD	Storage	Tape	$103 844,96
2017	12	FTR-4567	1G	9975	536	12PP	Implementáció	SD	MVS	CPU	$938 044,26
2017	12	GCVL-6781	1G	9975	536	12PP	Támogatás	SD	MVS	TAPE	$599 000,92
2017	12	PRTS-9810	1G	9975	536	12KZ	Beszerzés	SD	MVS	DASD	$417 038,33
2017	12	COL-3245	1G	9975	536	12KZ	Implementáció	SD	MVS	CPU	$62 854,54

17. táblázat Informatikai költségek részletezése mérleg adatok alapján
Forrás: saját szerkesztés

A komplex üzleti, informatikai folyamatok mellett az informatikai költséganalitikához szükséges adatok összegyűjtése erőforrás igényes. Az informatikai költségek különböző rendszerekben vannak tárolva, a számlák leírásához tartozó kódok nem mindig mutatják és részletezik a mögötte álló szolgáltatást. Szükség van az informatikai alkalmazás portfólióra és ezen belül is a költségek monitorozására, mert a részletes elemzéssel, átvilágítással költségcsökkentést tud eredményezni a nagyvállalat. A vállalat felső vezetésének megfogalmaztuk az informatikai költségelszámolásban lévő hiányosságokat. A pénzügyi kapcsolattartók listája nem naprakész. Adott számlaszámon lévő költségelemek azonosítása több hónapot vesz igénybe a bonyolult és összetett elszámolási folyamatok miatt. Nincsen egységes, szabályozott utasításrendszer az informatikai alkalmazás költségelszámolásra. Az akciókutatás és az interjúk alapjáb megállapítom, hogy a nagyvállalatoknál az informatikai alkalmazás költséganalitikára szükség van.

3.4 Összefoglalás

A stratégiák kidolgozásával és implementálásával párhuzamosan az informatikai alkalmazások felülvizsgálata és konszolidációja együtt támogatja a fejlesztési irányokat. Az alkalmazások portfólióba sorolása és a redundáns alkalmazások kiszűrésével csökkenteni lehet a támogatási, fejlesztési és infrastrukturális költségeket. Ehhez azonban az szükséges, hogy az informatikai irányításnak része legyen az alkalmazás portfólió menedzsment. Az alkalmazás portfólió racionalizációval párhuzamosan, alkalmazás redundanciák csökkentésén keresztül, az informatikai alkalmazás költségek allokációjával költségmegtakarítást tudnak elérni. Az ITIL v3 tesz utalást az informatikai szolgáltatásokhoz tartozó költséganalitikára, de ezt még nem veszik figyelembe a nagyvállalatok. Szükség lenne egy olyan ajánlásra, kiegészítésre, ami felvázolja az alkalmazás portfólió menedzsment szükségességét és emellett egy útmutatást ad az alkalmazás szintű informatikai költségek elemzésére, nyilvántartására. A tudományos felmérések és az interjú eredmények elemzése igazolja hipotéziseimet. Az informatikai szolgáltatások menedzselésére széleskörűen használt ITIL ajánlás mellett szükség van egy kiegészítésre, ami az alkalmazás szintű költséganalitika kialakítását részletezi.

4. INFORMATIKAI KOCKÁZATMENEDZSMENT

Ebben a fejezetben az informatikai kockázatok analitikájának a fontosságát fejtem ki. Megvizsgálom a lehetséges kapcsolódási pontokat az informatikai alkalmazás portfólió képzéssel. A szervezeteknek biztonsági szempontrendszerébe be kell építeni azt, hogyan csökkenthetőek a kockázatok. Az előre nem látható, bekövetkezett események hatással vannak a vállalat működésére, folyamataira. A kockázatok értékelése nehéz a gyorsan változó technológia és az állandó fenyegetések miatt. A vezetésnek látnia kell, hogy milyen kockázatokat hordoznak az informatikai projektek, informatikai fejlesztések, informatikai alkalmazások nem megfelelő üzemeltetése. A vállalatoknak ismerniük kell az informatikai alkalmazásukat ahhoz, hogy a lehetséges támadásokra felkészüljenek, vagy akár kalkulációt végezzenek az informatikai incidensekből származó veszteségekre. A lehető legbiztonságosabb működés egyik feltétele a kockázatok szintjének és mennyiségének a csökkentése. A kockázatmendzsment a biztonság alapja. Az IT kockázatmenedzsmenti stratégiák kidolgozásánál figyelembe kell venni a szervezet specifikus kockázati profilját és az üzleti célokat is [129]. Az általános kockázatmenedzsment ismertetése után az informatikai kockázatok fogalmi keretét tisztázom. Az informatikai kockázatkezelésre ITIL v3 ajánlását, illetve a COBIT5 nemzetközi szabvány keretrendszernek a releváns részeit tanulmányozom. Egy esettanulmány bemutatása után az informatikai kockázatok beépítésének a lehetőségét igazolom az informatikai alkalmazás portfólióba. Informatikai keretrendszernek az implementálása hosszú és időigényes folyamat, az első lépés a bevezetésnél az üzleti folyamatoknak a feltérképezése. A második lépés az informatikai folyamatok vizsgálata, informatikai alkalmazások nyilvántartása, majd a kockázatok azonosítása, elemzése, mérése, monitorozása.

Több esettanulmány elemzi az előnyöket és fejlesztésre szoruló területeket, amit egy informatikai keretrendszer implementálása során tapasztaltak a szervezetek. A Sarbanes-Oxley törvény előírásainak kellett megfelelnie három brazil vállatnál. A felső vezetés támogatása kulcstényező volt a keretrendszer sikeres implementálásának [130]. A vállalati kultúra, a felső vezetés ismeretei, tudása is meghatározó tényező. Sok kockázatot azonosítottak a projekt során [131]. Fontos a tapasztalat, illetve a bevezetési projektben részt vevő személyeknek a szakmai tudása. A megfelelő keretrendszer kiválasztása után a szervezetre könnyen adaptálható technikák és eszközök felhasználása

mellett a dolgozóknak a képzése is kulcstényező [132], [133], [134]. Igaz sok vállalatnál vannak kezdeményezések, hogy az informatikai kockázatmenedzsment integrálódjon a vállalati „általános" kockázatmenedzsmentbe. Általános kockázatmenedzsment kezelésére a legtöbb vállalat a COSO által fejlesztett ERM (Enterprise Risk Management Framework), tehát vállalati kockázatmenedzsment keretrendszert használja [135]. Ennek a keretrendszernek a teljes, gördülékeny használata még nem kiforrott a szervezetekben. A bevezetés után nehéz mérni a hatékonyságot, valamint a bekövetkezett szervezeti változásokra lassan, nehézkesen reagálnak a munkavállalók [136]. 2017 márciusában publikáltak egy felmérést az ERM szakértői 586 felsővezetővel, szakértővel. Európa, Anglia, Ázsia, Ausztrália, Afrika, Közel-Kelet, és az USA országaiban. Az elmúlt 5 évben a kockázatoknak a számossága és komplexitása sokat nőtt, egyre összetettebbek, bonyolultabbak a szervezetekben. Ezzel párhuzamosan a válaszadó cégeknek csupán a 30%-a mondta azt, hogy befejezett, teljes ERM keretrendszer használnak [137]. Az informatikai kockázatmenedzsment elkülönül, a vállalati kockázatmenedzsmenttől. Nincs egységes ajánlás, mit kell tekinteni informatikai kockázatoknak, a vállalatoknak saját definiciót és listát kell készíteni. A kiberkockázatok alakulását és hatásait évről évre egyre nagyobb figyelemmel kísérik a cégek. A kiberkockázatokat üzleti és informatikai kockázatoknak is tekintik.

2017-ben készített egy felmérést a PWC (PriceWaterHouse) 80 különböző országban, 1581 válaszadóval. A szervezetben felsővezetői szinten kell, hogy beépüljön a vállalati kultúrába, kommunikációba, rutin döntéshozatali struktúrába a kockázatmenedzsment minden lépése [138]. Az Open Group felmérése azt mutatja, hogy a vállalatok 63%-a használ, több mint egy keretrendszer az informatikai kockázatok menedzselésére. A leggyakrabban használt keretrendszerek: ISO/IEC 27001, ISO/IEC 27005, ISO 31000, és a COBIT [139]. Problémát jelent a vállalatoknak a különböző keretrendszereket értelmezni. Nemcsak sok időt és energiát vesz igénybe, de pénzügyileg is költségigényes a tanácsadók alkalmazása, munkavállalók oktatása. Piacról képesítéssel rendelkező szakembereknek a bevonása pedig jelentős többletköltséggel is jár. A KPMG 2017-es tanulmánya 15 országban, 832 válaszadóval készült. A vállalatoknak 38%-nál van stabil kockázatmenedzsment rendszer kialakítva. A legnagyobb kihívásnak a vállalatok a jogi szabályozásnak való megfelelést, kiberbiztonság kockázatának a kezelését tekintik. Az ellenőrző egységek tagjainak több, mint a 40%-a gondolja azt, hogy a kockázatkezelési programok és folyamatok jelentős munkát igényelnek. Közel

ugyanannyian gondolják, hogy egyre nehezebb felügyelni a kockázatokat. A legnagyobb problémának a kiber kockázat kezelésére a szervezeti tudatosságot, kultúrának a hiányát, valamint az informatikai rendszerek naprakészen tartását tartják a válaszadók. A lehetséges megoldás a belső audit erősítése. A kulcs működési kockázatok, mint a kiber és technológiai kockázatok, a hozzájuk kapcsolódó ellenőrzések fontosak. Az audit terveknek rugalmasabbnak kell lenni, hogy alkalmazkodjon a változó üzleti környezetekhez. Kiterjesztett, bővített audit tervekre van szükség a kiber kockázatok kezelésére, a legfontosabb működési és technológiai kockázatokra [140]. Ernst & Young vállalat 2014-ben készített felmérést az informatikai kockázat menedzseléséről a pénzügyi szektorban. A megkérdezettek 92%-a már kialakított valamilyen keretrendszert az informatikai kockázatok kezelésére, valamint dedikálta munkavállalók is vannak, akik ezzel foglalkoznak. Fejlesztendő terület közé kell sorolni a közös kockázati nyelvet. Szükség van az üzlet és informatika összehangolására, valamint keretrendszerek létrehozására, ami elősegíti a kockázatok hatékony meghatározását és döntések előkészítését. Több keretrendszert is használnak az informatikai kockázatok kezelésére: 50% ISO27005:2008-at, 39%-a ISACA IT kockázati keretrendszert [141]. A CISCO nagyvállalat 2017-ben készített egy riportot, 13 országban, 3000 biztonsági vezetővel. Sok különböző biztonsági megoldást használnak a cégek egyszerre. A szervezeteknek a 38%-a különválasztja az informatikai és a biztonsági funkciókat. Az informatikai biztonság fejlesztéséhez nincs elegendő szakember a piacon, kevés az erre fordítható költségvetés, valamint a rendszerek kompatibilitásával is sok a probléma [142].

A következő alfejezetben egy rövid ismertetést adok a vállalati kockázatkezelésről. Az informatikai kockázatmenedzsmentre használt keretrendszerek, szabványok, ajánlások elkülönülnek a vállalat egész működésére, folyamataira alkalmazható szabványoktól. A szervezetekben kockázatmenedzsment elemzésével foglalkozó szakembereknek nehezen értik és látják át az informatikai folyamatokat és az informatikai kockázatokat.

4.1 Kockázatok meghatározása

A Nemeztközi Szabványügyi Szervezet (International Organisation of Standards, ISO), és a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, IEC) és hasonló szabályozó testületek összesen 42 db közvetlen és 211 db

közvetett módon a kockázatokkal foglalkozó szabványt tartanak érvényben [143]. A kockázat meghatározásánál nem készítek történeti áttekintést, illetve részletes, mindenre kiterjedő csoportosítást. A kockázatot a szakirodalom közgazdasági, műszaki, pszichológiai, szociológia és antropológiai megközelítést alkalmazza. Témámhoz a legközelebb a közgazdaságtani és műszaki szempontok állnak. Kockázat alatt a kedvezőtlen bekövetkezési valószínűségét értjük. Az esemény hatása lehet negatív és pozitív. A nagyvállalatoknál a pénzügyi veszteség csökkentése érdekében a negatív hatáselemzés a fontos. Frank H. Knight szerint a kockázatot és a bizonytalanságot el kell különíteni egymástól. Kockázat az, amikor nem tudjuk, hogy pontosan mi fog történni, de a bekövetkezési valószínűségeket ismerjük. Bizonytalanság pedig, amikor a bekövetkezési valószínűséget sem ismerjük [144]. Hillson megállapítása, hogy a kockázat bizonytalan eseményekre vonatkozik. Lehetnek negatív és pozitív hatásai [145]. A kockázatokra sokféle csoportosítás létezik.

A kockázatokat két fő csoportba soroljuk: **külső kockázatok**: piaci, vállalati, régiós és **belső k**ockázatok: folyamatok, szervezeti, beruházási, szervezeti kockázatok [146].

A **COSO** Vállalati Kockázatkezelési keretrendszer négy fő kategóriát határoz meg:

- **Stratégiai kockázatokhoz** olyan kockázatok tartoznak, amelyek az üzleti stratégiai döntésekkel, vagy üzleti tervek módosításával, innovációval, ügyfelekkel, piaccal, befektetővel, márkával, tervezéssel, külső partnerekkel, kutatás és fejlesztéssel kapcsolatosak.
- **Működési kockázatokat** okozhatják külső események, a nem megfelelően végzett üzleti folyamatok. Emberi, technológiai, vagy kommunikációs hibák, szabályok nem követése. Beletartozik a jogi kockázat, viszont kizárja a stratégiait.
- **Pénzügyi kockázatok** az inflációs és likviditási kockázatok.
- **Egyéb kockázatok** közé a projekt, harmadik féllel való együttműködésből fakadó kockázatok sorolhatóak. Környezeti, beruházási, gazdasági kockázatok [147].

Az integrált kockázatkezelésnek, más néven a vállalati kockázatkezelés 2.0-nak összevontan kell kezelnie a pénzügyi, működési, stratégiai és üzleti kockázatkezelést. A pénzügyi kockázatkezelésbe tartoznak a pénzügyi, fizetőképességi és hitel kockázatok. A működési kockázatkezelésbe a működéssel kapcsolatos kockázatok tartoznak. Stratégiaiba pedig a szervezet irányításával kapcsolatban felmerülő kockázatok, illetve a termékek, szolgáltatások kockázatai [148]. A kockázatok azonosításához elengedhetetlen

az üzleti folyamatok azonosítása. A folyamatmenedzsment és kockázatmenedzsment területeknek az összehangolása a legtöbb szervezetben nem megoldott, gyakran párhuzamos szabályozás történik a vállalatokban [149]. Véleményem szerint a legfontosabb a kockázatok megfelelő azonosítása, értelmezése, valamint a kezelt kockázatok körének a pontos körülhatárolása. Nagyvállalatoknál a szervezeti sajátosságból adódik, hogy a társosztályoknak, funkcionálisan elkülönült területeknek együtt kell dolgozniuk a bizonytalanságok felmérésénél. A kockázatkezelést sok eltérő nemzetközi keretrendszer, szabvány foglalja össze és rendszerezi.

Kockázatkezelési keretrendszerek, szabványok

A kockázatmenedzsment lépései: kockázat tervezés, kockázatok meghatározása, definiálása, minőségi vagy mennyiségi kockázat elemzés, kockázat értékelése és kezelése, majd a kockázat monitorozása, ellenőrzése.

Elterjedt kockázatkezelési keretrendszerek:

COSO (Committee of Sponsoring Organizations of the Treadway Commission): ERM (Enteprise Risk Management), Vállalati Kockázatmenedzsment [135].

M_o_R (Management of Risk) [150].

ISO31000: 2018 Kockázatmenedzsment és irányelvek [151].

ISO31010: 2018 Kockázatkezelés, kockázat felmérési eljárások [152].

Az M_o_R általános megközelítése mellett konkrét folyamatlépéseket is tartalmaz a kockázatkezelésre. Az ISO31000 érthetően, egyszerűen próbálja a vállalatokat támogatni azzal, hogyan kezeljék a kockázatokat. 2009 óta 2018-ban jelent meg a bővített, érthetőbb verzió. A COSO meghatározásával ellentétben, a kockázatnak nemcsak negatív, hanem pozitív hatása is lehet. ISO31010 pedig három fő részből áll: alapelvek, keretmodell és folyamat.

A különböző kockázatkezelési szabványok eltérő módszereket alkalmaznak a kockázatok azonosítására, a kockázatok bekövetkezési valószínűségének a becslésére, a kockázati érték meghatározására Eltérően javasolják a kockázatokra a reagálást, monitorozást. A **minőségi (kvalitatív)** kockázatelemzés viszonylag gyorsan adaptálható és olcsó megoldás. Mivel számszerűsíteni nem lehet az eredményeket, nehezebben

értékelhető, mint ha a **mennyiségi (kvantitatív)** kockázatelemzést végzünk. A számbavételt nehezíti az, hogy nem tudja a szervezet az összes kockázatot listázni, így a bekövetkezés valószínűsége és a veszély előfordulásából adódó kár értéke sem becsülhető. A kvalitatív mérésnél az elszenvedhető kár mértéke a bekövetkezés gyakoriságával arányos. A 18. táblázat tartalmazza a kockázatkezelésre, értékelésre alkalmazható eszközöket. Jól szemlélteti, hogy a kockázatértékelési folyamatban melyik eszköz és módszer mennyire alkalmazható [153].

Eszközök és módszerek	Kockázatértékelés folyamata				
	Kockázat azonosítása	Kockázatelemzés			Kockázat kiértékelése
		Következmény	Valószínűség	Kockázati szint	
Brainstorming	JA[1]	NA[2]	NA	NA	NA
Interjuk	JA	NA	NA	NA	NA
Delphi szakértői módszer	JA	NA	NA	NA	NA
Ellenőrzési jegyzék	JA	NA	NA	NA	NA
HAZOP	JA	JA	A[3]	A	A
HACCP	JA	JA	NA	NA	JA
Környezeti kockázat értékelése	JA	JA	JA	JA	JA
SWIFT (Mi van ha?)	JA	JA	JA	JA	JA
Szcenárió elemzés	JA	JA	A	A	A
Üzleti hatás elemzése	A	JA	A	A	A
Gyökérok-elemzés	NA	JA	JA	JA	JA
Hibamód és –hatás elemzése	JA	JA	JA	JA	JA
Hibafa-elemzés	A	NA	JA	A	A
Eseményfa-elemzés	A	JA	A	A	NA
Ok és következmény elemzése	A	JA	JA	A	A
Ok-hatás elemzés	JA	JA	NA	NA	NA
Döntésfa	NA	JA	JA	A	A
Emberi megbízhatóság elemzése	JA	JA	JA	JA	A
Csokornyakkendő-elemzés	NA	A	JA	JA	A
Megbízhatóság alapú karbantartás	JA	JA	JA	JA	JA
Markov-elemzés	A	JA	NA	NA	NA
Monte Carlo szimuláció	NA	NA	NA	NA	JA
Bayes-módszer	NA	JA	NA	NA	JA
FN görbék	A	JA	JA	A	JA
Következmény/valószínűség mátrix	JA	JA	JA	JA	A
[1] Jól alkalmazható; [2] Nem alkalmazható; [3] Alkalmazható					

18. táblázat A kockázatértékelés eszközeinek alkalmazhatósága
Forrás: [153]

A minőségi elemzésekhez a leggyakrabban használt módszerek: HAZOP (Hazard and Operability Studies) Veszély-és Üzemeltethetőség Vizsgálat [154], HACCP (Hazard Analysis and Critical Control Points) Veszély és Kritikus Szabályozási Pontok [155].

4.2 Informatikai kockázatok keretrendszere

Az informatikai kockázatok meghatározására sok meghatározás, szabvány van. Az Európai Hálózat és Információbiztonsági Ügynökség (European Union Agency for Network and Information Security, ENISA) ajánlása 16 IT-hoz kapcsolódó szabványt és módszert ajánl. Austrian IT Security Handbook, CRAMM (CCTA Risk Analysis and Management Method), ami az Egyesült Királyság Central Computer and Telecommunication Agency által kidolgozott kockázatelemzési és kezelési módszertan:

Dutch A&K Analysis, Ebios (Expression des Besoins et Identification des Objectifs de Sécurité, Ebios), ISAMM (Information Security Assessment and Monitoring Method, ISAMM), ISF (Information Security Forums) Methods, ISO/IEC 13335-2, ISO/IEC 17799, ISO/IEC 27001, IT-Grundschutz, Magerit, Marion, Mehari, MIGRA, Octave, RiskSafe Assessment, SP800-30 [156]. Egyéb törvények is vannak, mint például: SOX (Sarbanes-Oxley). Használatával növelik a vállalatok a pénzügyi átláthatóságukat [157]. HIPAA (Health Insurance and Accountability Act), Egészségbiztosítási Hordozhatósági és Felelősségi Törvény Titoktartási Szabálya [158]. GDPR (General Data Protection Regulation), Általános Adatvédelmi Előírás, ami egységes uniós adatkezelésre vonatkozó szabályrendszer [159].

A legtöbb szakirodalom, az informatikai szoftverek fejlesztési lépésihez definiálja a felmerülő informatikai kockázatokat, vagy informatikai projektekhez rendeli.

Informatikai kockázat az ISACA meghatározása alapján: olyan üzleti kockázat, amely az informatika bevonásához, használatához, működtetéséhez, befolyásolásához kapcsolódik. Az informatikával kapcsolatos eseményekből és feltételekből áll, amelyek potenciálisan befolyásolják az üzleti tevékenységet [160].

Informatikai kockázat (ISO/IEC 13335-1) meghatározása szerint: Az a lehetőség, hogy egy adott fenyegetés kihasználja az eszköz, vagy eszközcsoport sebezhetőségét, ezáltal kárt okozva a szervezetnek. A kárt az esemény valószínűségének és következményeknek a kombinációjával mérjük. Az eszközök alatt fizikai eszközöket (hardver, computer), információkat, adatokat, embereket értjük [161].

Boehm 1991-ben az informatikai szoftver projekt kockázatok közé sorolta az alábbiakat: személyekhez kapcsolódó kockázatok, irreális ütemtervek, hiányosságok, a követelményeknek a folyamatos változása, feladatok hiányosságai [162]. Schmidt 2001-ben 33 különböző szoftver kockázatokat definiál. Néhány ezek közül: Felhasználókhoz kapcsolható kockázatok: a felhasználók nem vesznek részt megfelelően a folyamatokban, tevékenységekben. Követelményekhez kapcsolható kockázatok: félreértett követelmények. Megfelelő készségek, szakértelem, tudás, hozzáállás hiánya. A vezetőség nem eléggé elkötelezett, tehát ennek a hiánya is komoly kockázatokat hordoz magában. [163]

Az ISACA az informatikai kockázatokat három kategóriába sorolja:

1.Informatikai előnyökhöz és értékmegőrzéshez kapcsolódó kockázatok: ezek a kockázatok, amelyek olyan kihagyott lehetőségekhez kapcsolódnak, melyek az üzleti folyamatok hatékonyságának a javítását segítenék elő. Konkrét példa, ha egy szervezet nem végez vizsgálatokat, elemzéseket arra vonatkozóan, hogy a szolgáltatásait felhő technológiával támogassa. Felhő alapú megoldásokkal a következő előnyöket érhetik el a szervezetek: költségmegtakarítás, időmegtakarítás, egyszerű telepítés és nagyobb rugalmasság, agilitás.

2.Informatikai program és projekt kockázatok: Azok az informatikai kockázatok tartoznak ide, amik akkor keletkezhetnek, amikor az informatika hozzájárul az új, vagy továbbfejlesztett üzleti megoldásokhoz projekteken és programokon keresztül.

3. Informatikai műveletekhez és szolgáltatásokhoz kapcsolódó kockázatok. Ide tartoznak az informatikai rendszerek és szolgáltatások teljesítményéhez tartozó kockázatok. Nem szabad figyelmen kívül hagyni a beszállítókkal, tehát egy harmadik féllel történő együttműködés során felléphető informatikai kockázatokat sem. A 11. ábra az ISACA csoprotosítása az informatikai kockázatokra. Az informatikai kockázatok benne vannak a szervezeti kockázatokban.

11. ábra Informatikai kockázatok kategóriái az ISACA ajánlása alapján
Forrás: [164]

Az ISACA ajánlása az informatikai kockázatmenedzsment keretrendszerre 3 területre bontja a kockázatmenedzsmentet:

Kockázatkezelés: az informatikai kockázatkezelési gyakorlatoknak be kell épülnie a vállalati folyamatokba, lehetővé téve az optimális kockázatot.

Kockázatértékelés: Az informatikával kapcsolatos kockázatokat és lehetőségeket üzleti szempontból azonosítani, elemezni és prezentálni kell.

Kockázatválasz: Az informatikával kapcsolatos kockázati tényezők, lehetőségek, események költséghatékony módon kezelhetőek, valamint összhangban vannak az üzleti prioritásokkal [164], [165].

A nagyvállalatok lassan alkalmazkodnak ahhoz, hogy kialakítsák a folyamatokat az informatikai kockázatok kezelésére. A probléma hátterében az áll, hogy kevés a megfelelően képzett szakember, valamint a cég felsővezetői nehezen ismerik fel azt, hogy az informatikai kockázatok hatással vannak az üzleti célokra, folyamatokra. Az egyik kihívás a kockázatelemzés megvalósítása a felhő alapú számítástechnikai megoldásokhoz, ami üzleti követelmények és technikai intézkedéseknek az együttese. A kiszervezett tevékenységre is meg kell találni a megfelelő kockázat elemzési eszközöket, technikákat [166]. Informatikai kockázathoz nemcsak a természeti katasztrófát, vagy tűz és robbanásveszélyeket kell sorolni. vagy a DRP, BCP készítését. A magyarországi informatikai kockázatkezelés helyzetére a nagyvállalati körben nincsen statisztika, a rendelkezésre álló felmérések elavultak.

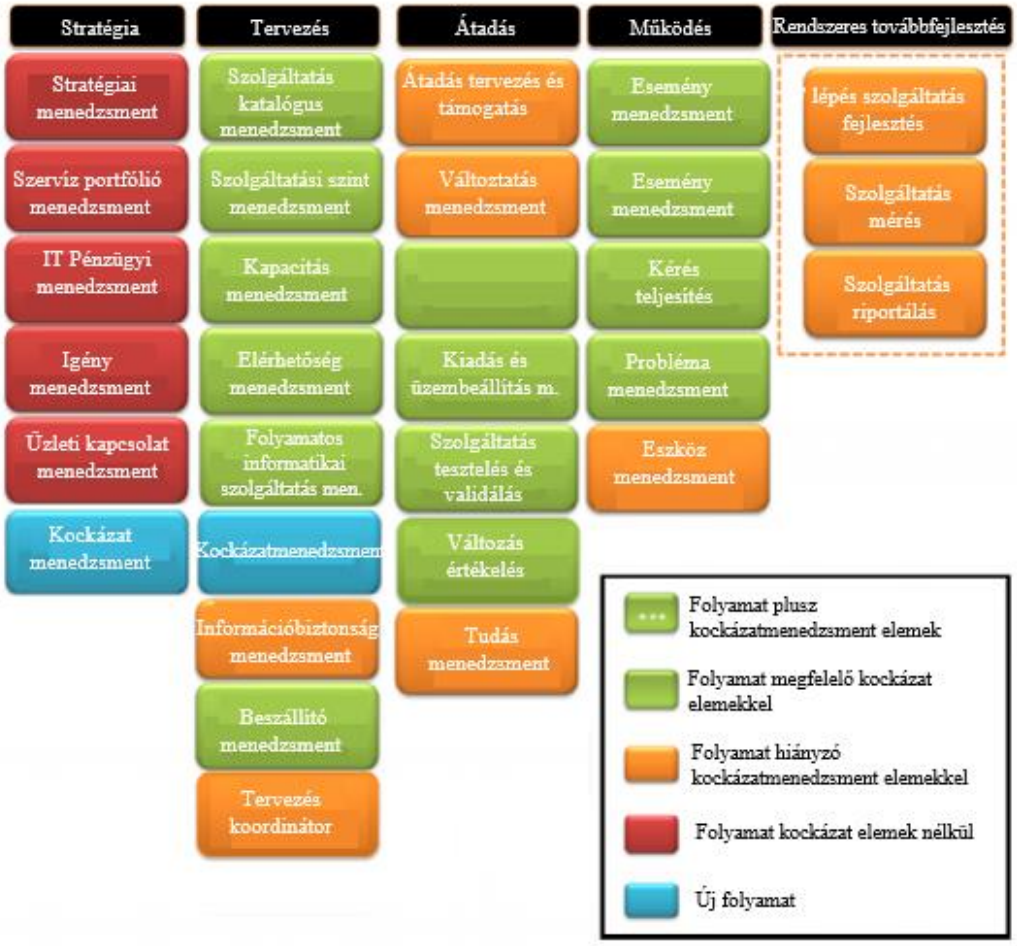
Informatikai kockázatok számszerűsítése: Az informatikai kockázatok azonosítása, számbavétele után az informatikai kockázatoknak a mérése a következő feladat. Ez a legnehezebben körülhatárolható terület az informatikai kockázatmenedzsmentben. Mit kell mérni és hogyan lehet számszerűsíteni a hatásokat.. A szabványok, ajánlások használatára koncentrálnak a nagyvállalatok. Az informatikai kockázatok nyilvántartása mellet számszerűsíteni kell a hatásokat is. A számszerűsítésnek, automatikusnak és dinamikusnak kell lennie. Legalább azokra a folyamatokra, alkalmazásokra el kell végezni az informatikai kockázat besorolást és számszerűsítést, amelyek élesben működnek. Ha kevés a kapacitása a nagyvállalatnak, akkor az üzletileg kritikus, vagy stratégiai alkalmazásokat kell fontossági sorrendben az első helyre helyezni. Egy adott informatikai káresemény bekövetkezési valószínűsége, okozott kár meghatározása sok kihívással, erőforrással jár. Véleményem szerint egy informatikai kockázati lista és egy rangsorolás megléte már nagy előrelépés lehet a kockázatok felülvizsgálatához. A felső vezetésnek támogatnia kell azt is, hogy a besorolás, értékeléshez felelősök legyenek rendelve. Az informatikai kockázatok mérésénél a hibák elkerülésére kell törekedni. A továbbiakban azt elemzem, hogy az

ITILv3, illetve a COBIT5 informatikai irányítási keretrendszerben hogyan jelenik meg az informatikai kockázat értékelés.

4.3 Az ITIL informatikai kockázatkezelése

Az ITIL-ben van utalás arra vonatkozóan, hogy a szervezeteknek kell foglalkozni a kockázatokkal. Az ITIL nem a kockázatkezelésre kiadott ajánlás, de kitér rá. Valószínű, hogy a szervezet más szabványt és ajánlást is fog használni a kockázatkezelésre az ITIL mellé, de az informatikai folyamatokhoz rendelhető informatikai kockázatok definiálása megtörténhet az ITIL implementálásával párhuzamosan.

A Szolgáltatásstratégia és a Folyamatos Szolgáltatásfejlesztés könyvek definiálják és meghatározzák, a kockázatokat és a kockázatmenedzsmentet. A kockázatkezelés konkrét folyamatának hiányát a Folyamatos Szolgáltatásfejlesztési (Continual Service Improvement) könyvben próbálják meg tisztázni. Az ajánlások szerint a kockázatkezelésnek a helye a tervezés (design) és az átadás (transition) fázisokban kell elhelyezkednie. Az ITIL-ben a kockázatmenedzsment egy folyamatos tevékenységet jelent. Első lépés a fenyegetések azonosítása, majd speciális, bizonyos fenyegetésekhez a kritikus eszközök sebezhetőségének értékelésének a meghatározása. Ezután következik a kockázat hatásának, valamint valószínűségének elemzése. A következő lépésben a kockázatok csökkentésének lehetséges alternatíváit kell meghatározni, majd a kockázatcsökkentő intézkedéseknek a priorizálása következik. A folyamatos ellenőrzéssel egy ciklikus menedzselés történik. Részletezi, hogy milyen terminológiákat kell használni a kockázatmenedzsmentben, valamint az egyes szerepköröket is kifejti felelősségi körök meghatározásával. Összességében leírja a fő szempontokat, amire figyelni kell a kockázatmenedzsment során az informatikai szolgáltatás oldaláról. Készült egy tanulmány az M_o_R és az ITIL lehetséges integrációs lépéseit vázolva. Ha a vállalat használja és alkalmazza az ITIL elveit, akkor azzal a problémával szembesül, hogy az informatikai szolgáltatásokhoz kapcsolódó kockázatok kezeléséhez nem kap teljes útmutatást. A tanulmány az M_o_R (Management of Risk) és az ITIL kapcsolatát elemzi. A 12. ábra szemlélteti a lehetséges kapcsolódási pontokat az ITIL és az M_o_R keretrendszer között. ITIL folyamatmodell kiegészítve a kockázatmenedzsment elemeivel, illetve új folyamat beépítésének az ajánlásával látható az ábrán.



12. ábra ITIL kiegészítése a kockázatmenedzsmenttel és új folyamatokkal
Forrás [167]

Ha egy szervezet használja és implementálja az ITIL-t és figyelmet fordít a különböző kockázatok kezelésére is, akkor kevés lehet az ITIL ajánlásban szereplő utalás a kockázatok kezelésére. A tanulmány összegzi, hogy az ITIL-ben lévő kockázatokra vonatkozó definíciók általánosak. A szerzők szerint a kockázatmenedzsment egészének az integrálását a szolgáltatás tervezés szakaszában kell végrehajtani. A kockázatmenedzsment céljainak, koncepciójának kidolgozása pedig a szolgáltatás stratégia részében kell, hogy helyet foglaljon. Az egész kockázatmenedzsmentet pedig a design, tehát a tervezés szakaszban kell megvalósítani [167]. Egy iparági ajánlást mutatok be, amit 2015-ben dolgozott ki a CAPGEMINI globális vezető vállalat egyik szakértője. A tanulmány a hangsúlyt arra helyezi, hogyan lehet a kockázatmenedzsmentet az ITIL folyamataiba beépíteni. A megközelítés kétirányú: „Bottom up”, és „Top down”. A „Bottom up” javaslat alapján az általános kockázatkezelés lépéseit kell integrálni az ITIL

egyes elemeibe. A „Top down” megközelítés szerint szükséges a meglévő folyamatok feltérképezése. A kritikus sikeres faktorok meghatározása is fontos. Következő lépés a kockázatok a definiálása. Az informatikai kockázatmenedzsmentek előkészítését a szolgáltatás stratégiába, a kockázatmenedzsmentet pedig a szolgáltatás tervezés fázisába kell beépíteni.

A szolgáltatás stratégiánál 3 lépést kell végrehajtani:

- Kockázatok forrása és kategóriák meghatározása.
- Kockázatok paramétereinek a definiálása.
- Kockázatmenedzsment stratégia kialakítása.

A siker alapja pedig az lehet, hogy egy dedikált személy, folyamat tulajdonos felelős az informatikai kockázatmenedzsment fejlesztéséért és implementálásáért a szervezetben [168].

A GT elemzés alapján az egyik elméleti kategória az ITIL és az informatikai kockázatmenedzsment kapcsolata. Az informatikai kockázatkezelés folyamata nincs teljes körűen kialakítva a legtöbb nagyvállalatnál. Az ITIL-nek a kockázatkezelésre vonatkozó részét nem elemzik a szakértők. Külön szakma az informatikai kockázatok kezelése, elkülönül az informatikai szolgáltatásmenedzsmenttől. Biztonságra kiterjedő kockázatkezelésre nem alkalmas az ITIL ajánlása, más szabványt, keretrendszert használnak a vállalatoknál. Folyamatos fejlesztésre van szükség az informatikai szolgáltatásmenedzsment területén és ebbe beletartozik az informatikai kockázatoknak a kezelése is. Mivel az incidenseknek vannak kockázataik, ezért bizonyos szinten összekapcsolódik az informatikai szolgáltatásmenedzsment az informatikai kockázatkezeléssel.

Az interjúalanyoknak a témához tartozó véleményéből pár idézet:

„az okozza a problémát, hogy kockázat fajták és kockázat típusok meg kezelésük is számtalan lehet. Nagyon sok kezelve van az IT-n. ....hardware szinten jól működik, ez egy működési kockázat alapvetően.”

„legtöbb rendszer, ami egyébként legalább azokra a rendszerekre, amik működési kockázatban megjelenhetnek, vagy veszteség eseményt generálhatnak, ezekre létezne szolgáltatási szint megállapodás, akkor az azt jelenti, ha ez van, hogy már fel vannak

térképezve az üzleti folyamatok, tudjuk, hogy mögöttük milyen alkalmazások vannak, milyen IT szolgáltatások mennek..”

„Az általános ajánlások jók, viszont amikor nekem egy olyan igényem van, hogy fogalmazzam meg, akkor nem. Tehát a menedzser kér tőlem valamit arra vonatkozóan, hogy ….tárjak fel. Például arra vonatkozóan, hogy egészségügyi adatokat akarunk a felhőben tárolni és.. az összes kockázatot... csak akkor tudják vállalni a felelősséget, hogyha minden kockázattal tisztában vannak. Akkor nem ad az ITIL nekem útmutatást arra vonatkozóan, hogy én hogyan tudok teljesen biztos lenni abban, hogy minden kockázatot feltártam.”

Az interjúk jó támpontot adtak az elméleti kutatásomhoz. Az ITIL-nek nem célja az informatikai kockázatok részletes elemzése, tesz rá utalást. A mindennapi tevékenységekben nehézséget okoz az informatikai kockázatok definiálása, számszerűsítése, riportálása. A menedzsment részéről nem érkezik igény a részletes kimutatásra, de az incidenskezelés részeként visszavezethető az, hogy melyek a legkritikusabb rendszerek, folyamatok. A keretrendszerek közül az COBIT-ot alkalmazzák az informatikai kockázatok kezelésére.

4.4 A COBIT5 informatikai kockázatkezelése

Az ISACA közreműködésével jött létre az IT irányítási intézet (IT Governance Institute), amely létrehozta a nemzetközi szabványt, a COBIT-ot 1996.-ban. A COBIT informatikai követelményeket, folyamatokat és erőforrásokat figyelembe ad ajánlást az informatikai auditok támogatásához. A COBIT5 beépíti az Informatikai Kockázat Menedzsment (Integrated Risk Management Framework, ITRM) lépéseit a tevékenységek közé

Az ITRM jelölései:

- RG: Risk Governance: Kockázat irányítás
- RE: Risk Evaluation: Kockázat értékelés
- RR: Risk Repsonse: Kockázat válasz

13. ábra mutatja a COBIT 5 folyamat referenciamodell, amely integráltan jeleníti meg a 2009-ben kidolgozott Risk IT folyamatmodelleket. 37 irányítási és menedzselési folyamatot tartalmaz.

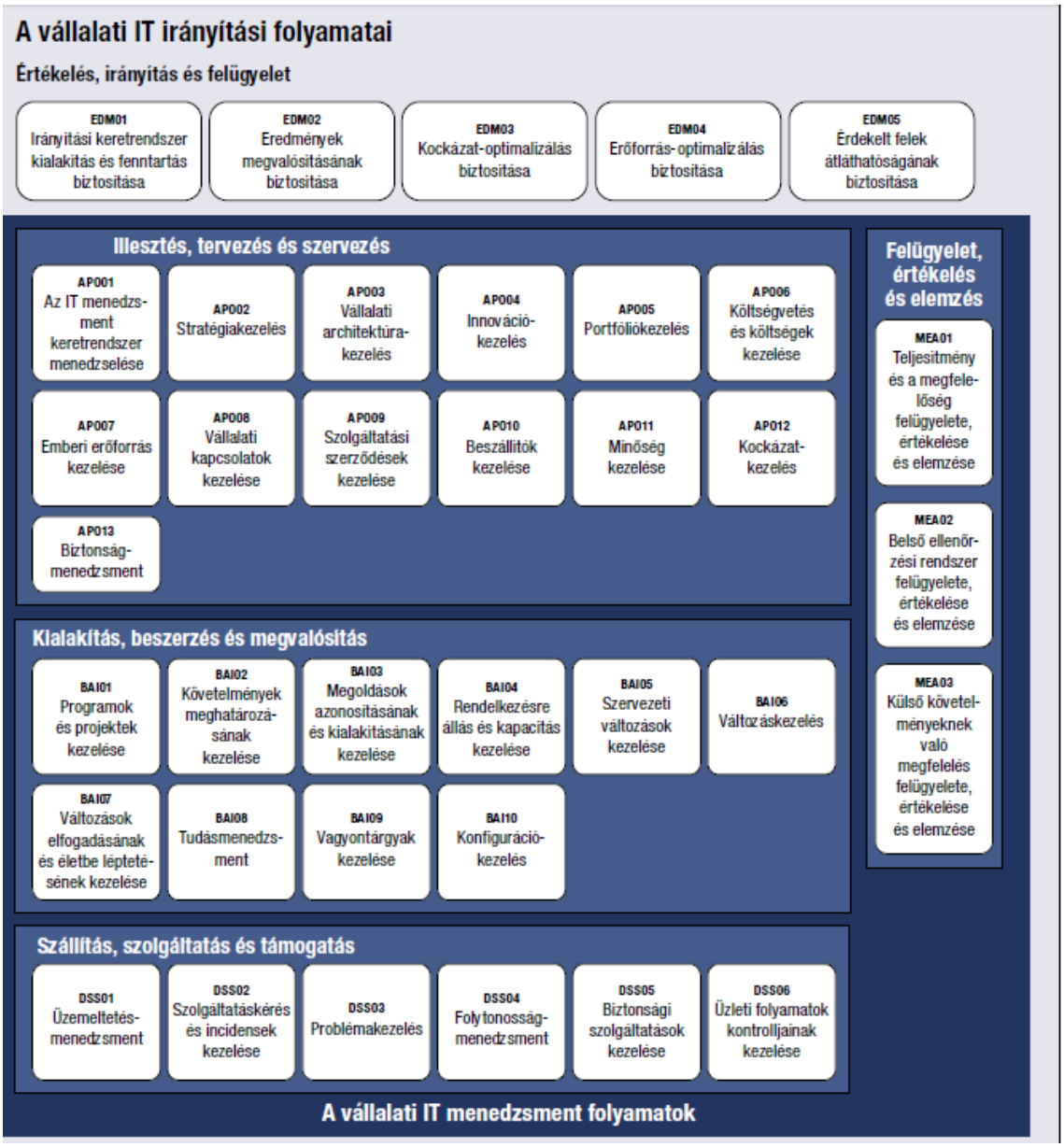
A COBIT 5 folyamatok jelölései:

APO (Align, Plan, Organization): illesztés, tervezés, szervezés.

EDM (Evaluate, Direct, Monitor): értékelés, irányítás és felügyelet.

DSS (Delivery, Service and Support) szállítás, szolgáltatás és támogatás.

A COBIT 5 segítségével az informatikai és üzleti terület folyamatai közelebb kerülnek egymáshoz, az erőforrások megfelelő használatán keresztül, valamint az irányítás és a menedzsment folyamatok megkülönböztetésével [169]. A COBIT 5 nem tér ki részletesen az informatikai alkalmazásokhoz rendelhető informatikai kockázatokra. A COBIT5 egy jó alapot ad a szervezeteknek az informatika folyamatok irányítására, értékelésére, felügyeletére. A COBIT5 mellett jól alkalmazható lenne, az irányelveket követve az informatikai alkalmazások részletes informatikai kockázati listájának az elkészítése. Az interjúkból kiderült, hogy Magyarországon lévő leányvállalatok használják a COBIT keretrendszert, de figyelembe kell venniük az anyavállalat előírásait is a kockázatok kezelésénél. A következő fejezetben az informatikai biztonság rövid elméleti ismertetése után, egy esettanulmányon keresztül mutatom be azokat a lépéseket, melyek szükségesek az informatikai kockázatok beépítéséhez az informatikai alkalmazás portfólióba.



13. ábra COBIT 5 Folyamat referenciamodell
Forrás: [169]

4.5 Összefoglalás

A negyedik fejezetben egy rövid áttekintést adtam a kockázatok definiálásáról és csoportosítási lehetőségekről. Elkülönítettem a szakirodalom alapján a vállalati kockázatmenedzsmentet és az informatikai kockázatmenedzsmentet. Ami nem informatikai kockázatmenedzsment, annak a megjelölésére az általános jelzőt használtam. Az általános kockázatmenedzsment beépül a nagyvállalati szervezeti

struktúrájába, azonban az üzleti területeken lévő folyamatokkal, tevékenységekkel párhuzamosan az informatikai osztályokon, egyes alterületeken pedig az informatikai kockázatoknak a kezelése történik. Az informatikai kockázatkezelés még gyerekcipőben jár. Nehezen körülhatárolható az informatikai kockázatok számbavétele, nyilvántartása, valamint az okozott kockázatoknak a számszerűsítése. Igaz, hogy létezik jó pár nemzetközi ajánlás, kidolgozás a kezelésre, menedzselésre, de azért ezeknek a napi szintű működésbe való beépítéshez sok tudásra, időre és pénzre van szükség. A kockázatok számszerűsítésére az üzleti területen különböző mérőszámot alkalmaznak, azonban az informatikai kockázatok pontos mérésére még nem elterjedtek a mérőszámok. Az ITIL nemzetközi ajánlást és a COBIT5 nemzetközi keretrendszer releváns részeit megvizsgálva, megállapítottam, hogy nem térnek ki részletesen az informatikai alkalmazások kockázati analitikájára.

5. BIZTONSÁGOS ALKALMAZÁS PORTFÓLIÓ

Az információ forrása az adat, amit védeni kell. Az adat értékes, egyedi, bizalmas. Az informatikai biztonságnak sok komponense, összetevője van. Számos kockázati tényező van, ami sértheti az adatokat. Lehet fizikai (rongálás, lopás), emberi mulasztás, illetve informatikai, technikai problémák, mint például hardver, szoftver meghibásodás. Az informatikai biztonság koncepciójának tartalmaznia kell azt, mit és mitől kell védeni, A veszélyforrásokat, kockázatokat fel kell tárni, elemezni és értékelni kell. Az alábbi fejezetben az informatikai biztonság rövid ismertetése után a biztonságos alkalmazás portfólió képzés lehetséges lépeseit mutatom be.

5.1 Az informatikai biztonság fogalma

A gazdasági szervezetekben a biztonságnak 4 összetevője van. A gazdasági biztonság, üzembiztonság, vagyonbiztonság és az informatikai biztonság. „Az informatikai biztonságon, olyan állapotot értünk, amikor a vállalat informatikai erőforrásai bizalmassága, sértetlensége és rendelkezésre állásának a fenyegetettsége minimális” [170].

A fennti kategóriák részletezve. **Bizalmasság** azt jelenti, hogy csak az arra jogosultak ismerhetik meg az információt. A **sértetlenség** alapján az információ az elvárt forrásból származik (hitelesség), igazolható, hogy megtörtént (letagadhatatlanság), egyértelműen azonosítható az információval kapcsolatos műveletek végzője (elszámoltathatóság). A **rendelkezésre állás** az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára egy meghatározott időben rendelkezésre állnak. A rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. A **zártság** jelentése, hogy az összes releváns veszélyt (fenyegetést) figyelembe kell venni, a **teljes körűség** pedig a rendszer minden elemére kiterjed a védelem. Ha időben folyamatosan megvalósul a védelem, akkor a folytonosság biztosított. A **kockázatokkal arányosság** jelentése, hogy a rendszer várható működésének időtartamában a védelem költsége arányban van a lehetséges kárral [171].

Az informatikai biztonságon belül lehet vizsgálni a fizikait, logikait és a szervezésit. A fizikai és logikai biztonságon belül kell figyelembe venni a rendelkezésre állással és a hozzáféréssel [170].

Az informatikai kockázatok kezelésénél jelenleg hazánkban a BCP és a DRP-n van a fókusz. Önmagában az Üzletmenet Folytonosság Menedzsment (Business Continuity Management, BCM), projektek sok költséggel és kockázattal járnak. Az IT kockázatmenedzsment területen megjelenik a veszélyforrások felmérése, kockázatok elemzése, becslése, lehetséges védelmi intézkedéseknek az előkészítése, kockázatoknak a kezelése. Az informatikai alkalmazásokra elvégzett informatikai kockázatelemzés a fenyegetések felmérését, sérülékenységek vizsgálatát foglalja magába. Az informatikai rendszerek működésfolytonosságának az objektív mérése lehetővé teszi a veszélyforrások felméréséből adódó kockázatok felmérését és lehetséges védekezési módszerek kidolgozását. Koncepcionális modell és mutatószámrendszer kialakítás jól megalapozza a működésfolytonosság összetevőinek a vizsgálatát, változásának kezelését [172]. A kockázatkezelési és az alkalmazás portfólió kapcsolatrendszer kérdéskörét vizsgálni lehet szervezeti, menedzsment, valamint operatív szinten. Az üzleti és informatikai folyamatok szervezésére, szabályrendszerek, vállalati kultúra eltérőek, szerteágazóak.

A SANS vállalat 2012. decemberében készült felmérése azt mutatja, hogy a vállalatoknál 23%-nak van kialakított és működőképes biztonsági programja az alkalmazások teljes életciklusára vonatkozóan. A felmérésben részt vevő vállalatoknak több, mint az egynegyede nem tudja pontosan az informatikai alkalmazásainak a számát. A felmérésből kiderül, hogy a biztonságos menedzselés, főleg az üzletkritikus alkalmazások nem menedzselhetőek. A megkérdezettek 23%-a alkalmaz és követ biztonsági előírásokat az informatikai alkalmazás életútjában. Azáltal, hogy a szervezet vezetése, érintett osztályok, felelősök nem tudják, mennyi és milyen informatikai alkalmazásokat használnak, menedzselnek, így a biztonsági előírások betartása, alkalmazása sem kivitelezhető. A biztonsági szabályokat be kell tartani egy szervezeten belül, valamint figyelmet kell fordítani az információs rendszerek biztonságának irányítására, szervezésére, koordinálására, a biztonsághoz kapcsolódó folyamatok tervezésére, fenntartására, kontrolálására vonatkozó előírásokat, ajánlásokat [173].

5.2 Az alkalmazás portfólió kockázatai

A Texas-i állami szervek egységére készült egy iránymutatás az informatikai alkalmazás portfólió képzésre 2018-ban. Több szempontrendszer alapján kell az alkalmazáshoz tartozó attríbutomokat leírni. Csoportosítást határoz meg az alkalmazás portfólióban. Általános információk az alkalmazásokról, architektúrális információk üzleti információk, pénzügyi információk, technikai információk. A technikai szekcióban kell részletezni a kockázatokat az informatikai alkalmazáshoz [174]. A 19. táblázat egy minta a dokumentációból. A táblázatban a biztonsági előírásokra vonatkozó kérdések vannak. Az alkalmazás portfólió kockázat kifejezést az iparági felméréseket tanulmányozva a TATA Consulting vállalat határozza meg, mint egy dimenzió az alkalmazás portfólió kezelésében [175]. 2011-ban készült egy rövid útmutatás, ajánlás, amely 5 dimenzióba sorolta a portfólió kockázatokat. Üzleti érték, technológiai kapcsolatok, alkalmazás portfólió kockázat, zöld „Footprint", költséghatékonyság. Az öt dimenzió közül az egyik alkalmazás portfólió kockázat. Alkalmazás portfólió kockázat meghatározása: Értékeli az üzleti kockázatok szintjét a kudarc valószínűsége, vagy a funkcionalitás romlása révén. Az üzleti tevékenységre gyakorolt hatás mértéke az alkalmazás, vagy a platform elavulása miatt.

1. **Operációs kockázat:** Figyelembe veszi az alkalmazás hatását az üzleti tevékenységre. Azokra az alkalmazásokra kell helyezni a hangsúlyt, melyek hozzájárulnak az üzleti bevétel, profit növeléséhez. Az alkalmazás portfólióra való figyelem csökkentheti a redundáns alkalmazások számát, ami csökkenteni fogja a kockázatokat.
2. **Kudarc kockázata:** Egy menedzselési folyamat kiépítése, segítené a vállalatokat abban, hogy merre és hogyan kell ellenőrizni a kudarcok kockázatának a számát. A lehetséges kockázatoknak a felismerése, kategorizálása, portfólióba való sorolása egy lépés.

Technikai kérdésszám	Indikátor	Kérdés elmagyarázása	Válaszlehetőségek
10	Biztonság	A TAC 202-re vonatkozó követelmények alapján várható, hogy az ügynökségek értékelik a szoftver- és hardverkörnyezetük biztonsági helyzetét. A felülvizsgálatok eredményeként az ügynökségeknek különböző biztonsági kockázatokat kellett volna azonosítaniuk a környezetük bármely rendszerében.	A szoftver biztonsági javításai már nem érhetők el a gyártótól, vagy nem alkalmazhatók a jelenlegi környezet kompatibilitási korlátai miatt.
			Szoftver nem támogatja a titkosítási szállítást.
			A korszerű hitelezési, engedélyezési és számviteli mechanizmusok hiánya.
			A biztonsági infrastruktúrán belül régi biztonsági protokollokat, vagy konfigurációkat kell használni; amely örökölt kockázatokat vezet be az új rendszerekre.
			A korlátozott teljesítmény miatt a Denial of Service (DoS) támadások könnyen befolyásolják a hardvert.
			A hardver nem tudja támogatni a szükséges modern, biztonságos szoftverrendszereket.

19. táblázat Alkalmazás portfólió: a biztonsági profilban szereplő kérdések
Forrás:Saját szerkesztés [174]

3. **Rendszer összetettség:** szükséges megfelelően összegyűjteni és megérteni a compliance, tehát a törvényi megfelelőségi kockázatokat, melyek az alkalmazásokkal kapcsolatosak. Minden biztonsági előírást és követelményt az alkalmazás életútján keresztül követni kell. A fejlesztésnél, karbantartásnál és az élesítés lépéseknél egyaránt.

4. **Alkalmazás támogatási kockázat**: Minden kockázat ide tartozik, amely bekövetkezhet, amikor egy alkalmazást fejlesztenek, vagy verziót váltanak. Tehát a személyi kockázatok, vagyis az emberi mulasztásból eredő kockázatok [179].

A kutatásom alapján javaslom, hogy a vállalatok hozzanak létre egy kockázati analitikát, ami beépíthető az alkalmazás portfólióba. A beépítés alatt azt értem, hogy hozzá rendelhető legyen az egyes alkalmazásokhoz az informatikai kockázati analitika. A kockázati elemzések készítésénél figyelembe kell venni az alkalmazások között meglévő és tervezett interfész kapcsolatokat, tehát az architektúrális kapcsolatrendszert. A szervezet működési profiljától függ, hogy mi szerepel az informatikai kockázati listán. A kiszervezett informatikai alkalmazásoknál több kockázati analitikára van szükség. Az alkalmazottak képesítése, képzettsége is egy kockázati faktor. A vállalatok mérete és az alkalmazottak biztonságtudatossága között van összefüggés. A nagyobb méretű vállalatoknál több oktatásra, tréningre van lehetőség, így a dolgozók is felkészültebbek a biztonsági szabályok betartására [176]. A folyamatos oktatással, képzéssel lehet csökkenteni az emberi mulasztásból eredő hibákat.

5.3 Esettanulmány

Az esettanulmányomban annál a nagyvállalatnál készítettem információ gyűjtést, ahol az akciókutatást végeztem. A felső vezetés igénye az volt, hogy az informatikai kockázatok definiáltak, mérhetőek és hozzárendelhetőek legyenek az informatikai alkalmazásokhoz. Az APM több éve jelen a nagyvállalatnál. Az informatikai kockázat mátrix kidolgozásához egy külsős céggel kötött szerződést a nagyvállalat. Az informatikai menedzsment terület és az informatikai alkalmazás portfólió menedzsment terület teljesen elkülönül a szervezetben, nincsenek átfedések a folyamatok között, illetve operatív szinten kommunikáció az alkalmazás tulajdonosok és az információbiztonsági szakemberek között. A projektben nem vettem részt, csak interjút készítettem az egyik szakemberrel. A projekt tervezési fázisában volt, és az összegyűjtött adatokat tudom

prezentálni a disszertációmban. Az előzetes egyeztetés alatt megosztott adatokat nem szerepeltethetem teljes körűen. A célja a kezdeményezésnek az volt, hogy lássa a szervezet a priorizált, fontosnak vélt informatikai kockázatokat alkalmazásonként. Az informatikai kockázatelemzés mellett az informatikai rendszer kockázatokkal arányos védelmének a meghatározása is feladat volt. Az informatikai kockázatok kategorizálásával párhuzamosan meghatározták a rendszerek informatikai biztonsági hiányosságait. Az alkalmazás portfólió nyilvántartási szoftverben lévő információk jó alapot biztosítottak volna a szervezetben, de ezt nem vették figyelembe a tervezés során. Az informatikai kockázatok definiálásánál bevonták az alkalmazásokat használó üzleti egységek vezetőit, felhasználóit is. A következő lépésben alkalmazásonként kellett egy kockázati besorolást meghatározni. A kockázatelemzéseknek a része volt a folyamatos kommunikáció az üzleti területek képviselőivel, tulajdonosaival. Az üzletileg kritikus folyamatok azonosítása meghatározó volt, mert ez befolyásolta, hogy milyen informatikai alkalmazások érintettek a felmérésben. A kockázati besorolás mögött létezik egy analitika, ahol láthatóak az összes informatikai kockázatok felsorolva, valamint a bekövetkezés valószínűsége és a hatása. Az egyes informatikai kockázatokhoz úgynevezett Threshold-okat, vagyis küszöbértékeket kell besorolni. Az aktuális érték és a súly megadása után a mátrix kiszámolja, hogy milyen kockázatos az alkalmazás. Az esettanulmány készítésekor azt állapítottam meg, hogy az alkalmazást támogató informatikai szakembereknek van a legnagyobb tudása és szerepe a nyilvántartás készítésénél. A biztonsági szakemberek feladata, hogy az informatikai biztonságot fenyegető tényezőket feltárják. A meglévő, vagy bevezetés alatt lévő szabályzatok, utasítások adják a támpontot. Minden technológiai kockázatot figyelembe kell venni. A 20. táblázatban szerepel a hozzáférési profilhoz tartozó kérdések. Az értékek a profil kalkulációt szemléltetik. Az aktuális érték meghatározása többszöri ellenőrzés és egyeztetések után került bele az adattáblába. A súlyok meghatározására az üzleti és informatikai területek egyetértésére volt szükség. A pontok értéke egy automatikus kalkuláció eredménye, illetve a külső beszállító cég adta a kalkulációs logikát, beágyazott függvényekkel Excel adattáblában. A pontok, súlyok meghatározásához az üzleti területek jóváhagyására volt szükség. Teljes körűen nem írhatom le a számolási logikát, ami a pontok, illetve a súlyozott eredményekre vonatkozik. A pontok 0-3-as skálán vannak meghatározva. Soronként a súlyozott érték kalkuláció alapja a súly és a pont értéke. A példa alapján a 40% szorozva 2-vel, osztva 100-al egyenlő 0,8. A súlyozott eredmények a tábla jobb felső részében található. A mintában az érték 0,78. Az érték az

utolsó oszlopban lévő súlyozott értékeknek az összege, osztva 2-vel. Ez minden kockázati profilnál ugyanaz. Az adatok nem tükrözik a valóságos adatokat. A táblában szereplő informatikai kockázati besorolások a legfontosabbak. A 21. táblázatban DRP olvashatóságára vonatkozik. Az első sorban a naprakész és jóváhagyott üzletfolytonosság nélküli szervezeti egységek száma szerepel. Ez azt jelenti, hogy számszerűsíteni kell, hogy az alkalmazásokhoz tartozó DRP-k melyik üzleti egységekben nincsenek elkészítve. A következő méréshez korábbi adatokat és tesztelési eredményeket kell figyelembe venni. Kritikus, stratégiai besorolású informatikai alkalmazásoknál fontos a határértékek pontos meghatározása. A külső beszállító egy informatikai kockázati profilként szerepel, a 23. táblázat mutatja az informatikai kockázatokhoz tartozó kérdéseket. A kiszervezés, outsourcing során az informatikai tevékenységek egy részének vagy egészének szerződésben foglaltak alapján történő átadását jelenti. Veszélyforrásnak tekinthető, ha a vállalat adataihoz hozzáfér egy külső cég. A belső vállalati adatokhoz hozzáférést kell biztosítani a vendoroknak, de emellett a rendszeres ellenőrzésük is részét kell képeznie az informatikai kockázat kezelésnek. A nagyvállalatnál az alkalmazás tulajdonosok töltötték ki a táblázat értékeit, nekik volt elegendő információjuk a beszállító tevékenységéről. A 24. táblázat a szemlélteti a munkaerő képzettségét, felkészültségét. Informatikai kockázati elemként jelenik egy informatikai alkalmazáshoz tartozó incidensek száma, amit a felhasználók okoztak. Ehhez az információhoz egy társosztály tudott adatot biztosítani. Az incidenskezelésen lévő informatikai szoftverből lehúzott riportból lehetett kinyerni az értéket.

A szükséges dokumentációk listája, tartalmára vonatkozó követelmények szervezeti sajátosság. Ha az adott alkalmazás pénzügyi üzleti funkciókat, például tranzakciókat támogat, akkor valószínűsíthető, hogy a külső ellenőrzések, auditok száma nagyobb lesz az alkalmazáson, összehasonlítva egy olyan alkalmazással, amiben nincsenek pénzügyi információk. Ezért a dokumentáció minősége, mint informatikai kockázati profil, magas besorolást, súlyértéket fog kapni az adott alkalmazásra. A következő lépés az aggregálás a besorolás alapján. Adott alkalmazáshoz elkészíthető sok és különböző informatikai kockázati mátrix. Informatikai alkalmazásonként, rendszerenként. A mátrixok eredményéből számolódik ki egy végső kockázati besorolás, amit majd az alkalmazás portfólióba, mint attríbutum szerepeltetni kell.

Adat hozzáférési ellenőrzés						Súlyozott eredmény		0,78
					Határérték			
Almérés	Aktuális érték	Szín	Súly	A mérés egysége	Sárga	Zöld	Pontok	Súlyozott értéke
Átlagos napok száma a hozzáférési jogosultságok ellenőrzése között.	20	G	40%	napok	180	90	2,00	0,80
Hozzáférési jogok ellenőrzése alapján a felhasználókhoz rendelt belépési felhasználói accountok száma.	22	Y	20%	#	30	10	1,40	0,28
Azoknak a felhasználóknak a száma, akik külső tevékenységből adódóan van joguk az alkalmazáshoz	900	Y	20%	#	1100	800	1,67	0,33
Átlagos napok száma egy hozzáférés törléséhez.	3	R	20%	napok	2	0	0,75	0,15

20. táblázat Adathozzáférési kockázati profil
Forrás: Saját szerkesztés

Katasztrófa elhárítás helyzetkép						Súlyozott eredmény		0,75
					Határérték			
Almérés	Aktuális érték	Szín	Súly	A mérés egysége	Sárga	Zöld	Pontok	Súlyozott értéke
Naprakész és jóváhagyott üzletfolytonosság nélküli szervezeti egységek száma.	3	G	60%	#	7	4	2,00	1,20
Átlagos idő az elérhetőség helyreállításhoz az információbiztonsági incidens után.	6	R	40%	óra	4	1	0,75	0,30

21. táblázat Katasztrófaelhárítási helyzetkép kockázati profi
Forrás: Saját szerkesztés

Külső beszállítóval kapcsolatos helyzetkép						Súlyozott eredmény		0,72
					Határérték			
Almérés	Aktuális érték	Szín	Súly	A mérés egysége	Sárga	Zöld	Pontok	Súlyozott értéke
Felhasználók száma, akiknek nincs megerősítve a hozzáférési jogosultság.	80	G	10%	#	500	100	2,00	0,20
Külső beszállítók száma, ahol a hozzáférési jogosultság nem lett ellenőrizve a belső szabályzatokkal összhangban.	60	Y	20%	#	70	50	0,00	0,00
A beszállítók száma, akik hozzáférnek bizalmas adatokhoz és nem lettek auditálva az elmúlt egy évben.	6	G	20%	#	14	7	2,00	0,40
Szerződések száma, ami nem felel meg a törvényi előírásoknak.	6	R	10%	#	4	2	0,30	0,03
A kérdőívek száma, ami ellenőrzés alatt van.	3	G	20%	#	40	30	2,00	0,40
Külső kapcsolatok száma, amelyeken nincs biztonsági ellenőrzés.	0	G	20%	#	5	2	2,00	0,40

22. táblázat Külső beszállítói helyzetkép kockázati profil
Forrás: Saját szerkesztés

Biztonsági tudatosság						Súlyozott eredmény		0,75
					Határértékek			
Almérés	Aktuális érték	Szín	Súly	A mérés egysége	Sárga	Zöld	Pontok	Súlyozott értéke
A felhasználók száma, aki nem nézték át a biztonsági szabályzatot az elmúlt 6 hónapban.	30	Y	30%	#	40	2	1,26	0,38
Az incidensek száma, amit a felhasználók okoztak.	30	Y	10%	#	30	10	1,00	0,10
Felhasználók száma, aki nem végezték el a biztonsági szabályokat tartalmazó tréningeket.	8	Y	10%	#	10	5	1,40	0,14
Felhasználók száma, akik nem megfelelően alkamazták a biztonsági eszközöket (pl. E-mal titkosítás).	5	Y	50%	#	8	4	1,75	0,88

23. táblázat Biztonsági tudatosság kockázati profil
Forrás: Saját szerkesztés

5.4 Biztonságos alkalmazás portfólió menedzsment

A biztonságos alkalmazás portfólió alapjait az előző fejezetekben részleteztem. Célom, hogy a nagyvállalatok részére ajánlást tegyek egy integrált alkalmazás-informatikai kockázati analitika portfólióra. Az ajánlásomhoz hozzátartozik az is, hogy adott szinten a megfelelő szaktudással rendelkező szakemberek végezzék a kategóriák meghatározását, valamint a kockázatok hozzárendelését az alkalmazásokhoz. Ennek az integrált nyilvántartásnak a megléte az auditok előkészítését támogatja. A gyakorlati megvalósításhoz az implementálási és fejlesztési költségekkel kalkulálni kell.

Biztonságos alkalmazás portfólió: Olyan integrált és összehangolt eljárásoknak, folyamatoknak az összessége, mely figyelembe veszi az alkalmazás portfólió képzésnél és menedzselésnél a szervezetre, informatikai folyamatokra, informatikai alkalmazásokra vonatkozó informatikai kockázati és biztonsági előírásokat, szabványokat, szabályokat, ajánlásokat. Az informatikai alkalmazásokhoz készített informatikai kockázati analitika végső eredménye szerepel az alkalmazás portfólióban, mint az alkalmazás egyik attribútuma. Figyelembe kell venni az informatikai költségösszetevőket, biztonsági előírásokat, szabályokat az adott szervezetnél.

A biztonságos alkalmazás portfólió feltétele, hogy a vállalat beépíti a folyamataiba az alkalmazás portfólió képzést. A pénzügyi elszámolások, alkalmazás költségösszetevők részét képezik a portfóliónak. A második feltétel az informatikai kockázati profilok definiálása részletesen, kérdésekkel, határértékekkel, pontokkal, súlyértékekkel. A kalkulált informatikai kockázati értékeket alkalmazásonként kell meghatározni.

Biztonságos alkalmazás portfólió képzés fő lépései:

1. Alkalmazás portfólió létrehozása: lista készítés, portfólió logika meghatározása, informatikai költségek, attríbutumok kitöltése, pénzügyi adatok regisztrálása.

2. Kockázati profilok létrehozása alkalmazásokra lebontva: A szükséges informatikai kockázati profilok a kérdésekkel.

3. Pontok, értékek, küszöbértékek, súlyok meghatározása.

4. A szervezet informatikai szabályainak, keretrendszereinek figyelembevétele.

5. Kockázati besorolási eredmények alapján akciótervek kidolgozása.

6. Folyamatos monitorozása a létrehozott alkalmazás-kockázati portfólió mátrixnak, akciótervek kidolgozása a pirossal jelölt informatikai kockázati besorolásokhoz. A sárgával jelölt alkalmazásoknál pedig a fejlesztési lépések kidolgozása a feladat.

Az interjúk elemzéséből is kiderült, hogy informatikai kockázatkezelést nem alkalmazzák az informatikai alkalmazásokra a nagyvállalatok, de lenne igény rá. Az információkat egységesen, összevontan az informatikai alkalmazások szintjén kell tárolni. Az informatikai kockázatok beépítése az alkalmazás portfólió menedzsmentbe egy új megközelítést ad az informatikai biztonság területén. Ahhoz, hogy a szervezet biztonságos informatikai rendszert működtessen, ismernie kell az informatikai alkalmazásokat, az alkalmazások által támogatott üzleti folyamatokat, a bennük tárolt adatok fontosságát és azt, hogy mennyit költ az adott informatikai alkalmazásra. Az informatikai szabályozásnak illeszkednie kell a vállalat meglévő felépítésébe, folyamataiba. Ha nincs egy központi, átlátható és könnyen karbantartható nyilvántartás a szervezetben futó alkalmazásokról és azokhoz kapcsolódó folyamatokról, akkor hogyan lehet definiálni, elemezni és monitorozni a hozzájuk kapcsolódó kockázatokat?

A szervezetben kidolgozott és alkalmazott ajánlásoknak, szabványoknak segíteni kell a szervezet biztonságos működését. Az informatikai kockázatkezelés aktualitása egyre nagyobb, mivel a felhő alapú szolgáltatások kialakításánál átkerülnek az adatok és a folyamatok a felhőbe. Új technológiák alkalmazásával a szervezetek célja a digitális kockázatok csökkentése, valamint a kockázatmenedzsment területek megszilárdítása. Nemcsak a megfelelő szabvány alkalmazása a kihívás a cégek számára, hanem az is, hogyan történik az ajánlásoknak, szabványoknak a kialakítása a szervezeten belül. Az alkalmazás portfólió, mint fogalom megjelenik a szakirodalmakban, valamint az előző fejezetekben részletesen leírt informatikai biztonsággal, kockázatkezeléssel, menedzsmenttel kapcsolatos definíciók is mutatják azt, mennyire fontos az informatikai biztonság. Azonban a két terület közötti kapcsolatrendszer fontossága nincs kiemelve. Igazoltam az alkalmazás portfólió menedzsment és az informatikai kockázatmenedzsment lehetséges integrációjának a keretét. A keretnek a feltétele az,

hogy a nagyvállalatoknak legyen kialakított működőképes kockázatmenedzselési keretrendszere. Az eredmény egy olyan alkalmazás portfólió mátrix, ami alkalmazás szinten mutatja a kockázati besorolások eredményét, az informatikai alkalmazás összköltségét és a compliance megfelelőség eredményét is. A három fő tényezőnek az összevetésével láthatóvá válik a menedzsmentnek, hogy hol vannak hiányosságok, mire kell figyelni. Az erőforrás-pénz allokációs döntésekhez ad információt, auditok előkészítéséhez is használható a mátrix. A 24. táblázat egy olyan mátrix, nyilvántartás, ami tartalmazza az informatikai alkalmazásra fordított összköltséget, az aggregált informatikai kockázati besorolást és a compliance megfelelőség vizsgálata alapján az eredményt. Azt veszem alapul, hogy az esettanulmányban lévő informatikai kockázati profilok együttes értékelése mit mutat. Az aggregált informatikai kockázati profil egy összesített érték és színjelölés az esettanulmányban feltüntetett informatikai kockázati analitika alapján. A vállalatoknak meg kell határozni, hogy az egyes színkategóriák milyen logika alapján keletkezzenek. Az informatikai kockázati profilok, a benne szereplő kérdések, határértékek, pontok, súlyok meghatározására van szükség az üzleti és informatikai szakértőknek közösen. Az első alkalmazás (A1) a portfólióban alacsony költséget képvisel, viszont technológiai szempontból magas kockázattal bír. A dokumentációk hiányosak, ezért van pirossal jelölve a törvényi megfelelőségi oszlop. Ez egy olyan informatikai alkalmazás, amire az informatikai szakemberek nagyobb figyelmet fordítanak. A hátterében az eredménynek lehet az, hogy egy elavult alkalmazás, de interfészei vannak stratégiai alkalmazásokkal. A második alkalmazásnak (A2) magasabb az összköltsége, ezért az üzlet nagyobb figyelemmel fogja kísérni az alkalmazásnak az informatikai költségösszetevőjét. Ezzel szemben az aggregált informatikai kockázati értéke alacsony. A compliance követelményeknek nem felel meg teljesen. Ezzel az alkalmazással az üzleti területek fognak többet foglalkozni, hiszen sokat költenek rá és a dokumentációk minősége sem kielégítő. A harmadik alkalmazás (A3) a portfólióban, amelyiknek magas nemcsak a költsége, de az informatikai kockázati értéke is. Tehát az informatikai kockázati profilok összesítése alapján sok fejlesztendő terület van, amivel foglalkoznia kell a szakértőknek. A biztonságos alkalmazás portfólió egyértelműen mutatja az alkalmazásokra költött összköltséget, informatikai kockázati értéket és azt, hogy a nemzetközi, vagy vállalati szabályzatok által előírt dokumentációk milyen állapotvan vannak. A mátrix egy szemléltető eszköz, könnyen olvasható. Az egyes értékek mögött analitikának kell lenni. Az éves összköltség vizsgálatánál a költség összetevők fontosak. Az informatikai kockázati értéknél pedig az, hogy melyik

informatikai kockázati helyzetképpel van probléma. A Compliance szempontok mögött pedig az esettanulmányban leírt application-compliance részletező mátrix mutat analitikus eredményt. A célom egy könnyen olvasható, kezelhető portfólió létrehozása volt. A menedzsment a nagyvállalatoknál az átláthatóságra törekszik az adatok értelmezésénél. A számok és színek mögötti analitikus nyilvántartás meglétére helyezem a hangsúlyt.

Alkalmazás neve	Alkalmazás azonosító	Alkalmazás éves összköltsége	Informatikai kockázati érték	Törvényi megfelelőségi érték
A1	ID_1	$100.000	alacsony	magas
A2	ID_2	$4.000.000	alacsony	alacsony
A3	ID_3	$8.000.000	magas	magas
A4	ID_4	$6.000.000	közepes	alacsony

24. táblázat Biztonságos alkalmazás portfólió
Forrás: saját szerkesztés

5.5 Összefoglalás

Ebben a fejezetben az informatikai biztonság definiálása után az alkalmazás portfólió kockázatokat összegeztem. Esettanulmányban részleteztem, hogyan épül fel az informatikai kockázati analitika egy multinacionális nagyvállalatnál. Az informatikai kockázatokra különböző profilokat lehet létrehozni. Az egyes profilokban szereplő kérdések összeállításához az üzleti és informatikai szakértők összehangolt munkájára van szükség. A kérdéseknél figyelembe kell venni az üzleti egységeknek fontos szempontrendszert és az informatikai szakértők véleményét. A javaslatom egy biztonságos alkalmazás portfólió. A mátrixban szerepel alkalmazásonként az összköltség, összesített informatikai kockázati érték és a törvényi megfelelőség helyzetképe. A szervezetben az auditálás előkészítéséhez, kockázatok felismerésére és mérséklésére ajánlom a mátrix használatát. A nagyvállalatok biztonsága szempontjából fontos, hogy feltárják az informatikai alkalmazásokhoz tartozó kockázatokat, így a nem kívánt események bekövetkezésének a valószínűsége csökkenthető. Az informatikai költségek és az informatikai kockázatok együttes vizsgálata egy új megközelítés a nagyvállalati körben.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Új tudományos eredmények

1. Tézis: A nagyvállalatokban az informatikai alkalmazások portfóliójának kialakítására szükség van.

A szakirodalmak feldolgozása, akciókutatás és a mélyinterjú vélemények összegzése alapján az alábbi megállapításokat teszem. A legtöbb nagyvállalatnál létezik informatikai alkalmazás nyilvántartás valamilyen formában. A nyilvántartást informatika rendszerekben, vagy Excelekben oldják meg. Az alkalmazás nyilvántartásokban az informatikai alkalmazásokhoz nincsenek hozzárendelve az üzleti folyamatok. A szolgáltatásalapú megközelítés, amit az ITIL képvisel, jó alapokat biztosít az alkalmazások nyilvántartására. Azokban a szervezetekben ahol valamennyire figyelembe veszik az ITIL ajánlást, nincs összefüggés az alkalmazás nyilvántartások és az ITIL-ben szereplő alkalmazás portfólió képzésre vonatkozó ajánlás között. Az ITIL tesz utalást az informatikai alkalmazás portfólió képzésre. Szükség lenne a nagyvállalatoknak egy útmutatásra az informatikai alkalmazás portfólió pontos lépéseinek a meghatározására, és az elérhető előnyök ismertetésére. Egyértelmű eredmény a kutatás alapján, hogy nagyvállalati körben van igény az informatikai alkalmazások portfólióba sorolására [177], [178], [180].

2. Tézis: A nagyvállalatokban az informatikai alkalmazások költségkezelése beépítendő az alkalmazás portfólióba.

A nagyvállalatoknál az informatikai költségek kezelése nem követ elfogadott keretrendszert. ITIL ajánlásban szereplő pénzügyi megközelítést kevés szervezet alkalmazza. A mindennapi működésnél, informatikai kiszervezések során igény van az informatikai költségek hozzárendelésére az alkalmazásokhoz. Az informatikai alkalmazás portfólió képzés beépítésével párhuzamosan az informatikai költségek analitikus nyilvántartását is létre kell hozni [179], [183].

3.Tézis: Az informatikai kockázatok nyilvántartási rendszere elengedhetetlen feltétele a biztonságos alkalmazás portfólió menedzsmentnek.

A biztonságos alkalmazás portfólió része az informatikai alkalmazások portfólióba sorolása. Az informatikai költséganalitika és az informatikai kockázati analitika mérés eredményeinek a beépítése a portfólióba. A nagyvállalatnál végzett esettanulmány igazolja, hogy az informatikai kockázati profilok létrehozhatóak alkalmazás szinten [177], [179], [181].

Ajánlások

1. Javaslom az általam megfogalmazott tudományos eredményeket a nagyvállalati környezet üzleti és informatikai egységek vezetőinek az informatikai szolgáltatás minőségének a javítása, valamint az üzleti terület elégedettség növelése érdekében.

2. Javaslom azoknál a szervezeteknél, ahol az ITIL már valamilyen szinten jelen van és alkalmazzák, hogy egészítsék ki az informatikai folyamataikat informatikai alkalmazás portfólió menedzsmenttel, hozzá tartozó informatikai költséganalitikával. Az alkalmazás portfólió menedzsment használatával párhuzamosan fordítsanak több erőforrást és időt az informatikai alkalmazásokhoz kapcsolódó különböző informatikai költségek nyilvántartására, elemzésére, riportálására.

3. Javaslom, hogy a nagyvállalatok tegyenek előrelépéseket annak érdekében, hogy az alkalmazás portfólió menedzsment és az informatikai kockázatmenedzsment területek közötti kommunikáció, együttműködés kialakuljon.

További kutatási elképzelések

- A szervezeti sajátosságok, például a szervezeti felépítés, szervezeti kultúra, struktúra, vezetői támogatás hatása az alkalmazás portfólió menedzsmentre.
- Az üzleti és informatikai folyamatok összetettségének és dokumentáltságának hatása az informatikai folyamatokra, üzemeltetés mindennapi működésére.
- Az alkalmazások informatikai költségének kapcsolati rendszere a többi informatikai költséggel.

IRODALOMJEGYZÉK

[1] BABBIE, E.: A társadalomtudományi kutatás gyakorlata, Balassi Kiadó 1996. ISBN: 963-506-563-9

[2] SCHLEICHER, N.: Kvalitatív kutatási módszerek a társadalomtudományokban. BKF jegyzet. Századvég, Budapest. 2007. ISBN:9637340536

[3] HORVÁTH, D., ARIEL M.: Alternatív kvalitatív kutatási kézikönyv, Alinea kiadó, ISBN:978-615-5303-82-1, 2015.

[4] KURT, L.: Action Research and Minority Problems, 1946. http://www.cscd.osakau.ac.jp/user/rosaldo/K_Lewin_Action_research_minority_1946.pdf (letöltve: 2019.01.12.)

[5] WEST, D., STANSFIELD M.H.: Structuring Action and Reflection in Information Systems Action Research Studies Using Checkland´s FMA Model, Systemic Practice and Action Research, Volume 14. Issue 3. 2001. pp. 251-281. DOI:10.1023/A:1011355214452 (letöltve: 2019.01.12.)

[6] BASKERVILLE, R.L.,WOOD-HARPER A.T.: A Critical Perspective on Action Research as a Method for Information Systems Research, Journal of Information Technology Volume 11, 1996., pp. 235-246. DOI:10.1177/026839629601100305 (letöltve: 2019.02.01.)

[7] MANSELL, G.: Action research in information systems development, Journal of Information Systems Volume 1, Issue 1., 1991., pp. 29-40. DOI:10.1111/j.1362575.1991.tb00025.x (letöltve: 2019.02.01.)

[8] MUMFORD, E., HIRSCHHEIM R., FITZEGERALD G., WOOD-HARPER, T.A.: Research Methods in Information Systems, Amsterdam: North-Holland, 1985., pp. 169-191. ISBN: 0-444-87807-6 (letöltve: 2019.01.21.)

[9] BASKERVILLE, R.: Investigating Information Systems with Action Research. Communications of the Association for Information Systems, Volume 2, Issue 3., 1999. DOI: 10.17705/1CAIS.00219 (letöltve: 2019.01.21.)

[10] LAU, F.: A Review on the Use of Action Research in Information Systems Studies. Information Systems and Qualitative Research. IFIP:The International Federation for Information Processing. Springer, Boston, 1997. ISBN: 978-1-4757-5487-2 DOI:10.1007/978-0-387-35309-8_4 (letöltve: 2019.01.21.)

[11] PAUL, C., DAVID C.: Action research for operation management, International Journal of Operations and Production Management Volume 22, Issue 2, 2002., pp. 220-240. DOI:10.1108/01443570210417515 (letöltve: 2019.03.01.)

[12] BRONTE, V.D. H: Discussing project status with the project-space model: An action research study, International Journal of Project Management, Volume 34, Issue 8., 2016., pp. 1638-1657. DOI:10.1016/j.ijproman.2016.09.001 (letöltve: 2019.03.01.)

[13] SILVIA, MAYUMI T.M.: Competency mapping in project management: An action research study in an engineering company, International Journal of Project Management, volume 33, Issue 4., 2015., pp. 784-796. DOI:10.1016/j.ijproman.2014.10.013 (letöltve: 2019.02.11.)

[14] JOHN, W. C.: Educational Research, Planning, conducting and evaluating quantitive and qualitive research, 2015. ISBN-13: 978-0-13-136739-5 http://basu.nahad.ir/uploads/creswell.pdf (letöltve: 2019.01.25.)

[15] MILLS, G. E.: Action research: A guide for the teacher researcher 4th Edition. Upper Saddle River, NJ: Pearson. 2011. ISBN-13: 978-0137003143

[16] MARROW, A. J.: The practical theorist the life and work of Kurt Lewin. New York: Basic Books, 1969. pp.198-199. https://psychological.files.wordpress.com/2015/12/kurt-lewin-practical-theorist.pdf (letöltve: 2019.01.14.)

[17] EDLY, F. RAMLY, MOHD S. O.: Development of Risk Management Framework. Case Studies, Proceedings of the International Conference on Industrial Engineering and Operations Management Paris, France, 2018. http://www.ieomsociety.org/paris2018/papers/481.pdf (letöltve: 2018.11.14.)

[18] KHALFAN, A. M.: Information Security Considerations in IS/IT Outsourcing Projects: A Descriptive Case Study of Ttwo Sectors, International Journal of Information Management Volume 24, Issue 1., 2004., pp. 29–42. DOI: 10.1016/j.ijinfomgt.2003.12.001 (letöltve: 2018.11.14.)

[19] AUBERT, B., PATRY M., RIVARD S., SMITH H.: IT Outsourcing Risk Management at British Petroleum, Proceedings of the 34th Hawaii International Conference on System Sciences,Volume 8. pp.8076., CA: IEEE Computer Society Press., ISBN:0-7695-0981-9 (letöltve: 2018.10.14.)

[20] ARKIN, B.: Software Security Analysis: an Example Case Study. In: Ghosh A.K. E-Commerce Security and Privacy. Advances in Information Security, Volume 2, 2001. Springer, Boston, ISBN:978-1-4613-5568-7 DOI:10.1007/978-1-4615-1467-1_2 (letöltve: 2018.10.14.)

[21] CHEN, M., WANG SC: The Business Data Integrity Risk Management Model: A Benchmark Data Center Case of IT Service Firm. In: Chou SY., Trappey A., Pokojski J., Smith S. (eds) Global Perspective for Competitive Enterprise, Economy and Ecology. Advanced Concurrent Engineering. 2009. Springer, London, 978-1-84882-761-5 DOI:10.1007/978-1-84882-762-2_67 (letöltve: 2018.11.14.)

[22] SARIF, S, RAHMAN N.A., YUNUS Y.M.: Strategic Information System Planning (SISP) Success: A Case Study. In: Lokman A., Yamanaka T., Lévy P., Chen K., Koyama S. (eds) Proceedings of the 7th International Conference on Kansei Engineering and Emotion Research Advances in Intelligent Systems and Computing, Volume 739. 2018. Springer, Singapore DOI:10.1007/978-981-10-8612-0_72 (letöltve: 2019.03.04.)

[23] MONTENEGRO, C., NUNEZ N: Integrated IT Governance and Management Model: Evaluation in a Developing Country. In: Mejia J.,

Muñoz M., Rocha Á., Quiñonez Y., Calvo-Manzano J. (eds) Trends and Applications in Software Engineering. CIMPS 2017. Advances in Intelligent Systems and Computing, Volume 688. Springer. DOI:10.1007/978-3-319-69341-5_7 (letöltve: 2019.03.04.)

[24] CATER-STEEL, A., TOLEMAN M, TAN W-G: Transforming IT service management- The ITIL impact. Paper presented at the 17th Australasian Conference on Information Systems. ACIS, 2006. Adelaide, pp. 6–8. https://eprints.usq.edu.au/1612/1/Cater-Steel_Toleman_Tan.pdf (letöltve: 2019.03.04.)

[25] TAN W-G, CATER-STEEL A., TOLEMAN M: Implementing it service management: A case study focussing on criticalsuccess factors. Journal Computer Information System, Volume 50, Issue 2. 2009., pp.1–12. (letöltve: 2019.02.24.)

[26] MASAFUMI, K., JUNICHI I.: IT applications portfolio management under business and implementation uncertainty, Journal of Systems Science and Systems Engineering, Volume 17, Issue 1. 2008., pp 109–124, ISSN: 1004-3756, DOI: 10.1007/s11518-008-5066-x (letöltve: 2019.02.24.)

[27] JANNIS B, ALEATRATI K, JANNIS B., FLORIAN M., ROBERT W.: Causes and Consequences of Application Portfolio Complexity – An Exploratory Study IFIP International Federation for Information Processing, Published by Springer International Publishing Switzerland 2016., pp. 11–25, DOI: 10.1007/978-3-319-48393-1 2 (letöltve: 2019.01.24.)

[28] BARNEY, G.G., ANSELM L.S.: The Discovery of Grounded Theory, Aldine ISBN: 780202302607

[29] DEREK, L: Grounded Theory: A constructive critique. Journal of the Theory of Social Behavior, Volume 12, Issue 1., 1982. pp. 103–122. DOI:10.1111/j.1468-5914.1982.tb00441.x (letöltve: 2019.05.04.)

[30] STRAUSS, A, CORBIN J.: Basics of qualitative research. 3rd ed. 2008., Sage Publications, Thousand Oaks, California, DOI:10.4135/9781452230153 (letöltve: 2019.05.02.)

[31] CHARMAZ, K.: Grounded theory: Objectivist and constructivist methods. In: Denzin N. K., Lincoln, Y.S. 2000., Handbook of qualitative research. Sage Publications, Thousand Oaks, California.

[32] THORNBERG, R.: Informed grounded theory, Scandinavian Journal of Educational Research, Volume 56, Issue 3, 2012., pp. 243–259. DOI: 10.1080/00313831.2011.581686 (letöltve: 2019.05.02.)

[33] MANUAL, W., MARLEN, C.J., PHILIP, W.Y, HELMUT K.: Grounded Theory Methodology in information system research, MIS QUARTERLY, Volume 41 Issue, 3, 2007.,pp. 685-701 https://misq.org/skin/frontend/default/misq/pdf/appendices/2017/V41I3Appendices/12382_MA_Wiesche.pdf (letöltve: 2019.05.02.)

[34] ALENA, Y.C., MICHAEL L. -DOUG J.T: Investigation of employee security behavior: A grounded theory approach, 30th IFIP International Information

Security Conference (SEC),2015, Hamburg, Germany. pp.283-296, DOI: DOI:10.1007/978-3-319-18467-8_19 (letöltve: 2019.04.02.)

[35] RABIAH, A.-ZAHRI Y.-SHARIN S.: Understanding cyber terrorism: The grounded theory applied, IEEE, ISBN 978-1-4673-1426-8, 2012. DOI: 10.1109/CyberSec.2012.6246081 (letöltve: 2018.05.02.)

[36] HAISSA, D.-GLEISON S.: Improvement of IT processes, Journal of Software Engineering Research and Development. Volume 2, Issue 4. 2014., DOI:10.1186/2195-1721-2-4 (letöltve: 2018.05.02.)

[37] AIDA, BENGT S., GERRY L.: Reflexive Serendipity. Grounded Theory and serendipity in disaster management and military research, Qualitative Sociology Review Volume 12, Issue 3. 2016. http://www.qualitativesociologyreview.org/ENG/Volume38/QSR_12_3_Alviniu s_Starrin_Larsson.pdf (letöltve: 2019.01.11.)

[38] JAMES, O. W. JR.: A grounded theory study of the risks and benefits associated with the use of online social networking applications in a military organization, Capella University, ProQuest Dissertations Publishing, 2012. https://search.proquest.com/docview/1009051043 (letöltve: 2019.01.15.)

[39] LISA B., NANCY H.: Being a Female Veteran: A Grounded Theory of Coping With Transitions. Social Work in Mental Health, 13:108–127, 2015, Published with license by Taylor & Francis, ISSN: 1533-2985 print/1533-2993, DOI: 10.1080/15332985.2013.870102, (letöltve: 2019.Május 02.)

[40] LORINZO, N: Journal of Psychological issues in Organizational Culture, volume 3, Issue 2. july 2012. pp. 30-58. A grounded theory study of training transfer among army noncommissioned officers, DOI:10.1002/jpoc.20101, (letöltve: 2019.02.24.)

[41] GLASER, BARNEY G.: ANSELM S.: The Discovery of Grounded Theory: Strategies for Qualitative Research. Chicago, IL: Aldine Publishing Co, 1967. (letöltve: 2019.02.24.)

[42] BOKOR A.,FERTETICS M., HIDEGH A.L. VÁRADI SZ. ZS.: Karrierváltók Magyarországon, Vezetéstudomány, 2009. 40 Évfolyam 11.szám, pp. 11-35. http://unipub.lib.uni-corvinus.hu/501/1/vt_201201p17.pdf (letöltve: 2019.02.24.)

[43] ESSE, B.: Adaptív döntéshozatal a beszállítóválasztás példáján, Vezetéstudomány,2013. Évfolyam:44, 11.szám pp. 34-42. http://unipub.lib.uni-corvinus.hu/1373/ (letöltve: 2019.02.20.)

[44] Application of Grounded Theory in Determining Required elements for Ipv6 risk assessment equation. MATEC, Web of conferences 150, 06005 2018 DOI:10.1051/matecconf/201815006005 MUCET 2017 (letöltve: 2019.02.21.)

[45] JAPHET, L., USMAN T.: The use of Grounded Theory Technique as a Practical Tool for Qualitative Data Collection and Analysis, Electronic Journal of Business Research Methods Volume 11 Issue 1 2013, pp. 29-40, ISSN 1477-7029 (letöltve: 2019.01.05.)

[46] HOSCHSTEIN, A, BRENNER W.: Implementation of service-oriented IT management: An empirical study on Swiss IT organizations. Paper presented at International Conference on Service Systems and Service Management. ICSSSM, Troyes, pp. 91–97. 2006. (letöltve: 2019.01.07.)

[47] COLEMAN, G, O'CONNOR R.: Investigating software process in practice: A grounded theory perspective. Journal System Software 2008. 81. pp.772–784

[48] ITIL: Diirr and Santos Journal of Software Engineering Research and Development 2014, Volume 2, Issue 4, http://www.jserd.com/content/2/1/4, Improvement of IT service processes: a study of critical success factors (letöltve: 2019.01.07.)

[49] POLLARD, C., CATER-STEEL A: Justifications, strategies, and critical success factors in successful ITIL implementations in U.S. and Australian companies: An exploratory study. Information System Management Volume 26 Issue 2. 2009. pp.164–175 DOI:10.1080/10580530902797540 (letöltve: 2019.01.07.)

[50] MANAL, A.A.F.: Grounded theory and action research as pillars for interpretive information systems research: A comparative study, Egyptian Informatics Journal, Volume 16, Issue 3, 2015, pp. 309-327 DOI:10.1016/j.eij.2015.07.002 (letöltve: 2019.01.04.)

[51] MARKOWITZ, H.: Portfolio Selection: The Journal of Finance, Volume 7, Issue 1. Március 1952, pp. 77-91 http://links.jstor.org/sici?sici=0022-1082%28195203%297%3A1%3C77%3APS%3E2.0.CO%3B2-1 (letöltve: 2019.01.15.)

[52] MCFARLAN, F. W.: Portfolio Approach to Information Systems, Harward Business Review, 1981., 59, 5 pp. 142-150. https://hbr.org/1981/09/portfolio-approach-to-information-systems (letöltve: 2016.05.01.)

[53] WARD, J. M.: Information System and technology application portfolio management-an assessment of matrix-based analysis. Journal of Information Technology Volume 3, Issue 3, 1987. pp. 205–215. https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/493/SWP3688.pdf?sequence=2&isAllowed=y (letöltve: 2017.10.01.)

[54] KWAN, S. K., WEST J.: Heterogeneity of IT Importance: Implications for Enterprise IT Portfolio Management, Proceedings of the 64th Annual Academy of Management Conference. 2004. http://joelwest.org/Papers/KwanWest2006.pdf (letöltve: 2018.10.01.)

[55] MAIZLISH, B., HANDLER, R: IT portfolio management step-by-step. John Wiley & Sons, Inc., New Jersey. 2005. http://www.epiheirimatikotita.gr/elibrary/management/John.Wiley.and.Sons.IT.Portfolio.Management.Step-by-Step.pdf (letöltve: 2018.10.01.)

[56] JOEY, V. A., VINCENT B., RONALD B.: Application Portfolio Management in Hospitals:, International Journal Of Healthcare Information Systems And Informatics, 2014. Volume 9, Issue 1. pp.61-74. DOI:10.4018/ijhisi.2014010104 (letöltve: 2018.10.01.)

[57] AJER, ANNE K. S, OLSEN, D. H.: Enterprise Architecture Challenges: A cases tudy of three public sectors. Twenty-Sixth European Conference on Information Systems Portsmouth, UK, June 2018, ISBN:9781861376671 http://ecis2018.eu/wp-content/uploads/2018/09/1336-doc.pdf (letöltve: 2018.11.01.)

[58] MUHA, L.: Fogalmak és definíciók, In.: Az informatikai biztonság kézikönyve Budapest: Verlag Dashöfer Szakkiadó, ISBN9639313122 2004.

[59] ITIL szakkifejezések és röviditések magyarul, ITIL Glossary of Terms english-Hungarian v.1.0, Axelos Limited 2012. https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_-HU-v1-0.pdf, (letöltve: 2017.09 12.)

[60] ISACA magyar szakkifejezés gyűjtemény, ISACA Magyarországi Egyesület, ISBN: 978-963-08-6769-6 2013. https://m.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Hungarian_1213.pdf (letöltve: 2018. 03. 30.)

[61] GARTNER IT Glossary, https://www.gartner.com/it-glossary/enterprise-applications (letöltve: 2018. 03. 30.)

[62] ITIL szakkifejezések és röviditések magyarul, ITIL Glossary of Terms english-Hungarian v.1.0, Axelos Limited 2012. https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_-HU-v1-0.pdf, (letöltve: 2017.09 12.)

[63] ISO/IEC: Information Technology, Systems and Software Engineering-Application Management, ISO/IEC: 16350: 2015 https://www.iso.org/obp/ui/#iso:std:57922:en, (letöltve: 2018. 04. 01.)

[64] DANIEL, S. KAI F., DETLEF S.: Application portfolio management, an integrated framework and a software tool evaluation approach. Communications of the Association for Information Systems, Volume 26, Issue 3, 2010. DOI: 10.17705/1CAIS.02603 (letöltve: 2019.02 12.)

[65] IBM Smarter Computing with Application Portfolio Management, 2012. ftp://public.dhe.ibm.com/software/uk/pdf/Ovum_-_Smarter_Computing_with_APM_-_FINAL.pdf (letöltve: 2018. 03. 30.)

[66] WARD, J.M.: Information System and technology application portfolio management-an assessment of matrix-based analysis, Journal of Information Technology Volume 3, Issue 3, 1987., pp. 205–215 https://dspace.lib.cranfield.ac.uk/bitstream/handle/1826/493/SWP3688.pdf?sequence=2&isAllowed=y (letöltve: 2017.10.01.)

[67] WARD J.- PEPPARD J.: Strategic Planning for Information systems, John Willey & Sons Ltd.. 2002. (letöltve: 2019.02 12.)

[68] KERSTEN B., C. VERHOEF: IT Portfolio Management: A Banker‘s Perspective on IT, Cutter IT Journal, 2003. Volume 16, Issue 4, pp. 27–33. https://www.cs.vu.nl/~x/bp/bp.pdf, (letöltve: 2018.10.01.)

[69] IBM Redbooks: Total Solution for System z, IBM Forum Amsterdam, 2002. ftp://www.redbooks.ibm.com/redbooks/2012_ITSO_Total_Solution_Event_System_z_Amsterdam/track_2_zEnterprise_for_IT_Architects/AR05_Application_Portfolio_Management.pdf (letöltve: 2018.04.02.)

[70] SOMMERVILLE, I: Software engineering, Ninth Edition, Addison-Wesley, ISBN:139780137035151, Pearson,2009 https://edisciplinas.usp.br/pluginfile.php/2150022/mod_resource/content/1/1429431793.203Software%20Engineering%20by%20Somerville.pdf (letöltve: 2018.04.02.)

[71] SIMON, D., FISCHBACK, K., SCHODER, D.: An Exploration of Enterprise Architecture Research. Communications of the Association for Information Systems, 2013. V olume 32, Issue 1. DOI: 10.17705/1CAIS.03201 (letöltve: 2019.01.02.)

[72] JAN, J.: An empirical analysis of the factors and measures of Enterprise Architecture Management success, Article in European Journal of Information Systems, 2015, DOI: 10.1057/ejis.2014.39 (letöltve: 2019.01.02.)

[73] GROOT, R., MARTIN S.: A Method to Redesign the IS Portfolios in Large Organisations, Proceedings of the 38th Hawaii International Conference on System Sciences 2005., Conference Paper, DOI: 10.1109/HICSS.2005.25 · (letöltve: 2019.01.02.)

[74] CARUSO, D.: Application portfolio management: a necessity for future IT. Manufacturing Business Technology, 2007. Volume 25, Issue 10, pp.48.

[75] JAMES D., McKEEN, HEATHER A. S.: Developments in Practice XXXIV: Application Portfolio Management, communications of the Association for Information System, Volume 26, Issue 9.2010 DOI: 10.17705/1CAIS.02609 (letöltve: 2019.01.02.)

[76] POUYA, A. K., JANNIS B., STEPHAN A.: What Drives Application Portfolio Complexity? An Empirical Analysis of Application Portfolio Cost Drivers at a Global Automotive Company, Electronic ISBN:978-1-5090-3231-0: 2016 IEEE 18th Conference on Business Informatics DOI:10.1109/CBI.2016.39 (letöltve: 2019.02.08.)

[77] BUSINESS Wire: i360Gov Releases IT Survey Report on application portfolio management in Federal Government, 2015. https://www.businesswire.com/news/home/20150713006342/en/i360Gov-Releases-Survey-Report-Application-Portfolio-Management (letöltve: 2018.05.02.)

[78] CENTRIX S.: The application portfolio landscape, The perception and the reality. A survey and analysis of the challenges of managing ned-user applications, 2014. http://www.centrixsoftware.com/sites/default/files/Vanson%20Bourne%20Centrix%20Software%20Application%20Usage%20Survey%20Summer%202014%20Final.pdf (letöltve: 2017.02.21.)

[79] MEGA: Turn Application Portfolio Management Into a governance tool for the CIO, 2012.

https://www.abilab.it/documents/10180/278010/01.%20MEGA%20White%20Paper%20-%20Application%20Portfolio%20Management.pdf (letöltve: 2017.05.01.)

[80] ORACLE: Benefits of Application Rationalization: Reduce Costs and Improve Services with a Systematic Approach 2009. http://www.oracle.com/us/products/applications/042763.pdf (letöltve:2017. január 21.)

[81] MATTHIAS, F., SJAAK B.: A method for application rationalization, Conference: Digital Information Management, 2007. ICDIM '07. 2nd International Conference on Volume 1, IEEE Xplore, DOI: 10.1109/ICDIM.2007.4444267 (letöltve:2019. január 21.)

[82] MOCKER, M.: What is Complex about 273 Applications? Untangling Application Architecture Complexity in a case of European Investment Banking. In: 42nd Hawaii International Conference on System Sciences 2009., IEEE, ISBN: 978-0-7695-3450-3 DOI:10.1109/HICSS.2009.506 (letöltve: 2017. 12 23.)

[83] SCHNEIDER A., RESCHENHOFER T., S.A., M.F..: Empirical Results for Application Landscape Complexity. In: 48th Hawaii International Conference on System Sciences, 2015., IEEE. DOI:10.1109/HICSS.2015.490 (letöltve: 2019. 05 01.)

[84] ITSM, IT Service Management: http://www.itsm.info/ITSM.htm (letöltve: 2018.03.25.)

[85] ITIL Service Strategy, 2011 London: TSO (The Stationary Office), ISBN 9780113313044

[86] ITIL Service Design, 2011 London: TSO (The Stationary Office), ISBN 9780113313051

[87] ITIL Service Transition, 2011 London: TSO (The Stationary Office) ISBN 9780113313068, (letöltve: 2018.03.23.)

[88] ITIL Service Operation, 2011 London: TSO (The Stationary Office) ISBN 9780113313075

[89] ITIL Continual Service Improvement, 2011 London: TSO (The Stationary Office) ISBN 9780113313082

[90] HOCHSTEIN, A. -TAMM G.-BRENNER W.: Service-oriented IT management: benefit, cost and success factors. 2005. In: Proceedings of the 13th European conference on information systems, Regensburg, DOI: 10.1007/s12599-010-0141-5 (letöltve: 2019.01.11.)

[91] POLLARD, C., CATER-STEEL A.: Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study", Information Systems Management,2009. Volume 26., Issue 2, pp. 164–175. ISSN 1058-0530, DOI: 10.1080/10580530902797540 (letöltve: 2019.01. 21.)

[92] MARRONE, M., KOLBE L.: ITIL: Providing More Than Just Operational Benefits: An Empirical Research, Multikonferenz Wirtschaftsinformatik 2010, Göttingen, Germany, pp. 281–292.

[93] IDEN, J., LANGELAND L.: Setting the Stage for a Successful ITIL Adoption: A Delphi Study of IT Experts in the Norwegian Armed Forces, Information Systems Management, 2010. Volume 27, Issue 2, pp. 103–112. DOI: 10.1080/10580531003708378 (letöltve: 2019.01. 21.)

[94] MAURICIO, M., LUTZ M. K.: Impact of IT Service Management Frameworks on the IT Organization, 2011 Business and Information Systems Engineering Volume 3, Issue 1, 5-18 DOI:10.1007/s12599-010-0141-5 (letöltve:2019. 01.25.)

[95] JON I., TOM Roar E.: Iden & Eikebrokk: Using the ITIL Process Reference Model for Realizing IT Governance: An Empirical Investigation, January 2014 Information Systems Management, Volume 31, Issue 1, pp.37-58. DOI: 10.1080/10580530.2014.854089 (letöltve:2019. 01.25.)

[96] MAURICIO, M, FRANCIS G.:IT Service Management: a Cross-national Study of ITIL adoption, Communications of the Association for Information Systems, February 2014. volume 34, Article 49. DOI: 10.17705/1CAIS.03449 (letöltve:2019. 01.25.)

[97] itSMF (IT service Management Forum) 2013 Global Survey on IT Service Management, http://www.itil.co.il/wp-content/uploads/2015/02/itSMF-2013-Service-Management-Survey-Report.pdf (letöltve: 2017.08. 10.)

[98] ED H. ITIL and IT Operations Optimization, Gartner Webinar, 2009. http://imagesrv.gartner.com/pdf/july22_itil_itoperations_ed_holub_final.pdf (letöltve: 2017.09. 21.)

[99] ERIK, D: Equinor Adapting ITIL, Case Study, Axelos, 2018 https://www.axelos.com/CMSPages/GetFile.aspx?guid=08e241c4-2e38-44a0-9a72-af8d8ea5d273 (letöltve: 2019.03. 11.)

[100] SHARIFI M., AYAT M., RAHMAN A.A., SAHIBUDIN, S. Lessons learned in ITIL implementation failure in: Information Technology, 2008. Volume 1, pp.1-4 IEEE DOI:10.1109/ITSIM.2008.4631627 (letöltve: 2018.01. 12.)

[101] itSMF IT Service Management Global Survey Report, 2017. http://www.itsmfi.org/custom_form.asp?id=1988D02F-E90E-48C3-AB15-F95046D7F83D (letöltve: 2018.04.20.)

[102] ALIEEN, C.S., WUI.G.T.: Implementation of IT Infrastructure Library (ITIL) in Australia: Progress and success factors. https://eprints.usq.edu.au/998/1/Cater-Steel_Tan_IT_Governance.pdf (letöltve: 2018.02.12.)[

[103] FEHÉR, P., SZABÓ Z.: ITSM Kutatás 2015, Fordulathoz közel, 2015. pp. 33. http://it-kutatas.hu/wp-content/uploads/2016/04/Fordulathoz-kozel-Corvinus-ITSM-kutatas-2015.pdf (letöltve: 2018.04.25.)

[104] Forbes Insight: Delivering Value to today's digital enterprise, The state of IT service management, 2017. https://www.bmc.com/content/dam/bmc/migration/pdf/Delivering-Value-to-Today%27s-Digital-Enterprise-FINAL.pdf (letöltve: 2018.05.01.)

[105] MARCO V.: The Value of ITIL in Enterprise Architecture, Conference Paper, 2013 September, Conference: Enterprise Distributed Object Computing Conference (EDOC), 2013 17th IEEE International, DOI:10.1109/EDOC.2013.24, (letöltve: 2019.04.01.)

[106] CRON, W.L. SOBOL, M.G. The Relationship Between Computerization and Performance: A Strategy for Maximizing the Economic Benefits of Computerization. Journal of Information and Management 1983., Volume 6, Issue 3. pp. 171-181. DOI:10.1016/0378-7206(83)90034-4 (letöltve: 2019.04.01.)

[107] STRASSMAN, P.A. The Business Value of Computers. Information Economics Press, New Canaan, Conn, 1990.

[108] PARSONS, D.J. GOTLIEB, C.C. DENNY, M. J.: Productivity and Computers in Canadian Banking, The Journal of Productivity Analysis, 1993. Volume 4, Issue 1-2., pp. 95-113.DOI:10.1007/BF01073468 (letöltve: 2019.05.01.)

[109]ALPAR, P. KIM, M. A Comparison of Approaches to the Measurement of IT Value. In Proceedings of the Twenty-Second Hawaii International Conference on System Science 990.

[110] LAPOINTE, L., MiGNERAT M., Vedel, I.:. The IT productivity paradox in health: A stakeholder's perspective. International Journal of Medical Informatics, 2011., Volume 80, Issue 2, pp.102- 115. DOI: 10.1016/j.ijmedinf.2010.11.004.

[111] LIU, T. K., CHEN, J. R.: Revisiting the productivity paradox: A semiparametric smooth coefficient approach based on evidence from Taiwan. Technological Forecasting and Social Change., 2013. DOI: 10.1016/j.techfore.2013.04.007

[112] CHUNG, K .H., WRIGHT P.,CHAROENWONG: Investment Opportuinites and and Market Reaction to Capital Expenditure Decisions, Journal of Banking and Finance 1998. Volume 22, Issue 1. pp.41-60 DOI: 10.1016/S0378-4266(97)00021-6 (letöltve: 2018.04.25.)

[113] ALAN, R.P.: A Study of Information Technology Operating and Capital Expenditures and Their Effect on Positive Firm Outcomes, Journal of Information Systems Applied Research (JISAR) Volume 7, Issue 3 ISSN: 1946-1836, 2014. http://jisar.org/2014-7/N3/JISARv7n3p4.pdf., (letöltve: 2018.04.25.)

[114] ELLRAM, L.M. A framework for Total Cost of Ownership Model, The International Journal of Logistics Management, 1993. Volume 4, Issue 2. pp.44-60. DOI:10.1108/09574099310804984 (letöltve: 2018.04.26.)

[115] ELLRAM, L.M. A Taxonomy of Total Cost of Ownership Model, Journal of Business Logistics, 1994. Volume 15. Issue 1. pp.171-191.

https://www.academia.edu/21768893/A_taxonomy_of_total_cost_of_ownership_models (letöltve: 2018.04.26.)

[116] ELLRAM, I. M., SIFERD S.P.: Total Cost of Ownership: Key Concept in Strategic cost Management Decisions, Journal of Business Logistics, Volume 19.,Issue 1. 1998. pp. 55-84. https://www.academia.edu/956539/Total_cost_of_ownership_a_key_concept_in_strategic_cost_management_decisions (letöltve: 2018.04.26.)

[117] GARTNER: Defining Gartner Total Cost of Ownership, 2005. https://barsand.files.wordpress.com/2015/03/gartner_tco.pdf (letöltve: 2017. 11. 25.)

[118] ANDERSON, S.W.: A framework for assessing cost management system changes: The case of activity based costing implementation at General Motors, 1986-1993. Journal of Management Accounting Research, 1995. Volume 7, pp.1-51. https://dspace.mit.edu/bitstream/handle/1721.1/1637/Imvp059a.pdf?sequence=2&isAllowed=y (letöltve: 2019. 02. 21.)

[119] ASKARANY, D., SMITH, M., YAZDIFAR, H.: Technological innovations, activity based costing and satisfaction, 2007. Journal of Accounting, Business and Management, Volume 14, pp.53-63.

[120] HAO, S.: Appraisal of the customer lifetime value of commercial banks based on unascertained measurement. International Conference on Information Management, Innovation Management and Industrial Engineering, 2009. pp. 399-402. DOI: 10.1109/ICIII.2009.253 (letöltve: 2019. 02. 21.)

[121] HUSSAIN, M., GUNASEKARA A.: Activity-based cost management in financial services industry. Managing Service Quality: An International Journal, 2001. Volume 11, Issue 3, pp.213-226. DOI: 10.1108/09604520110391324 (letöltve: 2019. 02. 21.)

[122] HUGHES, S.B.; GJERDE, K.P. Do Different Cost Systems Make a Difference? Scholarship and Professional Work-Business 11. https://digitalcommons.butler.edu/cob_papers/11 (letöltve:2019.03.15.)

[123] CARUSO, D.: Application portfolio management: a necessity for Future IT Manufacturing Business Technology, 2007., Volume 25., Issue 10, pp. 48-50. https://www.controleng.com/articles/application-portfolio-management-a-necessity-for-future-it/, (letöltve:2018.03.15.)

[124] MURPHY P.: The application Portfolio Management Landscape-Combine Process and Tools to Tame for Application Development and Delivery Professionals 2011. Forrester http://www.infobal.com/wp-content/uploads/2014/07/Forrester-APM-Landscape-Apr2011.pdf (letöltve: 2017. 12 23.)

[125] Computer Economics: IT spending and staffing Benchmarks 2017/2018. https://www.computereconomics.com/page.cfm?name=it%20spending%20and%20staffing%20study (letöltve:2018.03.25.)

[126] KPMG: CIO Survey, 2017. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/harvey-nash-kpmg-cio-survey-2017.pdf (letöltve:2018.03.25.)

[127] BOEHM W. PAPACCIO P.N.: Understanding and controlling software costs, IEEE Transactions on Software Engineering, Volume: 14 Issue 10, Oct 1988 pp.1462-1477. DOI**:**10.1109/32.6191 (letöltve:2019.02.18.)

[128] SOTTINI M.:IT Financial Management, 2009. https://www.vanharen.net/Samplefiles/9789087535018_it-financial-management.pdf, (letöltve:2019.02.14.)

[129] MOGOR T.-RAJNAI Z: Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása. XXIII. Évfolyam, 2014/2. Nemzeti Közszolgálati Egyetem Katonai Műszaki Tudományági Folyóirata, pp. 43-59., https://www.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2014_-ev-2_-szam.original.pdf (letöltve:2019.05.20.)

[130] LUIZ C. D. S., LUCIEL H. de O., LUIZ M. S. S.: Organizational Risk Management- A Case Study in Companies that have won the Brazilian Quatity Award Prize, Journal of Technology Management and Innovation, 2001.,Volume 6, Issue 2. DOI:10.4067/S0718-27242011000200016 (letöltve:2019.04.18.)

[131] FRASER, R. S., SIMKINS B. J.:The challenges of and solutions for implementing enterprise risk management, 2016. Business Horizons, Elsevier Volume 59 Issue 6, pp. 689-698. DOI: 10.1016/j.bushor.2016.06.007 (letöltve:2019.03.10.)

[132] LUNDQVIST S. A.: Why firms implement risk governance – Stepping beyond traditional risk management to enterprise risk management. Journal of Accounting and Public Policy, 2015. Volume 34, Issue 5, pp. 441-466 DOI:10.1016/j.jaccpubpol.2015.05.002 (letöltve:2019.05.10.)

[133] MAZLINA, M., AMIRAH A.:A case study of Enterprise Risk Management implementation in Malaysian construction companies. International Journal of Economics and Financial Issues, Volume 5 Special Issue, pp.70-76 2015. http://www.econjournals.com/index.php/ijefi/article/view/1345/pdf (letöltve: 2019.04. 22.)

[134] ROSTAMI A., SOMMERVILLE, J., WONG, I. L.,LEE, C.:. Risk management implementation in small and medium enterprises in the UK construction industry. Engineering, Construction and Architectural Management, 2015. Volume 22. Issue 1, pp. 91-107. DOI:10.1108/ECAM-04-2014-0057 (letöltve:2019.01.10.)

[135] Committee of Sponsoring Organizations of the treadway commission (COSO), Enterprise Risk Management-Integrated Framework, https://www.coso.org/Pages/erm-integratedframework.aspx (letöltve: 2017.10.10.)

[136] JOSEPHINE E.,FREDRIK K.: Enterprise Risk Management -The usage of COSO's framework in recently publicly listed Swedish companies, Lund University, School of Economics and Management

http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8894370&fileOId=88943 (letöltve: 2017.08. 22.)

[137] MARK, B.,BRUCE, B., BONNIE, H.: The state of risk oversight: an overview of enterprise risk management practices, NC STATE: Poole College of Management, Enterprise Risk Management Initiative https://erm.ncsu.edu/az/erm/i/chan/library/AICPA_ERM_INITIATIVE_Research_Study_2017.pdf (letöltve: 2017.12. 01.)

[138] PWC: Risk in review, Managing risk from the front line, Annual study, 2017. https://www.pwc.com/us/en/risk-assurance/rir2017/pwc-2017-risk-in-review-study.pdf (letöltve: 2017.07. 15.)

[139] OPENGROUP,2015, IT Risk Management Survey Summary. White Paper. https://www2.opengroup.org/ogsys/catalog/w154, (letöltve: 2017.02.17.)

[140] KPMG, Is everything under control? 2017 Global Audit Committee Pulse Survey https://home.kpmg.com/content/dam/kpmg/xx/pdf/2017/01/2017-global-audit-committee-pulse-survey-global-non-interactive.pdf (letöltve: 2017. 08.04)

[141] ERNST&YOUNG: Addressing the evolving challenges of IT risk, IT Risk Management Survey 2014. http://www.ey.com/Publication/vwLUAssets/EY-it-risk-management-survey-2014/$FILE/EY-it-risk-management-survey-2014.pdf (letöltve: 2017.05.02.)

[142] CISCO: Annual Cybersecurity Report, 2017 https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf (letöltve: 2018. 03. 26.)

[143] STERLICZ A.: Kockázatirányítás új dimenziói, Vezetéstudomány, XLVII. Évfolyam, 2016. 1.szám http://unipub.lib.uni-corvinus.hu/2239/1/VT_2016n1p18.pdf, (letöltve: 2018. 01. 20.)

[144] KNIGHT F. H.: Risk, Uncertainty and Profit; Houghton Mifflin Company, Boston, 1921 https://fraser.stlouisfed.org/files/docs/publications/books/risk/riskuncertaintyprofit.pdf (letöltve: 2018. 01. 20.)

[145] HILLSON D.: Extending the risk process to manage opportunities, in: International Journal of Project Management, Volume 20, Issue 3. Elsevier, Amsterdam, 2002. pp.235-240. DOI:10.1016/S0263-7863(01)00074-6 (letöltve: 2019. 02. 01.)

[146] MICHELBERGER P.: Risk Management for Business Trust In: Michelberger Pál (ed.) MEB 2014: Management, Enterprise and Benchmarking in the 21st Century. 413 p. Budapest: Óbuda University, Keleti Károly Faculty of Business and Management, 2014. pp. 401-413.

[147] KRISTINA N.: Strategic risk management, The value of enterprise risk management in strategic planning, https://www.ermstrategies.com/blog/wpcontent/uploads/2012/07/StrategicRiskManagementUofUWorkshop.pdf (letöltve: 2017.12. 08.)

[148] FARKAS SZ.: A vállalati kockázatkezelés új korszaka-RM 2.0. p.4. http://kgk.sze.hu/images/dokumentumok/kautzkiadvany2014/Farkas%20Szilveszter.pdf (letöltve: 2018.01.10.)

[149] MICHELBERGER, P., HORVATH, ZS: Biztonságorientált folyamatmenedzsment, International Journal of Engineering and Management Sciences (IJEMS),2017. Volume 2, Issue 4. DOI: 10.21791/IJEMS.2017.4.28. (letöltve: 2019.01.10.)

[150] WILLIAMS G. Everything you wanted to know about Management of Risk, (M_o_R) in less than 1000 words, White Paper 2011., The Stationery Office http://miroslawdabrowski.com/downloads/M_o_R/White%20papers/Everything%20you%20wanted%20to%20know%20about%20Management%20of%20Risk%20(M_o_R)%20in%20less%20than%201000%20words%20%5B12.2011%5D.pdf (letöltve: 2017.március 10.)

[151] International Organization for Standardization: ISO31000:2018 Risk Management, https://www.iso.org/iso-31000-risk-management.html, (letöltve: 2017.09. 15.)

[152] International Organization for Standardization: ISO31010:2009 Risk Management,https://www.iso.org/standard/51073.html (letölve: 2017.09. 15.)

[153] BALOGH A.-HORVÁTH ZS.-SZLÁVIK P.: Magyar Minőség, XX. Évfolyam,03. 2011. pp.11.o. https://quality-mmt.hu/wp-content/uploads/2016/06/2011_03MM.pdf, (letöltve: 2018.01.15.)

[154] PQRI: Manufacturing Technology Committee-Risk Management Working Group, Hazard and Operability Analysis: HAZOP, 2015. http://pqri.org/wp-content/uploads/2015/08/pdf/HAZOP_Training_Guide.pdf (letöltve: 2016.05.10.)

[155] CLMEMENS P.L. –RODNEY J.S., U.S. Department of Health and Human Services: System safety and risk management,1998. Failure modes and effects analysis, Lesson V. https://www.cdc.gov/niosh/topics/SHAPE/pdfs/safriskengineer.pdf (letöltve: 2016.05.10.)

[156] European Union Agency for Network and Information Security (ENISA): Inventory of Risk Management/Risk Assessment Methods, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods (letöltve: 2018.04. 15.)

[157] The Sarbanes-Oxley Act: 2002, http://www.soxlaw.com/ (letöltve: 2016.04.30.)

[158] Health Information Privacy: Summary of the HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (letöltve: 2017.01.30.)

[159] EUR-Lex: Access to European Union Law**:** Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

(általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679 (letöltve: 2017.05.31.)

[160] ISACA: The RiskIT Farmework. Rolling Meadows, IL 60008 USA: ISACA 2009. https://m.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf (letöltve:2019.04.19.)

[161] ISO/IEC 13335-1: 2004, https://www.opensecurityarchitecture.org/cms/definitions/it-risk

[162] BOEHM W.: Software Risk Management: Principles and Practices, IEEE Software, 1991. Volume 8, Issue 1, pp.32-41 DOI:10.1109/52.62930 (letöltve:2019.04.29.)

[163] SCHMIDT R., LYYTINEN K.. KEIL, M. CULE P.. Identifying Software Project Risks: An International Delphi Study, Journal of Management Information Systems, 2001.,Volume 17, number 4, pp. 5-36, https://pdfs.semanticscholar.org/2bec/971dec8ed7f13b7ec39189693e0e313ef960.pdf (letöltve:2019.04.29.)

[164] RON S., ANTHONY M., Performing a Security risk assessment, ISACA Journal, Volume 1. 2010. https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx (letöltve:2018. 03.18.)

[165] MUKUL P. Technology Risk Measurement and reporting, ISACA Journal, Volume 6. 2011. https://m.isaca.org/Journal/archives/2011/Volume-6/Documents/11v6-Technology-Risk-Measurement-and-Reporting.pdf (letöltve:2018. 03.18.)

[166] SZÁDECZKY T. :Risk Management of New Technologies, 2016. AARMS, Volume 15. Issue 3 pp.279-290. http://real.mtak.hu/50003/1/aarms_2016_3_08_szadeczky.original_u.pdf (letöltve:2019. 04.29.)

[167] SARAH V. R: Risk Management Model in ITIL, 2012. https://fenix.tecnico.ulisboa.pt/downloadFile/395144242579/Risk%20management%20on%20ITIL%20(Article).pdf (letöltve: 2017.10.20.)

[168] HERVÉ D. Management of risk and its integration within ITIL, CAPGEMINI 2015. https://www.slideshare.net/hdoornbos/risk-mgt-itil (letöltve: 2017.10.20.)

[169] COBIT 5: Vállalati IT irányítás és menedzsment üzleti keretrendszere, ISACA 2012.

[170] HORVÁTH L., LUKÁCS GY., TUZSON T., VASVÁRI GY.: Informatikai biztonsági rendszerek, Budapest 2001. pp.6-7.

[171] MUHA L.: Fogalmak és definíciók: 2.4. in: Maha L.: Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig., Budapest: Verlag Dashöfer, 2004. pp. 1–37

[172] BEINSCHRÓTH J.: Informatikai rendszerekkel támogatott folyamatok működésfolytonosságának modellezése és mérése, Hadmérnök, 2006. 1. évf. 2. sz, 4-17.o.

[173] SANS survey on Application Security and Programs, JimBird, Frank Kim, 2012. https://www.sans.org/reading-room/whitepapers/analyst/membership/35150 (letöltve: 2019.04.15.)

[174] FY2018 SPECTRUM Application Portfolio Management, Guidance for Texas state agencies, 2018. Texas Department of Information Resources, https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/FY%2018%20Application%20Portfolio%20Management%20Assessment%20and%20Validation%20Instructions.docx (letöltve: 2019.05.15.)

[175] TATA Consultancy: Next generation application portfolio rationalization, 2011., White Paper. https://www.platformmodernization.org/tcs/Lists/ResearchPapers/Attachments/3/Consulting_Whitepaper_Next-Generation-Application-Portfolio-Rationalization_09_2011.pdf?Mobile=1 (letöltve: 2019.05.15.)

[176] SASVÁRI P., NEMESLAKI A., WOLF R.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises, AARMS Volume 14, Issue 1 2015., 63–78. https://folyoiratok.uni-nke.hu/document/uni-nke-hu/aarms-2015-1-sasvari.original.pdf (letöltve: 2019.05.15.)

HIVATKOZOTT SAJÁT PUBLIKÁCIÓK

[177] KOVACSNE MOZSAR, L.A. MICHELBERGER P.: IT risk management and application portfolio management, Polish Journal of Management Studies, Volume 17, Issue 2 2018. pp. 112-122. DOI: 10.17512/pjms.2018.17.2.10

[178] MOZSÁR, L. A. Informatikai alkalmazások menedzsment kérdéskörei, Taylor: Gazdálkodás- és szervezéstudományi folyóirat: A virtuális intézet Közép-Európa Kutatására Közleményei, 7 Évfolyam, 1-2.szám, 2015. pp. 163-168., http://vikek.eu/wp-content/uploads/2015/10/TAYLOR_2015-nyomdai.pdf

[179] KOVACSNE MOZSAR L.A.: Reducing IT costs and ensuring safe operation with application of portfolio management, Serbian Journal of Management Volume 12, Issue 1 2017. pp. 143-155., doi: 10.5937/sjm12-11452

[180] MOZSÁR, L. A.: Application Portfolio Management In: Michelberger, Pál (szerk.) MEB 2014: Management, Enterprise and Benchmarking in the 21st Century Budapest, Magyarország: Óbudai Egyetem Keleti Károly Gazdasági Kar, 2014 pp. 383-392. https://kgk.uni-obuda.hu/sites/default/files/26_Mozsar_1.pdf

[181] KOVACSNE MOZSAR L. A.: Integrating Risk Management into Application Portfolio Management. In: Gabriela, Kristová; Peter, Schmidt; Miroslav, Hudec; Janette, Brixová; Mária, Szivosová; Pavol, Jurík (szerk.) Reviewed Proceedings: Fifth International Scientific Videoconference of Scientists and PhD. students or candidates: Trends and Innovations in E- business, Education and Security, Bratislava, Szlovákia: University of Economics in Bratislava, 2015 pp.43-52 http://webkonf.ponuky.info/index.php/archiv/2015

[182] MOZSÁR, L. A.: Kockázatmenedzsment és informatikai alkalmazások menedzsmentjének kapcsolata, Taylor: Gazdálkodás- és szervezéstudományi folyóirat: A virtuális intézet Közép-Európa Kutatására Közleményei, 7.Évfolyam, 3-4.szám, 2015. pp. 155-161. http://vikek.eu/wp-content/uploads/2018/07/TaylorNo20-212015.3.%C3%A9s4.sz%C3%A1m-1.pdf

[183] MOZSÁR, L., MICHELBERGER, P.: The Relationship between Enterprise Architectural Management and Application Management in Large Companies, Scientific and Educational Forum on Business Information Systems, SEFBIS JOURNAL, (NJSZT) 9. Évfolyam 2014. pp. 22-27.

RÖVIDÍTÉSJEGYZÉK

APM: Application Portfolio Management, Alkalmazás Portfólió Menedzsment

BCM: Business Continuity Management, Üzletmenet Folytonosság Menedzsment

BCP: Business Continuity Plan, Üzletmenet Folytonossági Terv

BSI: British Standards Institution, Brit Szabványügyi Hivatal

CAPEX: Capital Expenditure, Tőke Kiadás

CCTA: Central Computer and Telecommunication Agency, Központi Számítógép és Távközlési Ügynökség

CI: Configuration Item, Konfigurációs Elem

CIO: Chief Information Officer, Informatikai Igazgató

CISA: Certified Information System Auditor, Képesített Informatikai Ellenőr

CISM: Certified Information Security Manager, Képesített Informatikai Biztonsági Menedzser

CMDB: Configuration Management Database, Konfiguráció Menedzsment Adatbázis

CMMI: Capability Maturity Model Integration, Integrált Képességi-Érettségi Modell

COBIT: Control Objecitves for Information and Related Technology, Informatikai Ellenőrzési célok

COSO: Committee of Sponsoring Organizations of the Treadway Commission, Felelős Vállalat-Irányítás Nemzetközileg Elfogadott Szabványa

CPU: Central Processing Unit, Központi Feldolgozó Egység

CRAMM: CCTA Risk Analysis and Management Method, Kockázat Elemzés-és Kezelési Módszertan

CSF: Critical Success Factor, Kritikus Sikerességi Faktor

DRP: Disaster Reovery Plan, Katasztrófahelyreállítási Terv

ENISA: European Union Agency for Network and Information Security, Európai Hálózat és Információbiztonsági Ügynökség

ERM: Enterprise Risk Management, Vállalati Kockázatmenedzsment

ETA: Event-tree Analysis, Eseményfa-Elemzés

FMEA: Failure Mode and Effects Analysis, Hibamód-és Hibahatás Elemzés

FTA: Fault Tree Analysis, Hibafa Elemzés

GDPR: General Data Protection Regulation, Általános Adatvédelmi Rendelet

GT: Grounded Theory, Megalapozott Elmélet

HAZOP: Hazard and Operability Studies, Működőkepesség és Veszélyelemzés

HIPAA: Health Insurance and Accountability Act, Egészségbiztosítási Hordozhatósági és Felelősségi Törvény

IEC: International Electrotechnical Commission, Nemzetközi Elektrotechnikai Bizottság

ISACA: Information System Audit and Control Association, Informatikai Auditorok és Ellenőrök Szövetsége

ISO: International Organisation of Standards, Nemzetközi Szabványügyi Szervezet

ITIL: Information Technology Infrastructure Library, Informatikai Infrastruktúra Könyvtár

ITRM: Information Technology Risk Management, Informatikai Kockázat Menedzsment

itSMF: IT service Management Forum, Informatikai Szolgáltatás Menedzsment Fórum

M_o_R : Management of Risk, Kockázat Menedzselése

MOF: Microsoft Operation Framework, Microsoft Operációs Keretrendszer

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

OPEX: Operating Expense, Operatív Kiadások

PDCA: Pland Do Check Act, Tervezés-Cselekvés-Ellenőrzés-Cselekvés

SOD: Separation Of Duties, Feladatkörök Elkülönítése

SLA: Service Level Agreement, Szolgáltatás-Szint Megállapodás

TCO: Total Cost of Ownership, Teljes Költség Tulajdonos

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

1. számú Melléklet: Interjúkérdések

K1: Használ-e a szervezet bármilyen megoldást, eszközt az informatikai alkalmazások nyilvántartására?

K2: Hallott már bármilyen módszertanról, ami segíti az informatikai alkalmazások nyilvántartását? Ha igen, melyekről? Történik valamilyen szempont alapján alkalmazás kategorizálás a nyilvántartásban?

K3 (Ha K2 Igen): Milyen területek vannak bevonva a szervezetben az APM/alkalmazás nyilvántartással foglalkozó osztályok munkájába?

K4: Ki a felelős, melyik egység, részleg az informatikai alkalmazások nyilvántartásáért?

K5: Milyen szabvány, előírás, ajánlás alapján történik az informatikai alkalmazások nyilvántartása?

K6: Használnak az alkalmazások nyilvántartására valamilyen szempont szerinti kategorizálást (portfólió) képzést? Ha igen, mi alapján képezik?

K7: A használt ajánlás, szabvány megfelelően részletes és útmutatást ad arra hogyan kell kezelni az informatikai alkalmazások portfolióba sorolását, illetve a portfoliók menedzselését?

K8: Mikor vezették be az ITIL-t a szervezetbe? Az ITIL bevezetésével párhuzamosan történt az informatikai alkalmazások nyilvántartására vonatkozóan bármilyen változás a szervezetben?

K9: A jelenleg használt ITIL ajánlás részletesen és teljeskörűen lefedi azt, hogyan kell kezelni az informatikai alkalmazások nyilvántartását?

K10: Problémát okoz-e a szervezetben, hogy az ITIL mellett elkülönülten egy másik ajánlást, módszertant, eszközt is használnak az informatikai alkalmazások nyilvántartására? (Ha van ilyen)

K11: Hogyan látja az ITIL-ben az alkalmazás portfólió kezelés részt, mennyire alkalmazható?

K12: Informatikai költségek nyilvántartása informatikai alkalmazásokra -Hogyan történik?

K13: Alkalmazás portfólió kezelés-informatikai költségek is láthatóak, mi a véleménye? Hasznos lenne?

K14: ITIL mennyire és hogyan tér ki az informatikai költség analitikára informatikai alkalmazás szinten?

K15: Az informatikai kockázatok kezelése hogyan történik a szervezetben? Valamilyen módszertan, szabvány alapján?

K16: Melyik szabványt, nemzetközileg elismert sztenderdet használják az informatikai kockázatok kezelésére?

K17: A vállalati kockázatok kezelésénél figyelembe veszik-e az informatikai alkalmazások működésénél, támogatásánál fellépő kockázatokat?

K18: Az informatikai alkalmazásokkal kapcsolatban felmerülő kockázatok nyilvántartására, nyomon követésére mit alkalmaznak?

K19: Van a szervezetnek jelenleg valamilyen összehangolt keretrendszere, működési formája, kapcsolódási pontja az informatikai kockázatmenedzsment és az APM integrált működésére?

K20: Milyen kockázatokat tudna felsorolni az alkalmazás portfolió menedzsment során fellépő tevékenységeknél?

K21: Ezekkel a fentebb felsorolt kockázatokkal részletesen foglalkozik és elemzi a szervezetnek a kockázatmenedzsment osztálya, részlege?

K22: El tudná azt képzelni, hogy van olyan megoldás, ami lefedi az informatikai kockázatokat és az informatikai alkalmazások nyilvántartására is ad részletes ajánlást, javaslatot?

K23: Növelhető a biztonság, biztonságos informatikai szolgáltatás azzal, ha az informatikai kockázatok integrálva, részletezve láthatóak lennének az informatikai alkalmazás nyilvántartásban?

K24: Egyéb problémák, javaslatok?

2. számú Melléklet: Interjúk kivonata

1. kérdés: Informatikai alkalmazások nyilvántartása

1. A szervezetben 400-500 informatikai alkalmazást tartanak nyilván a CMDB szoftverben. A CMDB egy konfigurációs adatbázis. A rendszerben nemcsak az informatikai alkalmazásokat, hanem az alkalmazások összetevőit, illetve különböző adatrétegeket is nyilvántartanak. A szoftver használata az ITIL ajánlásból jött, tehát van valamennyi módszertani alapja. A CMDB használatának több előnye van. Egyrészt a komponensek nyilvántartására alkalmas, mivel megjegyezhetetlenül sok alkalmazásuk van. Azonban a CMDB nem csak adatbázis célokra használják, hanem sok munkafolyamatok is kapcsolódnak hozzá, amik a változáskezeléssel vannak összekötve. A CMDB-ben tartják nyilván, ki felel az adott alkalmazásért. A CMDB-ben nem képződik automatikusan semmilyen kategorizálása az alkalmazásoknak. A felhasználók a CI-n (Configuration Item) keresztül képesek keresni. A CI lényegében egy attribútum. Néhány leíró adat az alkalmazásokra: rendszerfelelős neve, milyen programnyelven íródott az alkalmazás, üzemeltetési idő, forráskód helye. A CMDB-ben való keresés eredménye nemcsak alkalmazáslista lehet, hanem alkalmazásmodul és fájlmegosztás is. Le lehet kérdezni a virtuális szervereket, tűzfalakat is. Alkalmazáshoz kapcsolódó dokumentációkat itt nem lehet látni, illetve bármilyen alkalmazáshoz tartozó pénzügyi információkat sem. Informatikai költségek egyéb pénzügyi szoftverekben vannak tárolva.

2. Folyamatosan előkerülő probléma a szervezetben, hogy milyen alkalmazás nyilvántartásuk van, mit tekintenek igazán alkalmazásnak. Az alkalmazás definiálása nem tisztázott. Egy konkréteset, ami az elmúlt években történt, hogy egy vékony kliens bevezetésnél meg kellett nézni azt, hogy milyen alkalmazás portfóliója van a cégnek. Rengeteg különböző kimutatás készült. Később kiderült, hogy az alkalmazás lista nem teljes, mivel a bérszámfejtésnek is volt egy alkalmazása. Az alkalmazottak egy Excelben dolgoztak, megírt makrókkal. Nem sorolták az alkalmazások közé az Excelt, pedig szükségszerű lett volna. Az áttérés az Excelről egy másik technológiára nem volt lehetséges, így továbbra is az Excelt használják. Az ITIL v2-ben szereplő leírás a CMDB-ről jó alapot ad. Próbálták adatbázis szakértőkkel elkészítetni, de nehézkes volt. A CMDB jól lefedi a változáskezelés, probléma kezelés, valamint az incidens kezeléshez tartozó folyamatokat.

3. Az informatikai alkalmazások nyilvántartására CMDB-t használnak. Az alkalmazásokhoz tartozó különböző attribútumok is az adatbázisban találhatóak. Az alkalmazások monitorozása különböző eszközökkel történik, attól függően, hogy milyen technológiát használnak, milyen platformon futnak az alkalmazások. A CMDB előtt sok különböző nyilvántartása volt a szervezetnek, főleg Excelek. A CMDB első verzióban volt egy alap modell, aztán a rákövetkező verziókban már a kapcsolati rendszereket, összefüggéseket illetve a relációkat a különböző konfigurációs elemek között fejlesztették. A korábbi 3-4 kapcsolati lehetőségek száma 28-30-ra emelkedett.

4. Az interjúalany több szervezet esetében tapasztalta, hogy volt valamilyen nyilvántartás az alkalmazásokra vonatkozóan, de ezek legtöbbször Excelben készültek. Manuálisan töltötték az információkat a nyilvántartásba. A nyilvántartásban azt jegyezték fel, hogy konkrétan milyen alkalmazások érhetőek el a cégnél. Listázva volt szolgáltatásonként a szolgáltatás felelőse is, elérhetőséggel.

5. Ahol informatikai vezetői pozíciókat töltött be, ott az esetek nagy részében azzal a problémával küzdöttek, hogy nem tudták a szervezetek integráltan egy helyen nyilvántartani az alkalmazásokat. A Magyar Postánál is ezzel a problémával találkoztak. Ott több, mint 300 informatikai alkalmazásnak kellett volna összehangoltan működni. A nyilvántartások teljesen heterogén voltak. Az alkalmazás konszolidáció, mint problémakör megjelenik sok más nagyvállalatnál is. Globális nagyvállalatnál a telekommunikáció szektorban is problémát jelent, hogy nem rendelkeznek központi alkalmazás nyilvántartással.

6. Pályafutása alatt találkozott informatikai alkalmazás nyilvántartással. Azonban a legtöbbször nem volt megfelelően formalizálva.

7. A legtöbb nagyvállalatnál az informatikai alkalmazás nyilvántartás képzése üzleti modell alapján történik. Ahol több szervezeti egység, tehát organizáció van, ott az üzleti organizációra szokták csoportosítani az alkalmazásokat. Az egységbe való sorolás után jellemzően az üzleti szervezeti partnerrel rangsorolják az alkalmazásokat adat szempontjából. Ebben a lépésben elemzik a szakértők, hogy milyen típusú adatokat tárolnak, és milyen folyamatokat támogatnak. Az integrált nyilvántartásra többnyire saját fejlesztésű szoftver használnak a cégek.

2. kérdés: Informatikai alkalmazás portfólió képzés

1. Az alkalmazás portfólió értelmezése az, ahogy a CMDB szoftver kilistázza az összes alkalmazást és a lekérdezés eredménye megjelenik a képernyőn. A CMDB-ben nem lehet listázni részletesen az informatikai szolgáltatások mögött lévő üzleti folyamatokat. Ezáltal az üzletileg redundáns funkciókat sem tudják kiszűrni, elemezni. Igény van rá, hogy az egyes informatikai szolgáltatások mögött láthatóak legyenek az üzleti folyamatok, valamint a hozzá kapcsolódó informatikai alkalmazás lista is. Az összefüggés kialakítására, feltérképezésére nem alkalmas jelenleg a CMDB. Belső fejlesztéssel lehetne megoldani. Az informatikai alkalmazások közötti interfész kapcsolatok nem láthatóak a CMDB-ben.

2. Az ITIL ad útmutatást az alkalmazás nyilvántartásra, portfólióra képzésre, de ez sajnos nem elég. Mivel sok szempont szerint kell nyilvántartani az alkalmazásokat, ezért az ITIL csupán vezérelvként szolgálhat. Eljutottak odáig a szervezetek, hogy a statikus alkalmazás nyilvántartás kevés. Jelenleg paradigmaváltás van, a digitális transzformáció felé haladnak a szervezetek. A fejlődés megköveteli az informatikai szolgáltatások nyilvántartását, de ez már nem elég. A szolgáltatásokat mérni is kell. A méréshez pedig egy központosított, dinamikus nyilvántartásra van szükség.

3. A konfigurációs elemek osztályba vannak sorolva, s ezen belül megvan mindegyiknek a saját attribútum köre. A CMDB-ben csak technikai információk vannak, üzleti információk nincsenek. Tervezi a szervezet, készít egy térképet az üzleti folyamatokról, majd ezt integrálja a CMDB-be. A tervezett elméleti megoldás az, hogy az üzleti folyamatok konfigurációs elemek lesznek a szoftverben. Az integrálás után lekérdezhető lesz az üzleti folyamat, szolgáltatás mögött futó IT szolgáltatás, alkalmazás, hardver, infrastruktúra elemek valamint a köztük lévő összes kapcsolatrendszer. Az előnye a megoldásnak az incidenskezelésnél lesz látható, mérhető. Egy incidens esetén tudják majd azonosítani, és felmérni melyik üzleti, informatikai szolgáltatásra, informatikai alkalmazásra hat az adott probléma. Nem képeznek alkalmazás portfóliókat, de van egy nyilvántartásuk az összes alkalmazásról. Az alkalmazásokhoz tartozó dokumentációkat egy külön szakmai terület kezeli. A lehetőség, funkció megvan a CMDB-ben, hogy felcsatolják az alkalmazásokhoz rendelhető dokumentációkat, de ez nem történik meg. A dokumentáció feltöltés elmaradásának az oka a manualitás.

4. Ahol találkozott alkalmazás nyilvántartással ott a CARISMA szoftvert használták, de sajnos a legtöbb helyen nincs alkalmazás portfólió képzés, bár igény lenne rá és hasznosnak ítéli meg.

5. Találkozott olyan szoftverrel, amelyik üzleti folyamat menedzselés tervezésére és nyilvántartására volt alkalmas. Konkrét példa az Aris. Tapasztalata alapján a portfólió megközelítés a kockázat menedzsment szoftvereknél jellemzőbb, nem az alkalmazásoknál. Az SAP nagyvállalatnak is van egy olyan fejlesztése, globális modulja, ami alkalmas az alkalmazások portfólió nyilvántartására. A hangsúly a modul funkciójában azon van, hogy nyilván tartják azt, hogy mennyire kockázatos az adott alkalmazásnak a leállása, használata, üzleti folyamatra való hatása.

6. A szervezetek látják azt, hogy mit tartanak nyilván, de konkrétan a portfólió képzés alatt azt értették, hogy lebontották szakterületekre a használt alkalmazásokat. A portfólió nyilvántartásra nem szoftvereket használtak, hanem saját fejlesztésű megoldásokat.

7. Munkája során azt tapasztalta, hogy az informatikai szolgáltatásokat, amit az IT terület nyújt, informatikai szolgáltatások alapján csoportosították, tehát szerviz portfólió képzés történik, aminek a felelőse a Megoldás (Solution) Architekt. Kezdeményezéseket már látott alkalmazás szinten való portfólió képzésre, de működő modellt még nem.

3. kérdés: ITIL és alkalmazás portfólió menedzsment

1. Az informatikai folyamatok támogatására, mint egy módszertani gyűjtemény alkalmas az ITIL, azonban a teljes körű bevezetése, leképezése részletesen az informatikai folyamatokra költség és időigényes. Jelenleg a konkrétan mérhető pénzt generáló projekteken van a hangsúly, prioritás a szervezetben. Az informatikai osztályon dolgozó személyek részt vesznek ITIL oktatáson, képzésen. Ha az ITIL-t teljes körűen bevezetnék az informatikai osztályon, akkor a jelenlegi informatikai alkalmazott létszám kevés lenne. Az ITIL ajánlásban szereplő alkalmazás portfólió azt jelenti, hogy a CMDB-ben listázható az összes alkalmazás. A jelenlegi ITIL ajánlás tartalmaz néhány információt arra vonatkozóan, mit kellene tartalmazni az alkalmazás portfoliónak. Az ITIL alkalmazás portfólióra vonatkozó ajánlás, tehát a táblázatban szereplő példák jó ötletek. Azonban nincsenek részletezve, hogy mit kell az egyes attríbutomok alatt érteni. Konkrétan nehéz értelmezni a „user interface”-t. Egyértelmű, hogy nem lehet 100%-osan átmásolni az ajánlást. Az ITIL nem tesz ajánlást arra vonatkozóan hogyan lehetne, vagy

kellene az alkalmazás portfólió attribútumokat integrálni a CMDB-be. Szükséges az ITIL ajánlásnak, a bővítése, kidolgozása, amely támogatja az informatikai alkalmazások portfólióba sorolását és menedzselését.

2. Az ITIL kitér arra, hogy szerver, vagy alkalmazás nyilvántartásnál milyen információkat kell összegyűjteni, listázni, azonban nem részletezi a megvalósítási lépéseket. Az ITIL-nek nincsenek olyan részei, ami konkretizálná az alkalmazás nyilvántartásokra vonatkozó lépéseket. Irányelveket ad a nyilvántartásra vonatkozóan, de nem részletes. A piacon sok szakember, tanácsadó van, akik képesek az egyedi megoldást létrehozni.

3. Az ITIL -nek a konfigurációs adatbázis részére vonatkozó ajánlása nem eléggé kidolgozott. Egy szervezetben sok időt vesz igénybe, amíg egységesítik a nyilvántartásokat. Tipikus probléma, hogy adott kifejezés mögött a szervezetben a szakértők mást értenek, ennek az egységesítése is nehéz feladat. A szervezetben 40 különböző személynek, 40 különböző módon van szüksége ugyanarra az információra. A CMDB mellett vannak egyéb nyilvántartások is, Excelekben, amit nem tud a szervezet a CMDB-be feltölteni. Konkrét példa: egy rack szerkénynek a tartalma ábrával. Szükség lenne olyan ajánlásra, ami támogatná azt, hogy egy adott incidens bejelentésnél, ahol 5-6 különböző informatikai alkalmazás van összekapcsolva, akkor látható legyen az átfolyó adatoknak a minősége, mennyisége, elvárások, folyamatábrákkal kiegészítve.

4. Portfólióba nem igazán sorolták az alkalmazásokat. Igazából ebben a megfogalmazásban a portfólióba a szolgáltatások sorolása lehetséges. A jelenlegi cég, ahol dolgozik, több mint 7000 főt foglalkoztat. Felismerték azt, hogy az informatikai szolgáltatások támogatására az ITIL-t ajánlásait figyelembe kell venniük, mert anélkül rengeteg informatikai folyamat nem kellően szabályozott. Nem használják az összes komponensét, mert nincs elég idejük a bevezetésre. Azonban az első feladatok közé tartozott a feladatlistán, hogy a szolgáltatásokat csoportosították. Ahhoz hogy ne vesszenek el abban, hogy ki mit csinál, a Manage Engineering rendszert használnak. Így tudják nyomon követni, hogy melyik szolgáltatás kihez tartozik.

5. Az interjúalany olvasott róla, hogy az új változata az ITIL-nek kitér az alkalmazás nyilvántartásra, de gyakorlatban még nem találkozott vele, hogy ezt használták volna. Ahol szóba került, hogy elkezdik használni, ott is inkább az informatikai üzemeltetés kiszervezéskor merült fel.

6. Tudatában van annak, hogy az ITIL tesz az alkalmazás portfólió képzésről említést. Véleménye szerint használható.

7. Az üzleti területek felől érkező igény a szolgáltatások költségcsökkentésére irányul a legtöbbször. Természetesen nem szeretnének olyan szolgáltatásért fizetni, amit nem használnak. A következő lépés a szolgáltatás támogatáshoz használt informatikai alkalmazásoknak az elemzése. Nem találkozott informatikai alkalmazás portfólió képzéssel, csak szolgáltatás portfólióval.

4. kérdés: Informatikai költség nyilvántartás az alkalmazás portfólió menedzsment részeként

1. A CMDB nem tartalmazza az informatikai költségeket. Az integrálása, tehát az informatikai költségek átvezetése a CMDB-be költséges és időigényes feladat lenne, ezért az erre a célra egy másik rendszert használ a szervezet. Az üzlet felől egyelőre nem érkezett igény arra, hogy alkalmazás szinten részletezve legyenek a pénzügyi információk rendelve, ezért ebbe az irányba egyelőre nem történt semmilyen előrelépés.

2. A nagy IT környezettel rendelkező nagyvállalatok a pénzügyi kimutatások készítésénél nem veszik figyelembe az ITIL-t . A szervezetek a saját, bevált módszerük alapján számolják a költségeket. Két költségkategóriát határoznak meg: az OPEX-et és a CAPEX-et. A költséganalitikánál az egyes költségelemek sem tisztázottak, nem tudják mit tartalma. A szervezetek nem tudják, hogy amit elkészítenek, az pontosan mennyibe is kerül. Az ITIL támpontod ad, azokra a költségelemekre, amire figyelni kell, mint például: licenc költség, amortizáció. Van ajánlás, de nem kielégítő és ez nehéz téma.

3. Hasznosnak ítéli meg, ha lenne egy olyan nyilvántartás, ahol az alkalmazásokhoz analitikusan van rendelve az informatikai költségek. Költségallokáció van már a szervezetben, azonban folyamatosan fejlesztésre szorul. Az informatikai költségeket nem a CMDB-ben, hanem Excelben tartják nyilván. A költségallokációs modellhez minden évben készül a CMDB aktuális adatai, információi alapján egy hozzárendelés. Ha képezne a szervezet üzleti folyamat alapján alkalmazás portfóliókat és úgy látná részletesen az informatikai költségeket alkalmazásonként, akkor ez hasznos lehetne. Ehhez természetesen menedzsment egyetértés kell.

4. Több olyan helyen is dolgozott, ahol tervezték, hogy alkalmazás szinten láthatóak legyenek az informatikai költségek, azonban ezek megvalósítása elmaradt. A

jelenlegi munkahelyén már sikerült a költségeket két kategóriára bontani: CAPEX és OPEX -ra. Bonyolult volt szétszedni, hogy milyen költségek hogyan tartoznak egy szolgáltatáshoz. Több ponton módosított ITIL módszer alapján készítették, de a megvalósítás hiányosra sikerült. Összességében nem sikerült megvalósítani az integrált nyilvántartást.

5. Az informatikai pénzügyi nyilvántartás két oldalról is megközelíthető. Nagyvállalatoknál vagy központilag van nyilvántartva, vagy két helyen. Az informatika beruházásokból indulnak ki, hogy szükségesek információk az informatikai költségekről. Jellemző, hogy a nagyvállalatoknál már van IT controlling. Szervezeti kérdés, hogy az IT kontrolling a CIO alatt, vagy az üzleti terület pénzügyi osztályán kezelik. A pénzügyi osztályokon kezelt IT controlling-nál például fontos az, hogy az értékcsökkenés elszámolása esetén az informatikai alkalmazás aktiválásának a dátumát is figyelembe kell venni. A legtöbb helyen a pénzügyi analitika nem pontos. Sok helyen a belső fejlesztéssel megoldott költségekre kiválasztanak egy rendszert a komponenseivel együtt és arra aktiválják a fejlesztési költségeket. Ez pénzügyi és informatikai szempontból is pontatlan, hibás. Olyan szoftverrel, informatikai megoldással nem találkozott, ahol integráltan volt kezelve az informatikai alkalmazás és a hozzárendelhető informatikai költségek analitikusan. A két „nézet" összekapcsolása nem történik meg a nagyvállalatoknál. Pénzügyileg CAPEX vagy OPEX alá sorolják az informatikai költségeket.

6. Alkalmazás szinten találkozott beruházás, karbantartási költségek nyilvántartásával. Pontosan látták melyik alkalmazásra mennyit költöttek. A probléma inkább ott van, hogy ez nincs összekapcsolva az üzleti értékkel. Az ITIL használatával rá lesznek kényszerítve a szervezetek arra, hogy készítsenek informatikai pénzügyi költségnyilvántartást. A költség-érték kapcsolatrendszer megértése azonban bonyolult feladat.

7. Az informatikai szolgáltatásokhoz rendelhető költségeknek a nyilvántartása sincs megoldva, így az informatikai alkalmazásokra fordított költségkeretek sem. A legtöbb nagyvállalatnál szükség lenne az alkalmazás portfólióra, ezáltal az informatikai költségek nyilvántartására, de nem látott még jól működő modellt. A legtöbbször a különböző terület illetékesei olyan számokat használnak, elemeznek, amik nem is valósak. A napi szintű nyilvántartás, felülírása az informatikai költségnyilvántartásnak sincs megoldva.

5. kérdés: Informatikai kockázatok kezelése és ITIL

1. A kockázat az egyik leíró adat az alkalmazásokra a CMDB-ben. Három kockázati kategória van definiálva a CMDB-ben. A CMDB-nek ez a funkciója a saját fejlesztéssel lett megoldva, mivel a saját, szervezeti kockázatkezelési módszertanhoz kellett a rendszert illeszteni. Az alkalmazásokhoz elvégzik a kritikus besorolást, a dokumentációkat központilag tartják nyilván. A kockázati besorolás, illetve amit lehet látni a CMDB-ben, az egy részleges információ. Az informatikai kockázatok kezelése teljesen elkülönülten működik a szervezeten belül. Az ITIL ajánlást nem használja a szervezet az informatikai kockázatok kezelésére, tehát hiába tér ki erre, a szervezetnek más sztenderdeket, ajánlásokat is kell használnia. Részletesen az informatikai kockázatok kezelésére a COBIT és NIST ajánlásait használják. Az üzleti folyamatok kockázatait és a technikai kockázatokat pedig külön kezelik. Az alkalmazásokra vonatkozó kockázati besorolás megtörténik a szervezetben. Évente egyszer készítenek kockázati mátrixot. Azonban alkalmazás szintre nincsenek lebontva részletesen az informatikai kockázatok. Nincsenek az informatikai kockázatok listázva, tehát ami a CMDB-ben szerepel kockázati kategória, az nem egy részletes informatikai kockázatlista alapján készül. Részletes kockázat nyilvántartásra egy másik alkalmazást használnak. Azonban olyan jellegű kimutatás, ami az alkalmazásokat portfólióba sorolja és az informatikai kockázatokat is hozzárendeli alkalmazásszinten nincs. Az információk természetesen rendelkezésre állnak ehhez. Az ITIL és a többi ajánlás használhatóak valamennyire, hiszen előírják azt, hogy listázni kell a kockázatokat. Azonban a vállalati életben, a mindennapi működésbe nehéz adaptálni. Az alkalmazás támogatás mögött rengeteg kockázat van, ezek a kockázatok pedig a folyamatokban vannak jelen. Ha egy külső szállító fejleszt és támogat egy alkalmazást, akkor ott ki kell térni a szerződéshez kapcsolódó kockázatokra is, mint informatikai kockázat.

2.Az ITIL-nek vannak területei, ahol a kockázat, mint fogalom megjelenik és ezeknek a felmérése is. A kockázatmenedzsment az egy feladat, azonban ez egy külön szakma az informatikától függetlenül. Általános és főleg a biztonságra kitérő kockázat kezelés az nem jelenik meg az ITIL-ben, de hivatkozik rá. Az egyik problémát abban látja, hogy a szervezetek vezetőinek választani kell a sok ajánlás közül. A COBIT-nak van szolgáltatás menedzsment relevanciája is. A nagy megoldandó probléma, hogy lehet integráltan kezelni a sok különböző ajánlást. Az ITIL nem foglalkozik, csak érintőlegesen az IT biztonsággal. Fontos megemlíteni azt, hogy az ITIL alapvetően egy szolgáltatás

irányítási keretrendszer. Mindenképpen össze kell, hogy kapcsolódjanak a különböző területek. Szervezetekben az üzleti és informatikai egységek külön működnek. A keretrendszerek felhívják a szervezetek figyelmét, hogy szükséges a kockázatkezelés. Ha a szervezet csak ITIL-t vezetett be nem oldott meg mindent, hiszen az ITIL-t a szolgáltatás menedzselésre lehet alkalmazni, ezzel még a kockázatmenedzselés nincs megoldva.

3. A folyamatokhoz kapcsolódó kockázatok valamennyire megjelennek az IT incidenskezelésében. Dedikált, analitikus informatikai kockázatmenedzsment azonban nincs. Természetesen az informatikai kockázatok fajtái, típusai és kezelésük sokféle lehet. A működési kockázatra sok figyelmet fordítanak. Az információk egy részét a CMDB tartalmazza. A fő nyilvántartás külön van kezelve. A CMDB-ben lekérdezhető az informatikai alkalmazások életkora, de nincs egyedi kockázati besorolása valamilyen módszertan alapján. Pedig az elavult rendszerek sok veszélyforrást tartalmaznak. Igény lenne rá, hogy az alkalmazásokhoz rendeljék az informatikai kockázatokat.

4. Találkozott megoldásokkal az informatikai kockázatkezelésre. A megoldások kialakításánál figyelembe vették az ITIL-t, de gyakorlati használhatósága nem volt kielégítő. Tulajdonképpen az ITIL-nek egy részét, plusz valamilyen kockázat menedzsment ajánlásnak, sztenderdek egy részét alkalmazták. Olyannal, ami 100%-ig megfelelne a szabványoknak, nem találkozott. Tapasztalta, hogy egyes szervezetek bevezették az ISO 30001-et, és létrehozták a hozzá kötelező dokumentációt, a szerepköröket is. Azonban nem használták az ISO31000 szabványt a gyakorlatban. Igazából a lényeg az volt, hogy a cég mutatni tudja, hogy rendelkezik ISO31000 szabvánnyal.

5. Az informatikai kockázatokat a legtöbb szervezet figyelembe veszi, a compliance osztályok, szervezeti egységek foglalkoznak ezzel. A kockázat kezelésért felelős osztályoknál külön van IT kockázat kezeléssel foglalkozó egy-két szakember. Ezek a szakértők az alkalmazások működési kockázatát vizsgálták. A klasszikus IT szervezetek viszont az alap infrastruktúrák működési kockázataiból szoktak kiindulni és azt elemzik. Az informatikai kockázatok nincsenek lebontva alkalmazásokra. Nem lehet látni azt, hogy adott alkalmazáshoz milyen üzleti, technológiai, szervezeti kockázatok tartoznak. Összefoglaló nyilvántartás is csak auditok előtt készülnek. Excel táblázatba összegyűjtik

a szükséges információkat. Tapasztalata az, hogy nem használnak szoftvereket az informatikai kockázatok nyilvántartására, elemzésére.

6. Sok szabványok vannak a gyakorlatban az informatikai kockázatok kezelésére, de pontosan nem tudja mi alapján végezték a tevékenységeket. A szervezetek az informatikai kockázatokat informatikai dobozban kezelik, azonban ez nem helyes. Az informatikai kockázat az lényegében az üzleti kockázatnak a része. Az informatikai kockázat az üzleti kockázatnak a része. A cégek vezetésének abba az irányba kell lépnie, hogy az informatikai kockázatot együtt kezeljék az informatikai kockázatokkal. Amit az ITIL-t ajánl az jó alapnak, de az üzleti élet szereplői elzárkóznak ennek a megértésétől.

7. A legtöbb helyen az informatikai biztonság és információbiztonság elkülönül. Az informatikai kockázatok nyilvántartására Excel táblákat használnak. Az Excel tábla használata sok problémát okoz. Egy idő után eltűnik, vagy bekerül egy dokumentációba. Látott olyan nagyvállalatot, ahol dobozos szoftvert vásároltak azért, hogy támogassák az informatikai kockázatkezelést. A nyilvántartások inkább folyamatokra, például üzleti folyamatra, funkcionalitásra irányul. Ha bármilyen szempontból fókuszba kerülnek az informatikai kockázatok, akkor az infrastruktúrához rendelhető informatikai kockázatokat kísérik figyelemmel a szakemberek. Az ITIL egy ajánlás, csak egy ideális világban tudna jól működni.

6. kérdés: Elavult alkalmazások, mint kockázatok a szervezetben

1. A CMDB-ben lekérdezhetőek az elavult platformmal rendelkező informatikai alkalmazások Azonban a lekérdezésből nem látszik az, hogy melyik üzleti terület használja. A prioritás a mindennapi működés biztosítása és a hibák elhárítása ezeken a rendszereken.

2. Sok különböző alkalmazás nyilvántartást látott, ezekben szerepeltek.

3. Minden szempontból figyelmet fordítanak ezekre az alkalmazásokra, a szerződések, támogatás tevékenységek, helyi tudás és nem-tudás pótlása, addicionális beszállítók, külön katasztrófa-helyreállítási terv, megoldások terén. Az elavult alkalmazások cseréje költségigényes.

4. A jelenlegi szervezetben sok alkalmazáshoz még SLA sincs megkötve. A legtöbb szervezetben tudják mely alkalmazások elavultak.

5. A szervezetek a nyilvántartásoktól függetlenül tudják, hogy van-e ilyen alkalmazásuk és ez milyen kockázattal jár. A szó mögött beleértjük azt, hogy az informatikai alkalmazás az régi technológiával készült, illetve az is, hogy akik programozták az informatikai alkalmazást már nem elérhetőek. Természetesen találkozott olyan esettel is szakmai pályafutása alatt, hogy az elavult informatikai alkalmazást már nem lehetett működtetni. A személyek, akik programozták, azoknak a fele nem volt már elérhető. Az informatikai kockázatok közé tartozik ez is. A legtöbb esetben a szakemberek, akik programozták, vagy értene az elavult informatikai alkalmazás támogatásához a meglévő piaci ár, fizetés, juttatás többszörösét is elkérik. Ez pedig sok többletköltséggel jár. Konkrét példa, amivel találkozott, hogy az egyik nagyvállalatnál egy szakértő, aki programozott egy informatikai alkalmazást elment nyugdíjba. Csak úgy volt s csakúgy volt hajlandó folytatni alkalmazás támogatást, ha a juttatást nyugdíj kiegészítésként kapja meg. A szervezet rá volt kényszerítve, hogy fizesse a szakembert, mivel az egyik legnagyobb ügyfelüket szolgálták ki az elavult alkalmazással. Az ilyen jellegű problémákkal, kockázatokkal foglalkozni kell.

6. Nem volt különösebb elemzés ezekre az alkalmazásokra.

7. Nem kezelték kiemelten, speciálisan ezeket az alkalmazásokat.

7. kérdés: Alkalmazás portfólió menedzsment, informatikai kockázatkezelés

1. A biztonságot növelné, ha a szervezet integráltan látná az informatikai alkalmazásokat és az informatikai kockázatokat alkalmazásonként. A kérdés az, hogyan lehetséges ennek a nyilvántartásnak naprakészen tartani. Hasznos lehet, ha üzleti szolgáltatás szintig is látják az információkat. Összességében, ha a nyilvántartás integrált, naprakész, zárt rendszerként működik és menedzselhető, akkor az architektúra tervezésben, az incidens kezelésében, a gyökér okoknak a megtalálásában, és az hatás elemzésben tud segíteni. Azonban sok erőforrást igényel a kialakítása.

2. Léteznek és használnak kimutatásokat, riportokat az incidensekről, érintett rendszerekről. Az információk összegyűjtésére a kimutatásokhoz sok időt kell szakítani. Nincs integráltan kezelve az informatikai alkalmazásokhoz tartozó kockázat. Több rendszerből gyűjtik össze az információkat. A kockázatokból eredő veszteség számszerűsítése is nyitott feladat. Az első lépés az üzleti folyamatok feltérképezése lenne, hiszen az informatikai szolgáltatások mögött kellene látni az üzleti szolgáltatásokat.

Ezután egy integrált képet kapna a szervezet az üzleti folyamatok alapján az informatikai alkalmazásokról is. Ha az alkalmazás portfólióhoz nyilván lenne tartva az informatikai kockázat, pénzügyi információkkal, növelné a biztonságos működést. Jelenleg nincs ilyen nyilvántartás a szervezetben. Megállná a helyét, ha a menedzsment is támogatná és az erőforrások biztosítva lennének hozzá. A mindennapi munkát támogatná, előnyös lenne, ha lenne egy integrált nyilvántartás.

3. Igény van a szervezeteknél arra, hogy integráltan lássák az alkalmazás portfólió menedzsmentet és az informatikai kockázatokat. Azonban a legtöbb kezdeményezés, javaslat már felsővezetői szinten nem került elfogadásra. Többnyire manuálisan létrehozott mátrixokat generálnak a szervezetek, ahol a sorokban a konfigurációs elemeket, költségeket sorolják. A mátrix az oszlopai, ahol kockázati besorolásokat kellene hozzárendelni az elemekhez azok már üresek, nincsenek azonosítva. Ahol jelenleg dolgozik ott már készítettek egy olyan nyilvántartást, hogy látják mi szerepelt a listán és mennyibe kerül. Le is tudják bontani osztályszintig. Viszont az utolsó lépés hiányzik, hogy ennek a kockázatnak az átadása nem történik meg. Konkrét példa, hogy szolgáltatásokhoz nincs SLA (Service Level Agreement) kötve. Tisztában vannak vele, hogy nem szabad megállni, folytatni kell a munkát, és az informatikai kockázatokat figyelembe kell venni.

4. Több szervezetnél is látta azt, hogy voltak valamilyen kockázati besorolások az informatikai alkalmazásokhoz. A probléma ott kezdődött, hogy amikor a menedzsment elé került a kockázati lista, akkor nem foglalkoztak vele. Ameddig működik egy informatika alkalmazás, addig nincs jelentősége az informatikai kockázat listának. Alapvetően a menedzsment támogatása hiányzik mindenhol az informatikai kockázat lista készítéshez. A legtöbbször a kockázat mátrixban a sorok megvannak, de az oszlopok üresek, amiben szerepeltetni kellene a kockázati besorolásokat. Hasznos lenne a szervezeteknek az integrált nyilvántartás.

5. Munkája során a gyakorlatiban nem találkozott olyannal, ahol integráltan tartották volna nyilván az informatikai alkalmazásokat portfólióba sorolva, hozzárendelve az informatikai kockázatokat. Hasznos lenne, ha lenne a szervezeteknél egy ilyen központi nyilvántartást. Beleértve az alkalmazás meghibásodási valószínűségét, vagy akár az alkalmazást támogató szakértőket is figyelembe venni, mint egy kockázati tényező, valószínűségi értékkel. Így létrejöhetne minden alkalmazásra egy kockázati

mátrix. Amivel találkozott, azok a kockázati besorolások, tényezők csupán az infrastruktúrára voltak meghatározva, Excelben, tehát nem szoftverben nyilvántartva. A megközelítés azért is jelent problémát, mert a felhasználókat az informatikai alkalmazás érdekli, amit nap, mint, nap használnak, nem az infrastruktúra. A legtöbb helyen, ahol informatikai kockázatokat mérnek, addig jutnak el, hogy mennyi az alkalmazás kiesésnek a valószínűsége. Probléma az is, hogy az informatikai kockázatokról alatt a legtöbb szervezetben a DRP-t (Disaster Recovery Plan) és -t (Business Continuity Planning) értene. Ez nem elégséges. A pénzügyi szektorban lévő auditok során is ezt a kettőt figyelik és elegendőnek találják a meglétét az auditok során. Talán részletesebb nyilvántartás lehet olyan szervezeteknél, ahol az ISACA szakemberei megfordulnak.

6. Az integrált nyilvántartás meglétére jó lenne, ha érkezne igény az üzlet részéről. A cég vezetése valós képet kapna a helyzetről egy integrált nyilvántartással. Valódi információkra van szükség. A kérdés azonban ott van, hogy melyik terület, egység finanszírozná meg a nyilvántartásnak a létrehozását.

7. Analitikus nyilvántartással, ahol látni lehetett az informatikai alkalmazásokhoz tartozó informatikai kockázatokat még sehol sem látott. Igény lenne rá, a kérdés mennyi időt vesz igénybe a létrehozása és mire van szükség a folyamatos karbantartásához.

8. Kérdés: Egyéb problémák, javaslatok

1. A legnagyobb probléma az, hogy nem alkalmas egy ajánlás és szabvány sem arra, hogy teljesen lefedje az informatikai szolgáltatást, illetve a kockázatok kezelését. Sok különböző keretrendszert, ajánlást, szabványt kell egyszerre használni. Ha a technikai kontrollokon van a hangsúly, akkor az ISO szabványcsalád, vagy az NIST alkalmas a hozzárendeléshez. Az informatikai kockázatkezelésre is két szabványt használnak. Az egyik a COBIT, a másik a NIST. A COBIT például nem alkalmas az elemi kockázatok felmérésére.

2. Az ITIL-nek vannak hiányosságai. Az IT stratégia jellegű dolgok, amik megjelentek az ITIL-ben kifejezetten a nagy szervezetekre, nagy informatikai személyzetekre vannak kitalálva. Sokan az ITIL-ről és COBIT-ról beszélnek az utóbbi 10 évben, azonban az igazság az, hogy az alapok nagyon sok helyen nincsenek úgy lefektetve, hogy arra aztán rá lehessen építeni egy magas szintű szolgáltatás menedzsmentet. Ha egy kis összehasonlítást teszünk az ITIL és COBIT között, akkor a COBIT valamennyire hasznosabb, mint az ITIL. A COBIT konkrétan leírja, hogy adott

helyzetekben az egyes tevékenységeket milyen sorrendben kell végrehajtani és annak mi lesz az eredménye. Az ITIL nem törekszik ebbe az irányba. .Ha készítünk egy összehasonlítást, akkor a COBIT előző verziójáig mindig használhatóbb volt az ITIL. Amit problémának érez az, hogy az ITIL nagyon sok olyan követelményt, folyamatot fogalmaz meg, aminek van menedzsere, végrehajtási rendje. Ha egy szervezet eleget tenne teljesen az ajánlásoknak, akkor legalább 200 fős szolgáltató szervezetet kell kialakítani. Az egész szakmának problémát okoz, hogy ennyi szabvánnyal és ajánlással kell foglalkozni. Rendkívül bonyolulttá és összetetté vált az informatika. Ma már nincs olyan személy, aki mindenhez ért és átlátja az egész IT-t. A szervezetek széttagoltan működnek. Menedzsment szinten egységes gondolkodásra lenne szükség.

3. Az ITIL a szolgáltatás oldalról indul ki, ami elég sokat sérült 2008-tól kezdve. A szolgáltatás alapú megközelítés kezdi érvényét veszteni. A gazdasági válság óta egyre nagyobb prioritás a projektek szállítása. Az informatikai folyamatok **módszertan** szerinti működése folyamatosan háttérbe szorult. A hangsúly az üzleti igények szállításán van, nem az informatikai folyamatok szervezésén, vagy bármilyen ajánlás alapján való működésen.

4. Az ITIL, mint általános ajánlás jó, viszont amikor egy konkrét igény érkezik menedzsment szintről, akkor már nem lehet használni. Egy példán keresztül szemléltetve. Ha az adatokat felhőben kellene tárolni, akkor nincs definiálva, hogy ott milyen kockázatokat kell figyelembe venni. A példán keresztül megértve az ITIL nem ad útmutatást arra vonatkozóan, hogyan tud az informatika teljesen biztos lenni abban, hogy minden kockázatot feltárt, számba vett. A kockázatok nyilvántartásának a módjára nem ad ajánlást, túl általánosan fogalmaz.

5.Probléma a legtöbb szervezetnél, hogy az IT biztonságot és az informatikai biztonságot együtt kezelik. A kérdés, hogyan lehet egyszerre definiálni a szabályokat meg ellenőrizni is. Nagyobb vállalatoknál a biztonságrészleg foglalkozik kockázatelemzéssel, monitoringgal, controllinggal és elkülönítik az informatikai szolgáltatástól, üzemeltetéstől. Alapvető kérdésre, ami a témához szorosan kapcsolódik: hogy például holnaptól egy szabályozásváltozás miatt, vagy egy új üzleti piaclehetőség miatt megváltoztatnánk egy funkciót egy adott alkalmazáson, vagy bevezetnénk egy új funkciót, ez milyen módosításokkal jár és ez mennyibe kerülne. Ez egy alapvető és egyszerű üzleti kérdés, azonban, mivel nincsenek integrálva az egyes folyamatok,

rendszerek, lassan tud az IT válaszolni. A válasz pedig nem elég pontos. Megnehezíti a dolgot, ha a folyamatba külső beszállító is be van vonva. A külső beszállítók kihasználva a helyzetüket nem adnak reális pénzügyi válaszokat a fejlesztési igényükre.

6. Az üzleti folyamatok automatizálása egyre népszerűbb, azonban ehhez az ITIL ajánlásai nem igazodnak. Az ajánlások inkább arra épülnek, hogy végfelhasználók vannak a folyamatokban és nem robotok.

A legtöbb szervezetben alkalmaznak az ITIL mellett más keretrendszert is. A legelterjedtebb a COBIT. Munkája során csupán egy szervezetben találkozott azzal, hogy nagyon jól tudták alkalmazni és implementálni a szolgáltatásokra a COBIT-ot. Azonban ez a cég informatikai szolgáltatást nyújtott. A COBIT az alkalmazások nyilvántartására nem alkalmas, ezért az alkalmazások menedzsmentre az ITIL-t használják.

KÖSZÖNETNYILVÁNÍTÁS

Köszönettel tartozom mindenkinek, akik támogattak, hogy elkészítsem a PhD értekezésemet.

Dr.Michelberer Pál Úrnak, az Óbudai Egyetemről, aki konzulensként támogatott.

Dr. Velencei Jolánnak, aki tanácsaival, meglátásaival sokat segített a disszertáció elkészítése alatt.

Volt munkatársamnak, Laza Sándornak a szakmai lektorálásért.

Hálás köszönettel tartozom az elhunyt édesanyámnak, aki végig támogatott, unokája, Balázska felügyeletével 2 éven keresztül. Külön hálával tartozom a férjemnek, aki sokat vigyázott a gyerekekekre. Valamint a férjem édesanyjának is hálás vagyok. Sokat támogatott két gyerekfelügyelő, Berki Petronella és Szemőkné Farkas Mária, hogy időm legyen a kettő 4 év alatti gyermekeim mellett az értekezés írására.