Pannon Egyetem

Gazdálkodás- és Szervezéstudományok Doktori Iskola

Spilák Viktor

Szervezeti kultúra, vezetői szerepek hatása az információbiztonsági kiválóságra és a felhő alapú megoldások alkalmazására

Doktori (PhD) értekezés

Témavezető: Dr. Kosztyán Zsolt Tibor

DOI:10.18136/PE.2020.737

Veszprém

2020.

Értekezés doktori (PhD) fokozat elnyerése érdekében

a Pannon Egyetem Gazdálkodás- és Szervezéstudomány

Szervezeti kultúra, vezetői szerepek hatása az információbiztonság kiválóságra és a felhő alapú megoldások alkalmazására

Az értekezés doktori (PhD) fokozat elnyerése érdekében készült a Pannon Egyetem Gazdálkodás- és Szervezéstudományok Doktori Iskolája keretében

Gazdálkodás- és Szervezéstudományok tudományágban

Írta: Spilák Viktor

Témavezető/i: Dr. Kosztyán Zsolt Tibor

Elfogadásra javaslom (igen / nem)

…….

(témavezető/k)

Az értekezést bírálóként elfogadásra javaslom:

Bíráló neve: …..... …..... igen /nem

…….

(bíráló)

Bíráló neve: …..... …..... igen /nem

…….

(bíráló)

A jelölt az értekezés nyilvános vitáján ….....%-ot ért el.

Veszprém/Keszthely, …….

(a Bíráló Bizottság elnöke)

A doktori (PhD) oklevél minősítése….....

Veszprém/Keszthely, …….

(az EDHT

Tartalomjegyzék

Ábrajegyzék

Táblázatjegyzék

Kivonat

Az információs technológiák és az általuk szavatolt biztonság napjainkra kritikus szerepet töltenek be a szervezetek mindennapi életében, és nagyban képesek támogatni azok sikerességét. Éppen ezért is fontos foglalkozni azzal, hogy a szervezet és annak vezetése hogyan hat a működés egyes területeire, beleértve az információbiztonságot is. Sok esetben nem a befektetett energián és erőforrásokon múlik csupán a kialakult biztonsági szint egy szervezeten belül, hanem az ott dolgozók, a felelős vezetés is képes előremozdítani, vagy hátráltatni annak működését.

A szervezetek igyekeznek minél kevesebbet költeni az informatikai szolgáltatásokra, mivel azokra gyakran, mint szükséges rosszra tekintenek. Ilyen esetben előkerülnek az olyan új technológiák, amelyek csökkenő költségeket és hatékonyabb működést hirdetnek. Az elmúlt 5 évben a felhő alapú megoldásokra, mint az IT szent galljára tekintettek pont azért, hogy képes egy alacsony költségekkel, megosztott infrastruktúrán úgy működni, hogy a korábbi óriási beruházások elkerülhetőek. Mégis sok szervezet kultúrája, dolgozói, vagy egyáltalán a vezetés nem nyitott még az ilyen típusú megoldásra. Tapasztalható azonban olyan is, amikor a vállalatok túlzott lelkesedést mutatnak anélkül, hogy felmérnék egy ilyen lehetőség használatának valódi kockázatait.

Kutatásom elsődleges célja ezért feltárni, hogy milyen hatást gyakorol a szervezet kultúrája és vezetői az IT meghatározó területeinek működésére. A szervezeti kultúra, vezetői szerepek, információbiztonság és a felhő szolgáltatások vizsgálata korábban közös modellben nem történt meg, melynek hiányában nem volt arra lehetőség, hogy a hatásokat egy rendszerben vizsgálják és megértsék. Kidolgoztam egy olyan új modellt (kiemelt hangsúlyt fektetve az információbiztonsági kiválóságra és a felhő alapú megoldásokra), mely segítséget nyújt a vizsgálni kívánt hatás feltárásában.

Kutatásomban a szervezeti kultúra és vezetői szerepek információbiztonságra és felhő alapú megoldások alkalmazására gyakorolt hatásaira fókuszáltam és a kvantitatív és kvalitatív vizsgálat eredményei alapján kimondható, hogy a szervezeti kultúra és vezetői szerepek befolyással vannak a szervezet információbiztonsági szintjére. Igazolásra került, hogy a Piac és Hierarchia típusú szervezeteknél az információbiztonság szignifikánsan fejletteb, mint a Klán és Adhokrácia esetében, továbbá a Koordinátor, Direktor, Producer és Monitor fejlettebb infomrációbiztonsággal rendelkező szervezetet menedzselnek, mint a Bróker, Innovátor, Mentor és Facilitátor vezetők. A felhő alapú megoldások alkalmazása esetében szinten kimutatható hatás a szervezeti kultúra és vezetői szerepek irányából, ahol a Klán és Adhokrácia szervezeti kultúrák, valamint az Innovátor, Bróker, Mentor és Facilitátor vezetők kedveztek ezen alkalmazások használatának.

Abstracts

Information and communication technologies and security provided by them have critical role in organisations' everyday life and they are able to support their success in large scale. Therefore, it is crucial to deal with that how effect an organisation and its leadership on certain field of operation including information security. In many cases it doesn't depend on the invested energy and sources the developed security level within an organisation but its workers and responsible management are able to move forward or hinder the lifting of security level.

Organisations are eager to spend less money on information technology services because they consider them as "necessary evil". In these cases, such new technologies emerge which declare diminishing expenses and more effective working. In the years past they looked on cloud base solutions as "Holy Grail" of information technology because they can operate at small cost on shared infrastructure on such way huge early investments are avoidable. Nevertheless culture, workers even management of many organisations don't have an open mind on this sort of solutions. It might be experienced when companies present exaggerated enthusiasm without assessing real risks of using these opportunities.

Primary goal of my research is to reveal what effects have organisational culture and its managers on the working of defining fields of information technology. Examining organisational culture, leadership roles, information security and cloud base solutions didn't happen in a common model earlier. In absence of it there weren't any possibilities to examine and understand its effect in the same system. I have elaborated a new model (focused on information security excellence and cloud base solutions) which helps to unveil the desired effects.

During my research I focused on effects on information security of organisational culture and leadership roles as well as using cloud base solutions and results of quantitative and qualitative examinations it might be said organisational culture and leadership roles have effect on information security level. It has been verified that Market and Hierarchy type organisations have more advanced information security than Clan and Adhocracy ones. Moreover Coordinator, Director, Producer and Monitor types manage more developed information security organisations than Broker, Innovator and Facilitator managers. In case of using cloud base solutions effects are verifiable from direction of organisational culture and leadership roles where Clan and Adhocracy organisational cultures as well as Innovator, Broker, Mentor and Facilitator managers favoured using these applications.

Köszönetnyilvánítás

Köszönetet szeretnék mondani témavezetőmnek, ***Dr. Kosztyán Zsolt Tibornak***, aki kutató munkám teljes időszaka alatt minden segítséget megadott és folyamatosan motivált annak érdekében, hogy kutatásom céljait elérhessem.

Köszönöm a Vezetés és Szervezeti tanszék minden oktatójának, kutatójának és munkatársának a támogatását és felkészültségét, mely nélkül nem tudtam volna elvégezni munkámat.

Ezúton is szeretnék köszönetet mondani ***Szüleimnek***, hogy segítettek, hogy munkámat a lehető legjobb tudásom szerint végezhessem el, nélkülük úgy érzem, minden nehezebb lett volna.

Végül szeretném megköszönni ***kedvesemnek és minden barátomnak*** a segítségét, akik mindvégig támogatták a kutatásba vetett hitemet és a folyamatos megismerés, az új dolgok létrehozása iránt érzett olthatatlan vágyamat!

1 Bevezetés

Az információs technológiák és az általuk szavatolt biztonság napjainkra kritikus szerepet töltenek be a szervezetek mindennapi életében, és nagyban képesek támogatni azok sikerességét (Yang , et al., 2015; Kovács & Krasznay, 2017). Ezen technológiák segítik az ügyfelek által támasztott elvárások, igények érzékelését és megértését (Roberts & Varun , 2014). Az üzleti világban lezajlódó gyors változások, a start-up vállalatok megjelenése, folyamatos fejlődése kihívást jelent a piac minden szereplőjének (Kollman Tobias, et al., 2015). Az elkövetkező években ennek hatása tovább fog erősödni, mivel az európai start-up-ok iránti érdeklődés az amerikai piac irányából is egyre erősödik. A létrehozott termékek és szolgáltatások fejlesztése és terjesztése egy erős felvásárló esetén további támogatást kaphat (Pisoni & Onetti, 2018). Korábban a felsővezetés nem értette igazán az IT biztonság jelentőségét. Mára azonban a kérdés már kicsit szofisztikáltabb és a miért szükségesből átalakult a hogyan és pontosan milyen szigorú információbiztonsági intézkedések irányába (Szádecky, 2016). A menedzsment célja, hogy a lehető legkevebbet fektessen az IT rendszerekbe (Szádecky, 2016). Ilyen körülmények között még súlyosabb, hogy a vezetők nincsenek tisztában azzal, hogy a szervezeti kultúra és vezetői szerepek milyen hatást képesek gyakorolni az információbiztonságra és a felhő alapú megoldások alkalmazására (Spilák & Kosztyán, 2013).

1.1 A kutatás aktualitása és jelentősége

A kutatás időszerűségét alátámasztja továbbá, hogy az intenzív árverseny esetén a vállalatok szenvedhetnek a decentralizált működéstől (Pekgünk, et al., 2016), valamint a technológiai előnyök képesek új lehetőségeket biztosítani annak érdekében, hogy rövidítsék termelésük/szolgáltatásuk biztosításának átfutási idejét (Marchese, et al., 2015). Az informatika mára olyan eszközzé vált, amely Marchese, Crane, Haley megállapítását is figyelembe véve képes hozzájárulni egy szervezet versenyképességéhez, illetve hatékonytalan működésének következtében ellentétes hatást kifejteni. A szervezetek igyekeznek a technológiákban rejlő lehetőségeket és kapacitásokat úgy kiaknázni, hogy közben a felmerülő költségeket minimalizálni vagy legalább megosztani tudják. Ezért a nagyvállalati környezetre jellemző a közös használatú erőforrások létrehozása és üzemeltetése. Ezáltal a meglévő szervereket felbontják kisebb alkotó elemekre, úgynevezett virtuális gépekre, így pedig egy időben a korábbiakhoz képest sokoldalúbb felhasználásra nyílik lehetőség (Fehér, et al., 2016). A magas rendelkezésre állást igénylő megoldásokhoz használható rendszerek esetében kritikus jelentőséggel bír a pontos tervezés, valamint a későbbi költséghatékony üzemeltetés és stabil működés megléte (Metzler, 2009).

Korábban kevés olyan kutatás történt, ami a szervezeti kultúrát, vezetői szerepeket, információbiztonsági kiválóságot és felhő alapú megoldásokat együttesen vizsgálta volna. Azonban ezen területek összekapcsolása segíthet abban, hogy megértsük, hogy a szervezeti kultúra és vezetői

szerepek milyen hatással vannak az információbiztonsági szintre, továbbá milyen felhő alapú megoldások alkalmazását támogatják.

Munkám további részeiben áttekintem a kutatáshoz kapcsolódó szakirodalmakat, bemutatom a létrehozott modellt. Ismertetem kutatásom során lefolytatott esettanulmányt, melynek tanulságait felhasználva elvégeztem a kérdőíves lekérdezést a kiválasztott mintán. Összegezem a levonható következtetéseket, illetve meghatározom munkám további fejlesztési lehetőségeit is.

1.2 Kutatási célok

A kutatás célja, hogy a menedzsment által vizsgált kultúra dimenziók és vezetői szerepek kérdéskörét kibővítsem és megvizsgáljam, hogy milyen hatással vannak ezen dimenziók az egyes szervezetek működését nagyban befolyásoló informatikai biztonságra és felhő alapú megoldások alkalmazására. Nagyon fontosnak tartom az IT minden területét, mellyel számos kutató részletesen foglalkozott, azonban a felhő alapú megoldások alkalmazásának vizsgálatát modellembe azért kezeltem kiemelten, mivel úgy gondolom, hogy ez egy olyan szegmense az információs rendszereknek, amely menedzsment szempontból nem volt korábban vizsgálva annak ellenére, hogy igen jelentős érdeklődés övezi napjainkban is. Ezen túlmenően meg kellett tartanom az egyensúlyt az egyes tudományterületek között, hogy kutatásom információs rendszerek és kiberbiztonság szempontjából ne kerüljön túlsúlyba.

Kiemelten fontos volt, hogy létrehozzak egy olyan információbiztonsági és felhő alapú megoldások alkalmazásának érettségét meghatározni képes modellt, mely képes azon túl, hogy felmérje a szervezetek helyzetét, alkalmas legyen megteremteni a szervezeti kultúra és vezetői szerepek információbiztonságra és felhő megoldások alkalmazására gyakorolt hatásának vizsgálati lehetőségét is.

Meggyőződésem, hogy a szervezeti kultúra és a vezetői szerepek nagy befolyással bírnak arra, hogy milyen a vállalat információbiztonsági szintje, valamint milyen felhő alapú megoldásokat használ. Az információbiztonság és a felhő megoldások ilyen aspektusú vizsgálata azért izgalmas, mivel számos irodalmi értekezés foglalkozik külön-külön ezen területekkel, azonban komplexen, egy rendszerbe foglalva nem tekintik át azokat. Kutatásom során nem célom a szakirodalomban található modellek egyértelmű felhasználása, mivel azok számos hiányossággal, a magyar viszonyok között nem alkalmazható tulajdonságokkal bírnak, ezért elengedhetetlennek tartom, hogy egy olyan új modellt hozzak létre, mely képes a vizsgált dimenziókat egyetlen rendszerben egyesíteni és értelmezni. Ezen keretrendszer indokoltását az adja, hogy segítségével a felsővezetés egyértelmű képet kap arról, hogy az információbiztonság és/vagy a felhő alapú megoldások alkalmazásának előmozdítását mely szervezeti kultúra és vezetői szerep képes támogatni. Ezáltal pedig a rájuk jellemző tulajdonságok előtérbe helyezésével már nem csak pénzügyi eszközökkel képesek a területeket fejleszteni, hanem csupán szervezeti kultúra és vezetői szerepek átalakításával is érhetnek el pozitív változásokat.

1.3 Kutatási kérdések

Célom volt, hogy feltárjam a kultúra dimenziók és vezetői szerepek által az információbiztonságra és felhő alapú megoldások alkalmazására gyakorolt hatásait.

- K1: Milyen vezetői szerepek mellett fejlett az információbiztonsági kiválóság?
- K2: Milyen szervezeti kultúra kedvez az információbiztonsági kiválóságnak?
- K3: Milyen vezetői szerepek megléte támogatja a felhő alapú megoldások alkalmazását?
- K4: Milyen szervezeti kultúra nyitott a felhő alapú megoldások alkalmazására?

1.4 A disszertáció felépítése

A disszertáció felépítése a társadalomtudományok területén elfogadott logikai sorrendet követi.

Az első, bevezető fejezet a kutatás aktualitását, jelentőségét, majd a kutatási célok pontos meghatározását tartalmazza. Ezt követően a témához kapcsolódó legfontosabb szakirodalmakat tekintem át. Részletesen foglalkozok a szervezeti kultúrához és vezetői szerepekhez tartozó alapvető fogalmakkal, kultúra és vezetői típusokkal és azok összehasonlításával. Ennek eredményeként kiválasztom a kutatásom szempontjából megfelelő szervezeti kultúra és vezetői szerepek modellt. Az irodalmi áttekintést az információbiztonsági és felhő megoldások alkalmazásával kapcsolatos modellek áttekintésével folytatom.

Az elméleti rész zárásaként meghatározom (alapozva a korábbi modellek áttekintésére) az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazásának vizsgálatához szükséges területeket.

A harmadik fejezetben az irodalmi áttekintés alapján megfogalmazom a kutatás fogalmi keretét. Megfogalmazom a kutatás hipotéziseit és bemutatom a kutatási modellemet, mely magába foglalja már mind a négy tudományterületet. Majd azoknak a kvantitatív és kvalitatív módszereknek a kifejtésével folytatom, melyek a hipotézisek helytállóságának ellenőrzéséhez szükségesek.

A negyedik fejezetben mutatom be az empirikus kutatást, melynek részként a kutatási folyamatot határozom meg. Meghatározom a vizsgálati minta kiválasztása során figyelembe vett kritériumokat. Bemutatom a kvalitatív és kvantitatív vizsgálat során kiválasztott pontos mintát és annak összetételét.

Az ötödik fejezetben ismertetem a kvalitatív vizsgálat eredményeit tartalmazó esettanulmányt, a hozzá kapcsolódó kutatási kérdéseket és az eredményekből levonható következtetéseket, mellyel célom volt, hogy kutatásom fókuszát és mélységét helyesen válasszam meg és szűkítsem a kvantitatív vizsgálat során tárgyalni kívánt területeket. Az eredmények értékelésének következő szakaszában a kvantitatív vizsgálatot tekintem át, melynek részeként ismertetem az egyed változókra vonatkozó statisztikai

adatokat, a változók mérhetővé tételéhez szükséges eljárásokat, valamint a változók közötti kapcsolatokat. A megkapott individuális eredményeket felhasználva vizsgáltam a szervezeti kultúra, vezetői szerepeket hatását az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazásának tekintetében. A feltárt kapcsolatok elemzésével rávilágítok arra, hogy milyen összefüggések vannak a domináns szervezeti kultúra, vezetői szerepek és az információbiztonsági kiválóság, valamint a felhő alapú megoldások alkalmazása között. Ezt követően elvégzem a hipotézisek helytállóságának vizsgálatát és megfogalmazom a kutatási téziseket.

A hatodik fejezetben a kutatási eredmények értelmezése következik és megválaszolom a kutatási kérdéseket. Meghatározom munkám gyakorlati felhasználásának lehetőségeit és további kutatás irányokat jelölök ki.

Az utolsó fejezet az elvégzett munka rövid áttekintését adja, mely egyben szintetizálja a megkapott eredményeket.

2 Szakirodalmi feldolgozás

A huszonegyedik században és legfőképpen évtizedünkben átalakulóban van az informatikai megoldások piaca. Olyan új termékek és szolgáltatások komplex ökoszisztémái vannak jelen, melyek nemcsak a piaci viszonyokat, hanem a szervezetek működését is nagyban megváltoztatják. Az üzemeltetés korábban szokványosnak, mindennapinak nevezett feladatai tűnnek el, miközben teljesen újak jelennek meg, melyek gyakran eltérő kompetencia meglétét igénylik. A szervezetek korábban élesen meghúzott határvonalai eltűnőben vannak, a munkatársak saját eszközeikről szeretnék elérni a céges levelezést, dokumentumokat.

Munkám további részében a kutatási kérdéskörökre fókuszálva a témával foglalkozó korábbi eredményeket, irodalmakat tekintettem át, mely két részre lehet osztani. Az első részben a szervezeti kultúrával, vezetői szerepekkel kapcsolatos szakirodalmakat mutattam be, míg a második szakaszban az információbiztonságot meghatározó, befolyásoló tényezőket, valamint az informatikai rendszereket korszerűsítő felhő megoldásokat tanulmányoztam.

2.1 Szervezeti kultúra és vezetői szerepek

A témával foglalkozó kutatások, irodalmak sokrétűsége is jól mutatja az akadémiai érdeklődést a vállalati kultúra iránt (Oju, 2009). A kultúra fogalmának meghatározása több aspektusból közelíthető meg és nincs egységesen elfogadott értelmezés, Kroeber és Kluckhohn több mint 160 definíciót gyűjtött össze (Kroeber & Kluckhohn, 1978). A kultúra meghatározása és fejlesztése kiemelkedő jelentőségű, ugyanis meghatározó alapja egy szervezet működésének, mivel a stratégiai tervezés önmagában nem képes a vállalat totális mozgósítására. Ahhoz szükség van a kultúrára is (Hax & Majluf, 1984). Számos modell született az évek során attól függően, hogy a kutatók milyen területeket tartottak fontosnak, illetve helyeztek a vizsgálat középpontjába (Balogh, et al., 2011). Korábban úgy vélték, hogy a szervezeti kultúra a siker legfontosabb eleme (Lippert, et al., 2015). Később ezt túlzónak ítélték, de abban továbbra is egyetértenek, hogy kulcsfontosságú szerepet játszik egy szervezet életében (Naranjo-Valencia, et al., 2011). Formálja annak vezetőjét, aki önmaga is hatást gyakorol arra, hogy milyen kultúra alakul ki a kollektíván belül (Gaál, et al., 2009). A kultúra megközelítések áttekintését azonban a kultúra fogalmának, annak szintjeinek, valamint az elemeinek tisztázásával kell kezdeni. A szervezeti kultúra mindig és mindenhol jelen van függetlenül attól, hogy annak vizsgálatával foglalkoznak-e az adott szervezet esetében. Fogalmának meghatározására számos törekvés történt a vezetéstudomány keretein belül is, azonban egyértelmű, egységesen elfogadott és használt kultúra definíció nem létezik. A kultúra megfogalmazásának sokszínűsége abból is adódik, hogy megjelenésének nagy része nem látható, így annak leírása nehéz (Lippert, et al., 2015). Ha egyszerűen szeretnénk fogalmazni, akkor a szervezeti kultúra nem más, mint a magatartások, értékek és normák, meggyőződések rendszere (Gaál, 1999). A szervezeti kultúrának számos funkciót tulajdonítottak eddig is és várhatóan a jövőben további olyan funkciók fognak megjelenni, amelyek a megváltozott munkastílusok miatt születnek meg. A

szervezet kultúra tehát nem más, mint azon elemeknek az összessége, amelyek egy szervezet megfelelő működéséhez elengedhetetlenek (Gaál, 1999).

Egy vállalat vezetése munkaadóként ügyel a jogi és szervezeti feltételekre, vezetőként fejleszti a munkavállalók képességeit, továbbá kultúra alakítóként támogatja az egyének igényeinek a kifejezésre jutását (Szabó & Dancsecz, 2009). Számos dimenzió mentén közelíthető meg a vezetés, valamint a vezetők feladatai (Lippert, et al., 2015). Ezen dimenziók a vezetői funkciók, a vezetői problémamegoldási folyamat, a vezetési stílus, a vezetési rendszerek és a vezetői szerepek (Dobák & Antal, 2016). Mivel a vezetői szerepek jelentősége kiemelkedő egy szervezet formálásban, ezért azt feltételezem, hogy szignifikáns hatással van az általam vizsgált területekre is. Így munkám során hangsúlyt fektetek ezen terület bevonására.

2.1.1 Szervezeti kultúra típusok összehasonlítása

Kutatásom során vizsgáltam a *Handy féle kultúra modellt,* mely az egyik leggyakrabban alkalmazott kultúra tipizálás és hazánkban is igen népszerű. Abból indult ki, hogy az eltérő tevékenységeket végző szervezetek eltérő kulturális sajátosságok jellemzik. Figyelembe kell venni alkalmazása során, hogy létrejöhetnek szubkultúrák is, amelyek erősíthetik, de gyengíthetik is a szervezet teljesítőképességét. Handy féle modell esetében meghatározott kultúra típusok nem minden esetben használhatók, mivel a szervezet tagjai gyakran rugalmatlanok, azaz hisznek abban, hogy ha valami jól működik az egyik kultúrában az jól fog a másikban is (Cacciattolo, 2014). Kutatásom során a Handy megközelítésében a jövő vizsgálatának hiánya jelenti a legnagyobb korlátot, mivel így későbbiekben nem nyílik arra lehetőség, hogy a vágyott kultúra figyelembevétele megtörténhessen. Ezáltal pedig alkalmatlan arra, hogy az időt, mint a változás egyik generálóját is figyelembe tudjam venni és megérthessem, hogy a szervezet szereplői mit tartanának a helyes iránynak. *Hofstade* a nemzetek közötti különbségeket dolgozta fel és állapította meg, hogy adott kultúrajellemzők kombinációja bizonyos szervezeti formák gyakori előfordulásával jár együtt (Lippert, et al., 2015; Hofstade, 2010). Jól használható kultúra modell a telekommunikációs szektorban, azonban vannak korlátai alkalmazásának. Mint minden nemzeti kultúra vizsgálat a kultúra határait a nemzeti határokkal veszi egybeesőnek (Török, 2017), ami nem megfelelő kutatásom során, ugyanis az általam későbbiekben vizsgálni kívánt szektor és vállalatok döntő része leányvállalat, így pedig információk elvesztését eredményezheti ez a megközelítés. Továbbá azt gondolom, hogy napjainkban már kevésbé jó irány a nemzeti határok szigorú értelmezése, mivel egy vállalat működésében sok esetben ez már ténylegesen eltűnt. Egy Magyarországon működő kínai vállalat legtöbb működési jellemzőjét otthonról hozzá és a helyi munkavállalók ehhez alakulnak és nem pedig alakítják. Így a megközelítést napjainkra kevéssé érzem helyesnek. A modell további hátránya, hogy technikailag bonyolult, így használata nehézkes (Mead, 1998). Célom, hogy olyan módszerrel tudjam vizsgálni a vállalatokat, amely könnyedén megismételhető, a felmérés folyamata pedig egyszerű. Vitatható pont továbbá, hogy az egyes dimenziókat az eltérő országok máshogy értelmezik, a modell

nem határozza meg a kontextust, így pedig az eredmények is torzulhatnak (Török, 2017). *Morgan féle kultúra modell* az alapján határozza meg a kultúrát, hogy a vezetők milyen módon tekintenek szervezetükre. Mechanikus kultúrában a szervezetet gépként fogják fel, azaz megbízhatóan és hatékonyan kell működnie, előre lefektetett célokat lehessen általa elérni. Ezzel ellentétben az organikus kultúra esetében, mint egy élő szervezetre tekintenek (Morgan, 2007; Balogh, et al., 2011). Morgan megközelítésének kritizálói (Jermier & Forbes, 2016; Kemp, 2016; Pinto, 2016) az empirikus felfogásra támaszkodva javasolják további metaforákkal bővíteni a modellt. Bírálják a mechanikus és organikus definíciót, mivel megfigyelés révén ezek szervezet és nem ember irányultságúak, így pedig elsődlegességük vitatható (Örtenblad, et al., 2016). Az általánosságban megfogalmazott kritikák Morgannel szemben kiemelik a személyi aspektus hiányát, ezért kutatásom során nehézkes lenne megteremteni a vezetői szerepekkel történő kapcsolatot. Továbbá azt gondolom, hogy ha egy modellben elhanyagoljuk a személyi tényezőt, akkor azzal egy nagyon fontos működési elem kerül ki a vizsgálatból, hiszen nem szabad elfelejteni, hogy az emberek személyes érzései egy vállalattal szemben nagyban befolyásolják tetteiket és teljesítőképességüket. *Trompenaars* szintén a kétpólusú dimenzióktól történő eltávolodást képviseli. Kluckhohn és Strodtbeck kategóriáiból indult ki és állította fel dimenzióit, amik 6 alapvető kérdésre vonatkoznak. Így szintén eltávolodik a Hofstede-i kétpólusú dimenzióktól (Török, 2017). Négy szervezeti kultúratípust határozott meg, melyek megmutatják a munkatársak véleményét a szervezet rendeltetéséről, céljairól és azon belül a saját szerepükről (Hampden-Turner & Trompenaars, 2006; Fekete - Berzsenyi, 2017). Trompenaars modell kritikája, hogy nem ismeri fel a személyiség jellemzők hatását a viselkedésre. Valamint Trompenaars és mások, mint pl. Hofstede azt vallják, hogy a vállalatoknak el kell ismernie a kulturális különbségeket, addig (Ohmae, 1999) és (Levitt, 2003) szerint a nemzeti határok csökkennek és a világot egy egészként kell tekinteni nem külön országokként eltérő kultúrával. Véleményem szerint 2020-ra az ilyen típusú megközelítések már nem aktuálisak, a globalizációval a vállalatok működéséből egyre inkább eltűnnek a lokális kulturális sajátosságok és a teljes vállalat, mint egy önálló, országokoz hasonló működést mutat saját szabályokkal, szokásokkal és értékrendekkel. Ezt pedig már nem befolyásolják az országhatárok. Azt gondolom, hogy ez mára elengedhetetlen ahhoz, hogy egy multinacionális nagyvállalat hatékonyan és egyáltalán kontrolállható módon legyen képes működni. Enélkül ugyanis csupán egy csoportban dolgozó, de egymástól elszigetelten létező országonkénti entitásokról beszélhetünk. Munkám során kiemelten fontosnak tartom, hogy a kultúrákat, határok nélkül tudjam vizsgálni. Ugyanis az általam későbbiekben elemezni kívánt vállalatok többége leány vagy anyavállat. Így pedig határok nélküli, egy egészként működő szervezetre kell tekintenem, amelyre Trompenaars modellje nem lenne alkalmas. *Cameron – Quinn Versengő értékek keretrendszere* azt vizsgálja, hogy a szervezetek milyen értékek figyelembevétele mellett törekszenek hatékonyságuk növelésére hosszú távon. A kultúradimenziók beazonosítása és mérése elkerülhetetlen annak érdekében, hogy a vezetők képesek legyenek a kultúra fejlesztésére (Cameron & Quinn, 2011; Fekete - Berzsenyi, 2017). Cameron – Quinn munkája azért jelentős, mivel egyetlen modellbe vonja össze a szervezet hatékonyságát befolyásoló értékeket. Ezt

felhasználva határozza meg, hogy a vezetés milyen céloknak tulajdonít értéket (Lippert, et al., 2015). Kutatásom során ezen hatékonysági tényezők ismerete fontos, mivel az IT rendszerek működése szintén képes a hatékonyságot befolyásolni, így pedig a két terület együttes „mozgását" is képesek lehetünk feltárni. Ezen túlmenően a Cameron – Quinn modell lehetőséget biztosít nem csak a jelenlegi, hanem a jövőben elérni kívánt állapot feltárására is. *Wong megközelítésében* megjelenik a hatalmi távolság és az individualizmus – kollektivizmus dimenziója hasonlóan Hofstede modelljéhez, valamint a természet értelmezése megfeleltethető Trompenaars féle környezet belső-külső kontrolljának. Wong további hét dimenziót definiál, mint az idő, cselekvés, kommunikáció, tér, versenyszellem, szervezet, formalitás (Fekete - Berzsenyi, 2017; Gaál, 1999). Azonban gondolkodásával a nemzeti kultúra modellek közé tartozik, így pedig Trompenaarshoz hasonlóan azt vallja, hogy a vállalatoknak el kell ismernie a kulturális különbözőségeket, ezáltal pedig nem alkalmas az általam kívánt határok nélküli szemléletmód megvalósítására. Választásom során azért került kizárása továbbá, mivel ez a modell hipotetikus, azaz empirikus tapasztalatok nem támasztják alá (Bognár & Gaál, 2013), így pedig nem alkalmas mélyebb vizsgálat lefolytatására. *Hall* megközelítése teljesen eltér Hofstade és Tronpenaarsétől. A cselekvésalapú vizsgálatot képviselte szemben az érték-kutatással (Török, 2017). A modell figyelembe veszi az időt, a kommunikációt, valamint a teret egyaránt (Tolbert & Hall, 2008). A napjainkban kivitelezett kutatások a Hall kultúra dimenziókat nem egymástól elszigetelten, hanem egymást kiegészítve használják (Török, 2017). Azonban nem jelenik meg benne olyan dimenzió, ami lehetőséget teremtene arra, hogy információbiztonság, valamint felhő alapú területekkel össze tudjam kapcsolni, ezáltal pedig használatával nehezen vagy egyáltalán nem tudnám megteremteni a kívánt egyéb tudományterületekkel a kapcsolatát. *Slevin – Covin* mechanikus és organikus kultúrákat különböztet meg. A mechanikus jellemzői a hierarchikusság és formalizáltság, de ezek a szervezetek nehezen alkalmazkodnak. Az organikus kultúra kevéssé formalizált, laza és az egyéni szaktudást helyezi előtérbe, mely alapja a sikerességének. Gyorsan változó, bizonytalan környezethez jól adaptálódnak az organikus vállalatok. A kultúrák ilyesfajta megkülönböztetése meghatározza az alkalmazkodás képességét (Covin & Slevin, 1990; Kiss & Csillag, 2014). Ez kutatásom során hasznos, de a modellt vizsgálva megállapítható, hogy a kommunikációs csatornák, azaz az alkalmazott technológiák csupán kis részarányt képviselnek. Így pedig az általam kívánt összekapcsolás más tudomány területekkel korlátozott vagy lehetetlen lenne. Továbbá mivel a szervezeteket csupán két típusba képes sorolni, így vizsgálatom során túl általános eredményeket kapnék. Azt gondolom, hogy a szervezetek elemzése és besorolása sokkal részletesebben és több típusba szükséges, mint amit Slevin – Covin típusú megközelítés által képes lennék. *Harrison féle kultúra modell* a strukturális, ellenőrzési, kapcsolódási és vezetői pontok alapján határozta meg a négy alapkultúra típust, melyek az erőn, a szerepen, az eredményen alapuló feladat és személy kultúrák (Caroll & Harrison, 2005; Matkó, 2016). Sajátossága a megközelítésnek, hogy nem ragadja ki a kultúrát a gazdasági környezetéből (Harrison, 1992), de ahogy Slevin – Covin nem alkalmas az összekapcsolásra, úgy Harrison modellnél sem lehet megvalósítani, így pedig kutatásom szempontjából nem megfelelő. *Henry Mintzberg féle szervezeti konfigurációban a*

szervezettervezés kulcsa a következetesség, valamint az összefüggés. A vállalat hatékony működése attól függ, hogy mennyire képes kapcsolatot kialakítani a szervezet kora, struktúrája, mérete és technológiája között. Ebből kiindulva olyan szervezeti alapformációkat különített el, amelyek egyrészt a környezet jellemzőivel, a technológiával, a csoport nagyságával függenek össze. Másrészt belső "mozgató erőikben", ideológiai, szervezeti életmódbeli kultúrájukban különböznek (Mintzberg, 2010; Matkó, 2016). Mintzberg megközelítését számos kritika érte, mely szerint tervezési alapelvei hiányosak, megállapításai ellentmondanak a megfigyelhető tényeknek, valamint az előíró és leíró megfigyelések elemzése hiányzik. Nem definiálja továbbá saját modelljének kontextusát sem (Ansoff, 1991). Azt gondolom, hogy a modell jó, azonban ilyen szintű hiányosságai miatt további kibontást és átgondolást igényelne, mivel a rengeteg hiányosság miatt olyan területekkel való összekapcsolása, ami korábban nem történt meg csak további kérdéseket és bizonytalanságokat vetne fel magával Mintzberg modelljével és így teljese megközelítésemmel kapcsolatosan. Ezáltal pedig nem tudom alkalmazni, mivel elengedhetetlen, hogy egy olyan rendszert használjak, ami kipróbált, bizonyított és hiányosságoktól mentes. *Kluckhohn és Strodtbeck* szerint a kultúra csak lassan változik és alapjaiban stabil. Ez a stabilitás teszi lehetővé, hogy vizsgálni lehessen a kulturális orientációkat. Hat dimenziót határoztak meg, melynek részeként vizsgálják az emberek természetét (jó, rossz, nem változtatható), az embereknek a természettel való viszonyát (uralkodó, harmonizáló, alázatos), az emberek egymás közti viszonyát (alárendelt, mellérendelt), az emberek aktivitását (tenni, létezni, kezdeményezni), az időt (múlt, jelen, jövő) és a teret (privát, közös, vegyes) (Kluckhohn & Strodtbeck, 1973; Matkó, 2016). Kluckhohn és Strodtbeck maguk is kimondták, hogy modelljük nem teljes, nem kezelik pl.: a munka természetét, a tér meghatározását, valamint a nemek közti kapcsolatokat (Hills, 2002). Modelljük inkább fókuszál az emberek jellemzőire, mintsem a teljes vállalat működésére. Így azt gondolom, hogy inkább kapnék eredményt a szervezetben dolgozókról, mint magáról a szervezetről egy ilyen megközelítés esetében, holott kutatásomban pont a szervezetre kívánok fókuszálni, mint az egy egyes emberekre. Ezért nem alkalmas azon tudomány területekkel történő összekötésre, melyek esetemben fontos lenne a vállalat működési jellemzőinek ismerete, így munkám során nem alkalmazható modelljük. *Globe-kérdőív* eltávolodik a kétpólusú kultúradimenzió megközelítéstől, bár részben a Hofstede-modellre épül, hiszen a Hofstede-dimenziókat, azok továbbfejlesztett változatát, valamint más kutatóktól átvett és módosított kategóriákat tartalmazza. Azonban már nem csak kvantitatív, hanem kvalitatív módszereket is használ Hofstedevel ellentétben és a szervezeti kultúra vizsgálata során tapasztalt eredményeket külön – külön is kutatja (Török, 2017). Míg a korábbi modellek a leíró dimenziók mentén mérik és értékelik a kultúrák egymástól való eltérését, addig a GLOBE ennél tovább megy és már nem csak azt vizsgálja, ahogy a dolgok vannak, hanem arra is kíváncsi, hogy miképp kellene lenniük. Így lehetőség van a kívánatos kultúrák mérésére is (Bakacsi, 2012), ami hosszú távon számomra is cél. A modell részletes, szofisztikált vizsgálatra ad lehetőséget, de csak az emberi tevékenységre fókuszál, így nem léteznek olyan területek, amelyeket össze lehetne kötni az információbiztonsággal. Jelen esetben a humánbiztonsági kérdésektől tekintsünk el, mivel fontos, de csupán apró szegmensei a biztonságnak.

A vizsgált modelleket az 1. táblázatban értékeltem az alapján, hogy alkalmasak-e az információbiztonsági és felhő kutatásokkal történő kapcsolat megteremtésére, milyen vizsgált dimenziók/értékelési kritériumok jellemzik, továbbá a vállalati értékeket/cselekvés mintákat/fő fókuszt hogyan értékelik.

1. táblázat: Vállalati kultúra modellek

Kultúra modell	Kultúra összehasonlító modell	Lehetséges kapcsolat az információbiztonsági/felhő kutatásokkal	Vizsgált dimenziók/ értékelési kritériumok	Vállalati értékek/cselekvés minták/fő fókusz
Handy féle kultúra modell (Handy, 1999)	x	Alkalmas - Figyelembe veszi az alkalmazott technológiákat.	Hogyan gyakoroljuk a hatalmat? A szabványok és eljárások fontosak, vagy az eredmények? A modell a szervezet múltját, tulajdonformáját, céljait, alkalmazott technológiát, környezetét és az embereket veszi figyelembe.	A szervezetek eltérő értékrenddel rendelkeznek. Így más a munkavégzés módja, ritmusa, más személyiségű embereket vonzanak, sokszor még a külső jegyek alapján is beazonosítható a kultúra.
Hofstede – Nemzeti kultúra modell (Hofstade, 2010)	x	Nem alkalmas - Csak az ember - emberhez való viszonyát vizsgálja.	Bizonytalanság kerülés és a hatalmi távolság által létrehozott négy síknegyedhez különböző szervezeti struktúrákat rendelt.	Hatalmi távolság és az individualizmus/kollektivizmus határozzák meg a cselekvés mintát.
Morgan féle kultúra modell (Morgan, 2007)		Nem alkalmas - Nem tér ki a technológiára, vagy a szervezetet kiszolgáló rendszerekre.	Vállalatvezetők szervezetszemléletét vizsgálta és annak alapján vont le a vállalati kultúrára vonatkozó következtetéseket.	A vezetők vagy úgy gondolnak a szervezetükre, mint egy adott művelet elvégzésére alkalmas, szakszerűen összeszerelt gépre (mechanikus), vagy úgy, mint egy élő szervezetre, amely életciklusa során folyamatosan alkalmazkodik környezetéhez (organikus).
Trompenaars kultúra dimenziók (Hampden-Turner & Trompenaars, 2006)	x	Nem alkalmas - A kultúratípusokat a szervezeti struktúra vertikális és horizontális jellege, illetve a szervezet és beosztottja közötti feladat- személyorientált hozzáállás dimenziói mentén állította fel.	Két tengely mentén csoportosítja a kultúrákat, az egyik tengely végpontjai a személy és a feladatorientált, a másiké pedig az egyenlőségre törekvő és a hierarchikus.	Hogyan gondolkodnak, tanulnak, motiválnak, jutalmaznak és oldják meg a konfliktusokat.

Kultúra modell	Kultúra összehasonlító modell	Lehetséges kapcsolat az információbiztonsági/felhő kutatásokkal	Vizsgált dimenziók/ értékelési kritériumok	Vállalati értékek/cselekvés minták/fő fókusz
Cameron – Quinn – Versengő értékek keretrendszere (Cameron, et al., 2007)	x	Alkalmas - A modellben szerepet kapnak a sikerkritériumok, amelyek egyik eleme tud lenni a technológia, annak hatékonysága, valamint maga a biztonság is. Az adhokrácia kultúrában összetartó erőként jelenik meg az innováció. Értékteremtő elemként tekintenek az innovatív tevékenységekre, megoldásokra.	Az értékpreferenciák feltárásával jellemzi és hasonlítja össze a szervezeteket. A kultúra típusokat két tengely mentén, négy síknegyedben helyezi el.	Annak fényében azonosíthatók a minták, hogy a szervezet a stabilitás, rend, irányítás, rugalmasság, dinamizmus, önállóság valamint a belső fókusz, integráció – külső fókusz, differenciálás mely tengelyén helyezkedik el.
Wong modell (Gaál, 1999)		Nem alkalmas - A használt dimenziók az emberi cselekvést, egymáshoz viszonyulást és annak tulajdonságait foglalják magukba, de sem a technológia, sem pedig az egyéb információs rendszer nem kap szerepet.	Tíz változóból álló vizsgálati modell. Természet, idő, cselekvés, kommunikáció, tér, hatalom, individualizmus, versenyszellem, szervezet, formalitás.	Egy önálló kultúradimenziót szentel a cselekvés témakörének. A modell megkülönböztet cselekvő kultúrákat, amelyekben a domináns viselkedésminta a haladni akarás, míg a létorientált kultúrákban a jelen és annak élvezete kerül előtérbe.
Hall modell (Tolbert & Hall, 2008)	x	Nem alkalmas - A technológia mint átadó közeg jelenik meg csupán.	Az elmélet a világ kommunikációjára építve készült el, melynek része a szavak, az üzleti, politikai és diplomáciai közeg, az anyagi dolgok, a státusz és a hatalom jellemzői. A viselkedés megmutatja, hogy hogyan éreznek az emberek és milyen technikákat alkalmaznak.	Az emberek a másoktól érkező szóbeli, írásbeli vagy egyéb jellegű üzeneteket közös tudásuk alapján értelmezik, amelynek szerves részét alkotják a kultúra beállítódásai, értékei és gondolkodásmintái.
Slevin – Covin modell (Covin & Slevin, 1990)		Nem alkalmas - Az infokommunikációs eszközök mint kommunikációs csatornák hangsúlya kicsi a teljes modellen belül.	Organikus és mechanikus szervezeti kultúra típusokat különböztet meg.	Szemlélteti, hogy a szervezet mennyire képes alkalmazkodni a változó környezethez.
Harrison féle kultúra modell (Caroll & Harrison, 2005)		Nem alkalmas - A modell által a szervezet fő jellemzőiként azonosított elemek között nincsen technikai terület.	Négy alapkultúra típust különböztet meg, melyek az alkalmazott strukturális, vezetői, ellenőrzési és kapcsolódási pontok alapján születtek meg.	A szervezet fő jellemzőiként tekinti a kontroll forrását, a kontroll eszközeit, a fő motiváció forrást, központi értékeket valamint a negatív jellemzőket/következmények.

Kultúra modell	Kultúra összehasonlító modell	Lehetséges kapcsolat az információbiztonsági/felhő kutatásokkal	Vizsgált dimenziók/ értékelési kritériumok	Vállalati értékek/cselekvés minták/fő fókusz
Henry Mintzberg - Szervezeti konfiguráció (Mintzberg, 2010)		Alkalmas - A technostruktúra magába foglalja azokat a személyeket, akik a számítógépes és pénzügyi rendszereket működtetik, így lehetséges az információbiztonsággal való összekapcsolása.	Az egész szervezet koordinált irányítása a részek egymással való kölcsönhatásán keresztül valósul meg.	Öt alapvető szervezeti részt azonosít, melyek meghatározzák a szervezeti értékeket és működést. Ezek közé tartozik a működési mag, a stratégiai csúcs, a közép-vonal, a technostruktúra valamint a segítő személyzet is.
Kluckhoh és Strodtbeck hat dimenziója (Kluckhohn & Strodtbeck, 1973)	x	Nem alkalmas - Csak az emberi tevékenységre fókuszál. Más tudományterületekkel való összekötéshez hiányoznak a kapcsolódási pontok.	Hat területet vizsgál. Figyelembe veszi az emberek természetét, az embereknek a természettel való kapcsolatát, az emberek egymás közti viszonyát, az emberek aktivitását, az időt és a teret.	A vizsgált területek alapján állapítja meg, hogy az amber természete „Jó” (változtatható – nem változtatható), „Rossz” (változtatható – nem változtatható), valamint a „Jó és a Rossz” keveréke.
Globe-kérdőív kulturális dimenziói (House, et al., 2004)	x	Nem alkalmas - Nem számol a szervezeten belül alkalmazott technológiákkal és azok befolyásoló hatásával.	A vizsgálat során meghatározott dimenziók: bizonytalanságkerülés, hatalmi távolság, individualizmus/ kollektivizmus, férfias/nőies értékek, jövőorientáció, teljesítményorientáció, humán orientáció, rámenősség.	Az értékek/kultúradimenziók szintjén ragadja meg a kultúrát. A kérdőív a kultúradimenziókat mind a szervezeti, mind pedig a társadalmi kultúrára vonatkoztatja.

A lehetséges kapcsolat megteremtése más kutatási területekkel azért kritikus, mert ennek hiányában csak két, egymástól független tudományág eredményeit igyekeznék egyesíteni, azonban az egymásra gyakorolt hatásuk viszonyát nem lehetne feltárni. Azon modelleket nyilvánítottam alkalmasnak a kapcsolat megteremtésére, ahol a dimenziók, vagy értékelési kritériumok között megjelentek olyan területek, melyek lehetőséget nyújtottak az összekötés létrehozására. Ezen területeket a következők szerint csoportosítottam:

- **Alkalmazott technológiák:** azon rendszerek összessége, melyek szükségesek a szervezet működtetéséhez és az általuk nyújtott szolgáltatások/termelés biztosításához. Ezen területek esetében fontos kérdés az információbiztonság, az adatok kezelése és a felhő megoldások alkalmazása.
- **Innováció:** olyan szervezetek esetében, ahol az innovációra, mint értékteremtő elemre tekintenek elengedhetetlen, hogy az IT rendszerek hatékonysága, biztonsága és stabilitása szavatolva legyen (Turulja & Bajgoric, 2016).

- **Üzemeltetés:** az a szakértői csapat, aki az IT rendszerek működtetéséért felelnek.

Ezek alapján a Handy féle kultúra modell, Cameron-Quinn versengő értékek keretrendszere, valamint Henry Mintzberg szervezeti konfigurációja megfelelt az összekapcsolási kritériumoknak (1. táblázat).

2.1.2 Vezetői szerepek összehasonlítása

A vezetéstudomány kezdetén *Taylor* elsőként határozta meg a menedzsment fogalmát, amelyet a feladat irányából közelített meg. Úgy vélte, hogy a vezetés felelősége pontosan tudni, hogy mit akar az embereitől, majd ellenőrizni, hogy a legjobban és költséghatékonyan végzik-e azt el (Taylor, 1983; Karcsics, 2012). Tehát a legfontosabb szervezeti érték a teljesítmény és a profitmaximalizálás lett (Lippert, et al., 2015). *Henri Fayol* 1916-ban az Administration industrielle et générale című művében már Taylorral ellentétben nem a termeléssel, hanem az igazgatással foglalkozott. Elsőként fogalmazta meg a menedzseri funkciót, melynek általa meghatározott részei a tervezés, szervezés, parancsnoklás, koordinálást és irányítás (Fayol, 1981). *Max Weber* munkamegosztás szempontjából két kategóriát különített el, a rendelkezőt és rendelkezéshez igazadót. Az első a vezetést, a második pedig a végrehajtást testesíti meg egy szervezeten belül. A vezetésre úgy tekint, mint a szervezetek létrejöttének előfeltételére, amely olyan professzionális feladat, amely a mások által végzet tevékenységek és a tevékenységhez szükséges eszközök, erőforrások összekapcsolására irányul. Weber megközelítésében további két funkció azonosítható, mint az igazgatás és a szabályozás. Az első a szervezeti cselekvésre fókuszál, míg a második arra irányul, hogy mit lehet megtenni (Weber, 1947; Török, 2012). *Henry Mintzberg* arra keresi a választ, hogy a vezetők személyközi (nyilvános megjelenések, főnöki, kapcsolatteremtő és kapcsolatápoló), információs (információgyűjtő, információ szétosztó, szóvívő) vagy döntési (vállalkozói, zavarelhárító, erőforrás elosztó, tárgyaló, megegyező) szerepeket töltenek-e be (Lippert, et al., 2015). Új megvilágításba helyezte a vezetői munkát azzal, hogy a mindennapos tevékenységüket vizsgálta. A modellt felsővezetők körében végzett empirikus vizsgálatokkal támasztották alá, így elsősorban erre a szintre igaz (Dobák & Antal, 2016). Ez azonban korlátot jelenthet számomra, hisz nem minden esetben csak felsővezetők bevonása történik meg kutatásom során. Kultúra modelljével történő összekapcsolás pozitív lehetőség, azonban tervezési alapelvi hiányosságok miatt alkalmazását elvetem. *John Kotter* nem tekinti a menedzsment részének a vezetést (Bogdány, 2014). A vezetői feladatokat két szerepre osztja, manager és leader. A vezető manageri szerepében a szervezeti komplexitással birkózik meg. A leader szerepében ezzel szemben a szükséges változásokra koncentrál (Bakacsi, 2010). Ez a két szerepkör elkülönített alkalmazása és felmérése túlságosan bonyolulttá teszi kutatásomban történő használathoz. Ezzel ellentétben *Dian Hosking* nem bontja fel két külön területre a vezetést, hanem a menedzseri szerepet definiálja részletesebben, ahol a szervezeti erőforrások tervezése, szervezése, vezetése és ellenőrzése a feladata (Draft, 2012). A menedzser célja, hogy azzá váljon, amit a vállalat elvár tőle. Jól bevált technikákat alkalmaz, túl elfoglalt ahhoz, hogy időt szánjon a nehéz dolgokra (Bogdány, 2014). Abraham Zaleznik hasonlóan Kotterhez a management

– leader szemléletet képviseli. Szerinte a leader új lehetőségeket keresi, míg a menedzser korlátozza a választási lehetőségeket. Eltérés van a vállalati célok értelmezésében is a két kategória között, mivel míg a leader alakítja, addig a menedzser elfogadja azokat (Angyal, 2009). A kormányzói szerepkör, mint kiegészítő terület jelenik meg, mely a hatalmi struktúra irányítója. Így pedig leginkább azon tulajdonosokat foglalja magába, aki részt akarnak venni a szervezet életében, azonban nem kívánnak egy teljes leader vagy menedzser pozíciót betölteni (Angyal, 2009). Zaleznik megközelítése ezért Kotteréhez hasonlóan bonyolult, a kormányzói szerepkör pedig további komplexitást ad hozzá. Ilyen szintű diverzifikálás és lebontás esetemben nem indokolt, így alkalmazása nem lenne megfelelő modellemhez. *Richard Boyatzis* személyorientált megközelítést képviseli. A vezető belső adottságaival, tulajdonságaival foglalkozik és ezeket tekinti a legfontosabb kompetenciáknak (Spencer & Spencer, 1993). Szerinte a kompetenciák egy személy meghatározó, alapvető jellemzői, melyek kapcsolatban állnak a teljesítményszinttel (Karoliny & Poór, 1994; Lippert, et al., 2015). A megközelítés szerint az egyéni hatékonyságot értékelni és fejleszteni akkor lehet, ha a legjobban teljesítők személyiség jegyeit vesszük alapul. Ez azonban megítélésem szerint nem minden esetben vezet eredményre, hiszen ha egy szervezetben kialakult „jól teljesítő" nem biztos, hogy az adott iparágban is jónak, vagy kiválónak számít. Ezáltal torz képet adhat és egy téves teljesítménymodellhez vezethet. A feladatorientált (Input) irányzat ezzel ellentétes megközelítést alkalmaz, azaz a kompetenciákat nem az egyéni adottságok határozzák meg, hanem a munkakörhöz tartozó feladatok hatékony teljesítése bizonyítja. Egy szervezet sikerességének szempontjából nem személyiségjegyeket, hanem munkaköri teljesítményt helyezi előtérbe (Karcsics, 2011). Quinn a feladatorientált (Outcome) megközelítést képviseli és a vezetők hatékony működését abban látja, hogy az ellentmondásokat milyen sikerességgel képesek megoldani (Pató, 2006). Quinn szerint fontos kérdés, hogy a vezető szervezeten belüli dolgokra helyezi a hangsúlyt, vagy a külső relációk a fontosak számára, továbbá a feladatok végrehajtása, vagy az alkalmazkodóképesség a hangsúlyosabb (Szintay, 2003).

A vizsgált vezetői szerepekkel kapcsolatos megközelítéseket a 2. táblázatban értékeltem az alapján, hogy outcome vagy input megközelítéshez tartoznak-e, milyen dimenziók/értékelési kritériumok jellemzik, továbbá a vállalati cselekvésminták/fő fókuszt hogyan értékelik. Kutatásom során az outcome megközelítést tartom megfelelőnek, mivel így nyílik arra lehetőség, hogy a vezetőket ne személyiség jegyeik, hanem tényleges munkahelyi teljesítményük alapján értékeljem.

2. táblázat: Vezetői szerepek

Vezetői modellek	Outcome megközelítés	Input megközelítés	Vizsgált dimenziók/ értékelési kritériumok	Cselekvésminták/fő fókusz
Henry Mintzberg (Mintzberg, 2010)		x	A vezetői szerepek hármas csoportosítását valósítja meg, így pedig személyközi, információs és döntési szerepeket azonosít.	Arra keresi a választ, hogy a vezetőnek milyen szerepeket kell betöltenie. A szerepelvárások függenek attól, hogy a vezető a hierarchia mely szintjén áll, vagy hogy milyen szervezetben dolgozik.
John Kotter (Kotter, 2012)		x	Vezetést és menedzsmentet külön fogalomként kezeli, amelyek egymást kiegészítő tevékenységek.	Menedzser – jól csinálja a dolgokat Leader – jó dolgokat csinál
Dian Hosking (Hosking, 1988)		x	A leadership általánosított feladata az alkotás, termelés, újratermelés, átalakítás körforgásának biztosítása indirekt és direkt tevékenységek mentén.	A menedzsert a helyzet racionális értékelése, szisztematikus fejlesztése, a szükséges erőforrások összerendezése jellemzi.
Abraham Zaleznik (Zaleznik, 1992)	x		Menedzser – leader szereposztást követi.	A menedzser korlátozza a választási lehetőségek számát, míg a leader folyton új lehetőségeket, megközelítéseket keres. A vállalati célokat a menedzser elfogadja, de a leader alakítja őket. A menedzser kapcsolata kevésbé emocionális, a leader ennek az ellenkezője, személyközi kapcsolata érzelmekkel dúsított.
Richard Boyatzis (Goleman, et al., 2003)		x	Menedzsment modelljében három dimenziót különített el: kompetencia csoportok, menedzseri funkciók, szervezeti környezet elemei.	A kompetenciák egy személy alapvető, meghatározó jellemzői, melyek okozati kapcsolatban állnak a kritériumszintnek megfelelő kiváló és hatékony teljesítménnyel.
Quinn (Quinn, et al., 2015)	x		Nem vagy-vagy típusú jellemzés, hanem a vezetőben mindegyik tulajdonság valamilyen mértékben jelen van. Négy elkülönített modellt határozott meg, mindegyik két vezetői szerepet tartalmaz.	Arra keresi a választ, hogy milyen irányultságú a vezető gondolkodása. Ez lehet a szervezeten belülre vagy a környezetre (partnerek, versenytársak) fókuszáló. Továbbá a nyitottság, az offenzív/adaptív stratégiák a jellemzők, vagy a koncentráltság, meghatározott irányok és projektek szisztematikus működtetése dominál (Szintay, 2003).

Elemzéseimet követően a Cameron-Quinn Versengő Értékek Keretrendszerét és Abraham Zaleznik megközelítését találtam alkalmasnak a más tudományterületekkel történő összekapcsolásra.

2.1.3 A kutatáshoz kiválasztott szervezeti kultúra és vezetői szerepek megközelítés

A különböző szervezeti kultúra és vezető szerepek megközelítéseket összehasonlítva és elemezve a Cameron Quinn Versnegrő Értékek Keretrendszerét választottam, ugyanis lehetőséget biztosít nem csak a szervezeti kultúra, hanem a vezetési stílus meghatározására is és a két terület összekapcsolása így könnyen megvalósítható. További előnye, hogy funkcionális, megfelelően alkalmazható jelen kutatásom céljait és az esettanulmányt, kérdőíves lekérdezést figyelembe véve. A módszer többféle értékelési megközelítést biztosít és lehetőséget teremt a jelenlegi és a vágyott kultúra egyidejű beazonosítására is. Ez azért is fontos, mert így a stratégiai gondolkodás elemzése is elvégezhető. A modell képes arra, hogy meghatározzam a kultúra típusok erősségét és a szervezeti tulajdonságok közötti kongruenciát. A Cameron-Quinn által megteremtett keretrendszer és a vezetői szerepek vizsgálata jól egészíti ki a szervezeti kultúra felmérését, így pedig támogatva vizsgálatom komplexitásának csökkentését. A vizsgált vezetők az eredményekkel jól jellemezhetők, minden fontos tulajdonságukat feltárva. Segítségével a szervezeti kultúra felmérés rövid idő alatt végrehajtható, és képes mind kvantitatív, mind kvalitatív elemek feldolgozására.

2.2 Információbiztonsági és felhő alapú rendszerek

Az információbiztonság fontosságát alátámasztja napjainkban, hogy a fegyveres konfliktusok, valamint a terrortámadások során a kibertér, valamint az ott elérhető rendszerek már nem csak célpontként, hanem mint eszközként kerülnek felhasználásra. Az is megfigyelhető, hogy a kiberhadviselés tudatosan, valamint összehangoltan történik a fizikai téren zajló küzdelmekkel, sőt akár már azokat megelőzve is elindulnak (Kovács & Krasznay, 2017). A kiberteret két nagy csoportra, virtuális és fizikai összetevőkre lehet osztani (Munk, 2018). Azt, hogy a kibertér milyen összetevőket tartalmaz első sorban az határozza meg, hogy virtuális, vagy fizikai összetevők is alkotják-e. A kibertér az összekapcsolódó informatikai rendszerek, eszközök, hálózatok által nyújtott képességek szolgáltatások együttese (Munk, 2018). Három nagy típusba sorolhatóak a kibertér virtuális összetevői. A legfontosabb típusát a kibertér virtuális infrastruktúra elemei, a teret alkotó hálózati csomópontok és a hálózati összeköttetések logikai szintű leírásai alkotják. Második csoportba az elérhető információ reprezentációk tartoznak. A harmadik típusba a kibertér virtuális szereplői (személyek, szervezetek, csoportok) sorolhatóak (Kovács, 2018). A kibertér fizikai megvalósulását egymásra épülő rétegek alkotják, magját az Internet fizikai összetevői, az összekapcsolódó hálózatok csomópontjai és összeköttetései jelentik. Ezzel párhuzamosan jelennek meg az Internetre csatlakozó számítógépek (számítógépes rendszerek, eszközök), amelyek közé az egyes szolgáltatást biztosító berendezések tartoznak. Harmadik rétegbe a tágabb értelemben vett informatikai rendszerek, eszközök sorolhatóak (Munk, 2018). A vállalatok működését támogató informatikai rendszerek (kibertér) stabilitását és biztonságát, valamint a felhasználók által érzékelt elérhetőségét az üzemeltetésért és információbiztonságért felelős szervezetek közösen teremtik meg, melyeknek egymástól függetlennek kell lenniük annak érdekében, hogy a biztonsági kontroll megvalósulhasson. Mindezek mellett nagy szerepet kap a felhő alapú megoldások használata is, mely

egyik eszköze lehet a rendelkezésre állás és a skálázhatóság további javításának. A virtuális környezetek, melyek a felhő rendszerek alapját képezik, lehetőséget teremtenek, hogy a vállalatok az aktuális igényeknek, valamint az igénybevételnek megfelelő és azokat kiszolgálni képes infrastruktúrát tudjanak rendelkezésre bocsájtani saját működésükhöz ügyfeleiknek, vagy igénybe venni külső szolgáltatótól (Grace, 2010). A felhő megoldások azzal az ígérettel jelentek meg, hogy az infrastruktúrát, alkalmazásokat olyan formában teszik elérhetővé, mint amilyenre korábban nem volt példa (Sultan, 2010). Ennek lehetőségét az elosztott, felhasználás alapú erőforrás rendelkezésre bocsátása jelentette (Beloglazov, 2013). Az ilyen szolgáltatások alapvetőn új megközelítést és működési modellt tesznek lehetővé a szervezetek számára, ami akár magasabb rendelkezésre állást és/vagy csökkenő költségeket is eredményezhet a méretgazdaságosságból fakadóan (Educause, 2009). Ugyanis nincs szükség saját eszközök vásárlására, fenntartására, továbbá saját üzemeltetési csapat alkalmazása se indokolt, mivel a beruházásokat és működtetési feladatokat a felhő szolgáltató elvégzi. Az ügyfeleknek csupán azért a szolgáltatásért kell fizetni, amit ténylegesen igénybe vesznek. A használat mértéke pedig rugalmasan (on-demand) változtatható, így alkalmazkodva az igényekhez. Ez óriási előnyt jelenthet, mivel az információstechnológiai beruházásokra szánt forrásokat a vállalatok profiljukhoz jobban illő és az ügyfelek elégedettséget növelő kezdeményezésekre fókuszálva tudják elkölteni (Spilák & Kosztyán, 2013). A felhő szolgáltatások képesek időt és költséget megtakarítani, valamint hatékonyabbá tenni a mindennapi működtetést (Rittinghouse & Ransome, 2009; Kavis, 2014). Négy fő csoportra bontjuk őket annak függvényében, hogy az erőforrásokat a közösség együttműködve biztosítja (közösségi felhő) (Zhao, et al., 2014), egy harmadik fél nyújtja (publikus felhő), házon belül épült ki (privát felhő), vagy pedig ezek kombinációja valósul meg (hibrid felhő) (Goyal, 2014). Számos szakember és kutató (pl.: (Wienman, 2012; Botta, 2016; Rittinghouse & Ransome, 2009; Chawla & Sogani, 2011; Buyya, et al., 2013; Agrawal, et al., 2012) úgy véli, hogy az IT jövője a publikus felhő, függetlenül a szükséges kapacitásoktól és vállalati mérettől (Weinman , 2016). A privát és publikus felhő szolgáltatások közötti gazdasági különbség abban mutatkozik meg, hogy a felmerült költségek fixek vagy felhasználás alapúak (Weinman, 2015). A publikus felhő szolgáltatásoknak költséghatékonyabb működést kellene elérniük a privát megoldásoknál, azonban a valóságban ez a kérdés jóval komplexebb, mint hogy ezt egyértelműen ki lehessen jelenteni. A kis- és középvállalkozások, sőt akár néhány nagyobb szervezet számára a publikus felhő lehet a legjobb választás. Vannak azonban ellenpéldák is, amikor a nagyvállalatok publikus szolgáltatótól saját infrastruktúrára történő költözéssel megtakarítást értek el (pl.: Instagram felvásárlását követően a Facebook saját privát felhőjébe történő átmozgatása esetén). Azonban nem szabad figyelmen kívül hagyni a hibrid megközelítésben rejlő lehetőségeket, amely a publikus, a privát és közösségi felhő modelljét ötvözi. A vállalatok így a felmerült kapacitás és szolgáltatás igényeiket a stratégiai, biztonsági és bizalmassági kritériumokhoz igazítva tudják kiszolgálni különböző felhő szolgáltatások egyidejű igénybevétele mellett (Puthal, et al., 2015; Chou, 2015; Weinman, 2015). Két kritikus kérdéskört azonban mindenképpen mérlegelni kell ezen megoldások alkalmazásakor. Egyrészt a felhő alapú szolgáltatások biztonságával, rendelkezésre állásával, integritásával kapcsolatos

problémák figyelembevétele (Ali, et al., 2015) (pl.: az 2017-ben az Amazonnál felmerült hiba még az Apple által üzemletetett iCloudra is kihatással volt), valamint a szervezet adatainak felhőbe mozgatásakor szükséges kockázatelemzés elvégzése elengedhetetlen. Az információs társadalom napjainkban már nagyon fejlett, ugyanakkor meglehetősen sebezhető. Ennek alapján az adja, hogy működése szorosan kapcsolódik globális, regionális és lokálisinformációs környezetkhez. Előnye, hogy az információs társadalom hatalmas teljesítményekre képes a tudomány, termelés, információcsere területén, azonban árnyoldalai is vannak, hiszen egy olyan világban, ahol minden fontosabb ügyünket a hálózaton intézzük annak kiesése felmérhetetlen károkat képes okozni (Haig, et al., 2009). A védelmi mechanizmusok és intézkedések ellenére a felhasználók továbbra is szkeptikusan tekintenek a felhőre (Mathur & Purohit, 2017). A szolgáltatók nem tudnak lépést tartani az új technológiákkal és kihívásokkal, így gyakoriak a biztonsági incidensek (Liveri & Skouloudi, 2016). Az információbiztonsági érettségi modelleket vizsgálva (pl.: ISM3, IBM-ISF, NIST CSEAT IT SMM, Gartner Security Maturity Model, SUNY ISI, SSE-CMM, INFOSYS IT Security Maturity Model, Cyber Security Model, stb.) megállapítható, hogy a hangsúly a technikai alapú biztonsági kontrollokra helyeződik, míg a nem technikai megoldások háttérbe szorulnak (Karokola, et al., 2011). Tehát a biztonsági szakemberek még mindig a védelmi eszközökben látják a megoldás kulcsát, és nem a szervezeti intézkedések, tudatosság kialakításában. A biztonsági incidensek felmerülésekor a bekövetkezés gyakoriságát, hatását és kiváltó okát vizsgálják még az előtt, hogy kidolgozásra kerülnének a lehetséges jövőbeni védelmi intézkedések (Ransbotham, et al., 2012). Azonban a vállalatok döntő részénél problémát jelent, hogy az incidenseket nem detektálják, illetve nem rendelkeznek részletes riportokkal (Dekker, et al., 2013). Ennek kritikussága tovább növekszik annak függvényében, hogy az Európai Unió szorgalmazza a felhő megoldások használatát a vállalati környezetben, felismerve annak pénzügyi és gazdasági előnyeit (Dekker, et al., 2013). A 2013-as Cybersecurity Strategy of European Union tanulmány igyekszik választ adni a fenti problémákra, mivel a pozitív kezdeményezés mellett komoly hangsúlyt fektet a tudatosságra, a biztonsági fenyegetettségek időbeni kommunikációjára és információmegosztásra (Cavelty, 2013). Barack Obama 2013. szeptember 12-én a létfontosságú infrastruktúrák információbiztonsági irányelvének részeként szintén a cyber biztonsági információmegosztás jelentőségét hangsúlyozzta (Boukalas, 2014). De a teljes nyilvánosságra hozatallal akár ellentétes hatást lehet elérni, azaz képes felgyorsítani a támadás térnyerését a megcélzott populáción belül, valamint növeli a „first attack” lehetőségét a sérülékenyég közzétételét követően (Mitra & Ransbotham, 2015).

A felhő környezetek flexibilitása és skálázhatósága hátrány is lehet biztonsági szempontból, mivel az erőforrások és az adatok magas koncentrációja ígéretes célponttá teszi ezen szolgáltatásokat (Catteddu & Hogben, 2009). Ezért egy vállalat adatainak felhőbe történő vitele esetén nem kerülhető meg a kockázatelemzés annak ellenére, hogy 2009 óta a felhő megoldások piaca nagyban megváltozott, a szolgáltatók érettebbé váltak, a felhasználók biztonság tudatossága javult (Dekker & Liveri, 2015). Az

ENISA által kiadott Benefits, risks and recommendations for information security tanulmány szabályozási – szervezeti, technológiai, jogi valamint nem felhő specifikus kockázati kategóriák alapján vizsgálja a felhő rendszereket annak érdekében, hogy a vállalatok átfogó képet kapjanak ezen technológiák korlátjairól (Catteddu & Hogben, 2009). A kockázatok azonban vállalatonként eltérhetnek, mivel nagyban függnek a szolgáltatótól, a tárolt adatoktól valamint folyamatoktól (Dekker & Liveri, 2015). A kötelező biztonsági standardok képesek elősegíteni/kikényszeríteni a minimális biztonsági kontrolt, ami kritikusan fontos, mivel a szervezeteknek nem csak magukat, hanem a rájuk bízott adatokat is meg kell tudniuk védeni. Tisztában kell lenni azzal, hogy a standardok megalkotói nem tudnak mindenre kiterjedő és elég részletezettségű kontrollt létrehozni, mivel az információs technológiák gyorsan fejlődő, komplex tényezők és rengeteg környezeti sajátossággal rendelkeznek (Lee, et al., 2016). A döntési és statikus játék teóriákat is alkalmazzák annak érdekében, hogy a szakemberek képesek legyenek felismerni és jellemezni a hackerek és a vállalatok stratégiáját. Azonban még így sem lehetséges a kockázati környezet dinamikáinak teljes kezelése, amely kiemelt eleme az olyan modern és elosztott informatikai rendszereknek, mint a felhő megoldások (Gao, et al., 2013). A biztonsági incidens gyanúja, vagy bekövetkezése esetén lefolytatott forensics vizsgálatok segítenek abban, hogy az események körét, az ügyfelek érintettségét meg lehessen határozni. A felhő rendszerek esetén ezen vizsgálatok bonyolultabbak, mint a nem elosztott megoldásoknál (Liveri & Skouloudi, 2016). A vizsgálat komplexitása függ a szolgáltatási modelltől (Infrastructure as a Service, Platform as a Service, Software as a Service, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing as-a-service), továbbá az igénybevétel módjától (privát, publikus, hibrid vagy közösségi felhő) (Liveri & Skouloudi, 2016). Mindezért indokoltnak tartom, hogy a szervezeti, informatikai és biztonsági területeket együttesen vizsgáljam. Korábbi kutatásom rámutatott arra, hogy a szervezetek döntő része rendelkezik minimális információbiztonsággal, valamint a szervezeti kultúra és információbiztonság között kapcsolat fedezhető fel (Spilák & Kosztyán, 2013). A terület mélyebb vizsgálata azonban képes további hasznos kapcsolatokra rávilágítani, valamint segíteni azok megértését.

2.2.1 Információbiztonsági modellek összehasonlítása

A kutatás során arra törekedtem, hogy a szervezeti kultúra, vezetői szerepek, információbiztonsági kiválóság és felhő alapú megoldások közötti relációk meghatározását egy olyan modell segítségével végezzem el, mely képes a területek közötti kölcsönhatások feltárására. A modell szervezeti kultúra és vezetői szerepek részét a korábban már említett Cameron-Quinn versengő értékek adta. Az információbiztonsági kiválóság meghatározását olyan tanulmányok pl.: (Buecker, et al., 2014; Scholtz , et al., 2016; Sjelin & White, 2016; Bowen & Kissel, 2017; Barrett, 2018) értékelése előzte meg, melyek kiválasztásakor szempont volt, hogy ne csak egy specifikus területet vizsgáljanak az információbiztonságon belül, hanem szélesebb – akár a menedzsment – aspektust is figyelembe vegyék. Ezért értékelésükkor (3. táblázat) öt tényezőre fókuszáltam, mint az információbiztonsági területekre, fenyegetettségek felismerésére, felelősségek meghatározására, információ biztonság menedzsmentjére,

valamint a fő kritériumok definiálására. Az értékelés során azért erre az öt tényezőre esett választásom, mivel az irodalomban szereplő megközelítéseket feldolgozva, a biztonsági szint meghatározásának a legalapvetőbb építőköveiként azonosítottam őket. Ahhoz, hogy egy szervezet biztonsági szintjét megfelelően meg tudjam határozni elengedhetetlen az információbiztonság minden területének (fizikai, logikai, humán) ismerete. Ezen túlmenően kiemelten fontos a fenyegetettségekkel tisztában lenni, hiszen enélkül nem tudnánk meghatározni, hogy egyáltalán a kialakított biztonság megfelelő-e, ha nem ismernénk magukat a veszélyeket, amikre választ kéne tudnunk adni segítségükkel. A felelőségek meghatározása nélkül, egy esetleges incidens során nem lenne kihez fordulni, mivel senki se tekintené magáénak a feladatot és igyekezne egy másik területre rámutatni. Természtesen az előző elemek önmagukban nem működnek együtt, ezért szükséges a biztonság menedzsmentjét is vizsgálni, hiszen ez, mint egy keretrendszer fogja közre a különálló területeket. Az ötödik tényező nem a biztonsági szint meghatározásának része, azonban a modellek értékelésében és áttekintésében kulcsfontosságú, ezért is vontam be az értékelés során.

3. táblázat: Információbiztonsági modellek dimenziói

Érettségi modell	Információbiztonsági kiválóság				Vizsgált dimenziók/Fő értékelési kritériumok
	Területek	Fenyegetettségek felismerése	Meghatározott felelősségek	Inf. biztonság menedzsment	
INFOSYS IT Security Maturity Model (Narasimhalu, et al., 2004)	x	x	x		Három dimenzió alapján vizsgálják a szervezeteket: infrastruktúra, IT biztonsági intelligencia és a folyamatok biztonsága. Ez alapján történik meg az egyes érettségi szintekbe való besorolás.
Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View (Karokola, et al., 2011)	x	x			Több tényező vizsgálatának segítségével sorolja a szervezeteket az egyes érettségi szintekbe, így figyelembe veszi: adminisztratív és vezetői, tudatossági, etikai és kulturális, jogi és szerződéses folyamatok, szoftver megoldások területeket.
Information Security Model (Saleh, 2011)	x	x	x	x	A biztonságot egy szervezetben a szervezet irányítása, a szervezet kultúrája, a rendszer architektúrája és a szolgáltatás menedzsment befolyásolja.
Information Security Management Maturity Model (O-ISM3) (The Open Group, 2011)	x	x	x	x	Hangsúly a folyamat integráltságon. Az egyes érettségi szervezetek méretének, erőforrásainak, fenyegetettségeinek, ezek hatásainak, kockázat vállalási készségüknek, gazdasági szektornak megfelelően kell alakítani.
IBM Information Security Framework (IBM-ISF) (Buecker, et al., 2014)	x	x		x	Alapját a Gap analízis adja. A középpontba a személyeket, adatokat, alkalmazásokat, az infrastruktúrát, a biztonsági intelligenciát és analízist helyezi. Ezen felül definiál egy érettségi modellt.
Cyber Security Capability Assessment (Hansen, 2016)		x		x	A szabályozottság és a cyber biztonság national aspektusú vetületét vizsgálja elsősorban.

Érettségi modell	Információbiztonsági kiválóság				Vizsgált dimenziók/Fő értékelési kritériumok
	Területek	Fenyegetettségek felismerése	Meghatározott felelősségek	Inf. biztonság menedzsment	
Gartner: ITScore for Information Security (Scholtz , et al., 2016)		x	x	x	Menedzsment eszközök és megvalósított funkcionalitás mentén értékel.
Community Cyber Security Maturity Model (CSMM) (Sjelin & White, 2016)		x		x	A közösségi erőfeszítést és tudás megosztást helyezi előtérbe.
Program Review for Information Security Management Assistance (PRISMA) (Bowen & Kissel, 2017)		x		x	Kiemelt hangsúlyt fektet a dokumentáltságra.
Framework for Improving Critical Infrastructure Cybersecurity (Barrett, 2018)		x		x	Elsődleges fókusz az azonosításon, védelmen, detektáláson, válaszadáson és visszaállításon van.

A 3. táblázatban összesített adatok alapján az elemzett kutatások mindegyike foglalkozik a fenyegetettségek felismerésével annak érdekében, hogy meg tudják határozni hatásukat és bekövetkezésük valószínűségét. Jól látható, hogy csupán ennek a területnek a vizsgálata nem elég, ezért egyéb területeket is bevontak (pl.: fizikai, logikai, humán biztonság, felelőségek, stb.). Itt azonban két táborra lehet osztani a feldolgozott tanulmányokat, mivel egy részük pl.: (Narasimhalu, et al., 2004; Karokola, et al., 2011; Buecker, et al., 2014) mélyebb informatikai vizsgálattal folytatta és kitért az egyes területekre, azok felépítésére és sajátosságaira. Mások pl.: (Saleh, 2011; The Open Group, 2011; Hansen, 2016; Scholtz , et al., 2016; Sjelin & White, 2016; Bowen & Kissel, 2017; Barrett, 2018) azonban ehelyett inkább az információbiztonság tudatos menedzselésére helyezték a hangsúlyt és nem minden esetben merültek el a technikai részletekben. Az információmegosztás jelentősége az utóbbi évek kutatásaiban pl.: (Scholtz , et al., 2016; Sjelin & White, 2016; Bowen & Kissel, 2017; Barrett, 2018) jelenik meg hangsúlyosan, azonban ennek számos előnye mellett néhány negatív hatása is lehet, mint például felgyorsítja a támadás térnyerését a megcélzott populáción belül, valamint növeli a „first attack” lehetőségét. Megjelenik a szervezeti kultúra, illetve az irányítás, mint befolyásoló tényező, de együttes vizsgálatuk csak részlegesen történt meg és nem foglalkoztak a szervezeti kultúra és vezetői szerepek pontos beazonosításával, a felhő alapú megoldások információbiztonságra gyakorolt hatásainak feltérképezésével. Az információbiztonsági kiválóságot a területek, fenyegetettségek felismerése, felelősségek meghatározása és az információbiztonság menedzsment elemekre bontottam fel, építve a korábbi kutatásokra, de bővítve azokat annak érdekében, hogy a korábban nem vizsgált kapcsolatokat képes legyek beazonosítani és értelmezni.

2.2.2 Felhő megoldások alkalmazásával kapcsolatos modellek összehasonlítása

A felhő alapú megoldások alkalmazásának meghatározását olyan modellek értékelésére alapoztam pl.: (Mattoon, et al., 2011; Guangming , et al., 2017), amelyek nem csupán technikai vagy technológiai aspektusból vizsgálták ezen szolgáltatásokat, hanem például információbiztonságra vagy az IT szervezetre gyakorolt hatásaikat is értelmezték. A felhő megoldásokkal kapcsolatos megközelítéseket a 4. táblázatban értékeltem öt tényező figyelembevételével, mint felhő modell, üzemeltetés, szolgáltatás modell, az információbiztonság menedzsment, valamint a fő értékelési kritériumok definiálását. Az értékelés során azért ezt az öt tényezőt vettem figyelembe, mivel a korábbi kutatásokat feldolgozva, mint minimum vizsgálandó területekként tudtam őket azonosítani. Ahhoz, hogy egy szervezet esetében meghatározzam, hogy milyen érettségi szinten áll a felhő megoldások használatának tekintetében, elengedhetetlen vizsgálni a felhő modelleket, azaz privát vagy publikus megoldásokra épít, fontos figyelembe venni, hogy az üzemeltetést belő, külső forrásból oldja meg, vagy ezek bizonyos kombinációjával. Az érettség meghatározásában továbbá kulcsszerepet játszik, hogy milyen szolgáltatási modellben gondolkozik, azaz infrastruktúra, platform, vagy szoftvert szolgáltatást vesz igénybe. Az információbiztonság a felhő megoldások esetében is kritikus, ezért szükséges a megközelítésnek tartalmaznia kell a biztonsági elvárásokkal kapcsolatos kitételeket, illetve figyelembe szükséges venni az adatok kihelyezhetőségét is. Az ötödik tényező nem a biztonsági szint meghatározásának része, azonban a modellek értékelésében és áttekintésében kulcsfontosságú, ezért is történt meg bevonása az összesítés során.

4. táblázat: Felhő megoldásokkal kapcsolatos modellek dimenziói

Érettségi modell	Felhő alapú megoldások alkalmazása				Vizsgálati dimenziók/fő értékelési kritériumok
	Felhő modell	Üzemeltetés	Szolgáltatás modell	Információbiztonság menedzsment	
Oracle: Cloud Computing Maturity Model Guiding Success with Cloud Capabilities (Mattoon, et al., 2011)	x	x	x	x	A szervezet érettségét a stratégia, architektúra, infrastruktúra, információk, üzemeltetés-menedzsment, project portfolió, szervezet és irányítás értékelésével határozza meg.
The Road to The Responsible Cloud (Drogseth, 2011)	x	x	x		Az időszakos fejlődés és a menedzsment kettőse alapján értékeli az egyes érettségi szinteket.

Érettségi modell	Felhő alapú megoldások alkalmazása				Vizsgálati dimenziók/fő értékelési kritériumok
	Felhő modell	Üzemeltetés	Szolgáltatás modell	Információbiztonság menedzsment	
Managing Cloud Computing: A Life Cycle Approach (Conway & Curry, 2012)	x	x		x	Life cycle management segítségével kívánja kontrollálni nem csak a felhő szolgáltatások bevezetését, hanem a publikus felhő mindennapi működését is.
Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels (Weiss, et al., 2013)	x	x		x	A felhő modellek domainjeit szervezeti és technikai csoportokra osztja. Kitér a szabályozásra, biztonságra, szervezeti készültségre, folyamatokra, infrastruktúrára és az üzemeltetés menedzsmentjére.
Cloud Maturity Model (Duarte & Mira da Silva, 2013)		x	x		Felhő érettségi modell alapját a kiszervezési életciklus és a CMMI (Capability Maturity Model Integration) képezi.
Cloud Computing With a Model Futuristic Maturity (Nagaraj & Sathish kumar, 2015)	x	x	x		Fázis megközelítést javasol, valamint öt kulcs komponenst határoz meg: konszolidáció, virtualizáció, automatizálás, felhasználás és felhő.
Cloud Data Governance Maturity Model (Guangming , et al., 2017)	x	x	x	x	Az adatkezelés érettségének vizsgálatára összpontosít a felhő megoldásokkal kapcsolatosan.
Enterprise Cloud Adoption - Cloud Maturity Assessment Model (Conway, et al., 2017)		x		x	11 kulcs komponenst azonosít, mely hatással van a felhő megoldások bevezetésére és használatára.
Maturity Level of Cloud Computing at HCT (Alqassemi, et al., 2017)	x	x			Szolgáltatás orientált architektúra megközelítést alkalmaz az érettségi modell mérésében.
FHNW Maturity Models for Cloud and Enterprise IT (Grivas, et al., 2018)	x	x	x	x	Nem a szokásos felhő érettségi modell értékelést követi, azaz milyen felhő szolgáltatást használnak, vagy a bevezetés milyen szakaszában áll a cég. Hanem arra fókuszál, hogy miért használják a felhő megoldásokat, és ez miképp változtatja meg az IT pozícióját és feladatait.

A 4. táblázatban összesített modellek döntő többségének középpontjában a szervezet digitalizáltsága, az informatikai és a felhő képességek szerepelnek pl.: (Mattoon, et al., 2011; Drogseth, 2011; Conway & Curry, 2012; Weiss, et al., 2013). Az érettséget kritériumok kombinációjaként határozzák meg és sorolják be a szervezeteket érettségi szintekbe (tanulmányonként négy-kilenc szint). 2017-től kerültek előtérbe az üzleti területeknek, az IT működésének, valamint a felhő megoldások alkalmazásának összehangolására irányuló törekvések pl.: (Guangming , et al., 2017; Conway, et al., 2017; Alqassemi, et al., 2017; Grivas, et al., 2018). Így a modellek már képesek segítséget nyújtani a szervezetek számára a fenti területeket érintő döntések meghozatalában is. Ezáltal támogatják a felhő megoldások jobb integrálhatóságát és a szervezetek digitális átalakítási folyamatát. Fontos kiemelni, hogy egyetlen modell sem képes megmondani, hogy miképpen használja egy szervezet ezen szolgáltatásokat, mivel alkalmazásuk formája és lehetőségei függenek a szervezet sajátosságaitól. Munkám során elemzett kutatások eredményeit felhasználva a felhő alapú megoldásokat a felhő modellek, üzemeltetés, szolgáltatások és információbiztonság menedzsment elemekre bontottam fel.

2.3 Az irodalmi elemzés eredményei

Az irodalmi elemzés részeként áttekintettem a szervezeti kultúrákkal, vezetői szerepekkel kapcsolatos modelleket és összehasonlításukat követően meghatároztam azok körét, amelyek alkalmasak lehetnek kutatásom során történő felhasználásra. Az információbiztonság és felhő alapú megoldásokkal foglalkozó megközelítéseket szintén részletesen elemeztem, melynek eredményeként a jelen fejezetben meghatározom, hogy mely elemek szükségesek egy olyan új felmérés létrehozásához, amely alkalmas a szervezeti és vezetői kapcsolatok megteremtésére is.

2.3.1 Szervezeti kultúra

Munkám során a Cameron – Quinn Versengő Értékek Keretrendszere által meghatározott kultúra típusokat választottam. A módszer számos értékelési megközelítést biztosít és lehetőséget teremt a jelenlegi és a vágyott kultúra egyidejű beazonosítására is. Ez azért is fontos, mivel így a stratégiai gondolkodás elemzése is elvégezhető. A modell képes arra, hogy meghatározzam a kultúra típusok erősségét és a szervezeti tulajdonságok közötti kongruenciát. A kutatás során a domináns szervezeti kultúrát veszem figyelembe. Azt a kultúrát tekintem dominánsnak, amely a hat szempont alapján kapott válaszok szerint a legnagyobb átlagos értéket adja (Cameron & Quinn, 2011). A domináns kultúra erősségét pedig az határozza meg, hogy a kapott átlagos érték mekkora (Lippert, et al., 2015). A kutatás során azért is előnyös a domináns értéket figyelembe venni, mivel a szervezetet ez a viselkedésforma jellemzi leginkább, azaz tagjai meghatározó részének cselekvését legpontosabban ez írja le.

A módszer különféle elemzési lehetőségeket biztosít, azonban kutatásom során a domináns kultúrát fogom a szervezet jellemzésére használni. Továbbá a Versengő Értékek Keretrendszere segítségével egy egységes rendszerben értelmezhető a vezetői szerepekkel, így pedig nem szükséges kidolgozni kapcsolatukat.

2.3.2 Vezetői szerep

Cameron – Quinn által megteremtett keretrendszer és a vezetői szerepek vizsgálata jól egészíti ki a szervezeti kultúra felmérését, így pedig támogatva munkám komplexitásának csökkentését. A vizsgált vezető az eredményekkel jól jellemezhető, annak minden fontos tulajdonságát feltárva. Lehetőséget biztosít a módszer arra, hogy a jelenlegi és a kívánatos állapotot is meghatározzam, azonban munkámban csak a jelen felmérésére fókuszáltam annak érdekében, hogy elkerüljem modellem komplexitásának növelését.

A vezetés jellemzését a domináns értékek figyelembevételével teszem meg, ennek értelmében azonban nem veszem figyelembe azon tulajdonságokat, amelyek csak kis mértékben jellemzik a vizsgált személyeket.

2.3.3 Információbiztonsági kiválóság

Az információbiztonság meghatározásakor olyan modelleket vettem alapul, mint pl.: (Buecker, et al., 2014; Scholtz , et al., 2016; Sjelin & White, 2016; Bowen & Kissel, 2017; Barrett, 2018) értékelése előzte meg, melyek kiválasztásakor szempont volt, hogy ne csak egy specifikus területet vizsgáljanak az információbiztonságon belül. Megközelítésemet olyan tényezőkre fókuszálva alakítottam ki, mint az információbiztonsági területekre, fenyegetettségek felismerésére, felelősségek meghatározására, információbiztonság menedzsmentjére. A feldolgozott tanulmányokat két táborra lehet osztani (3. táblázat), mivel egy részük pl.: (Narasimhalu, et al., 2004; Karokola, et al., 2011; Buecker, et al., 2014), mélyebb informatikai vizsgálatot tartotta fontosnak és kitért az egyes területekre, azok felépítésére és sajátosságaira. Mások pl.: (Saleh, 2011; The Open Group, 2011; Hansen, 2016; Scholtz , et al., 2016; Sjelin & White, 2016; Bowen & Kissel, 2017; Barrett, 2018) azonban ehelyett inkább az információbiztonság tudatos menedzselésére helyezték a hangsúlyt és nem minden esetben merültek el a technikai részletekben.

Meggyőződésem, hogy a két megközelítés ötvözése szükséges ahhoz, hogy az információbiztonság kérdéskörét megfelelő mélységben vizsgáljam, valamint megteremtsem a kapcsolódási lehetőségét más tudományterületekkel is (pl.: szervezeti kultúra). Az információbiztonsági kiválóságot ez alapján a területek, fenyegetettségek felismerése, felelősségek meghatározása és az információbiztonság menedzsment elemekre bontottam fel. Kiértékelését a domináns értékek figyelembevételével teszem meg.

2.3.4 Felhő alapú megoldások alkalmazása

A vizsgált modellek döntő többségének középpontjában a szervezet digitalizáltsága, az informatikai és a felhő képességek szerepelnek pl.: (Mattoon, et al., 2011; Drogseth, 2011; Conway & Curry, 2012; Weiss, et al., 2013). Az érettséget kritériumok kombinációjaként határozzák meg és sorolják be a szervezeteket érettségi szintekbe.

Arra következtetésre jutottam, hogy a legszignifikánsabb problémák nem a technológiai megvalósításban keresendők, hanem a vezetési és szervezeti kihívásokban rejlenek. A felhő megoldások alkalmazhatóságát ezért négy részegységre bontottam fel, melyek kitérnek a felhő szolgáltatási modelljére, üzemeltetésre, az igénybevett szolgáltatás típusára és a menedzsmentre.

3 Kutatási modell és módszertan

Ebben a fejezetben a szakirodalom ismeretében tisztázom munkám fogalmi kereteit, azaz kutatásom mire és mire nem terjed ki. Ismertetem hipotéziseimet, valamint létrehozom kutatási modellemet. Ezt követően definiálom a vizsgálati módszereket mind a kvalitatív, mind pedig a kvantitatív megközelítésre vonatkozóan.

3.1 Konceptualizálás

A kutatási kérdések meghatározását követően ki kell választanom a lehetséges utakból azt, amelyiken végig haladva eljuthatok a válaszokhoz (Balogh, et al., 2011). Szükséges továbbá, hogy pontosan meghatározzam, mit értek a használt fogalmak alatt, ugyanis ezek egyben korlátozást is fognak jelenteni, definiálják ugyanis mely területek esnek kívül kutatásom fókuszán. A szakirodalom értékelése és összehasonlítása során számos olyan témakört azonosítottam, melyek kapcsolata nem volt teljeskörű, vagy még kevés empirikus kutatás irányult rá.

Az egyik ilyen arra vonatkozik, hogy korábban csupán egy szakmai területre fókuszáltak a kutatók és azt próbálták minél részletesebben és átfogóbban körbejárni, újabb és újabb megközelítések létrehozásával. Azonban hiányzott, hogy az informatikai szakmával történő együttes vizsgálatot valósítsanak meg a szervezetek működését figyelembe véve. Csupán csak 2017-től kerültek előtérbe az üzleti területek, az IT működés, valamint a felhő megoldások alkalmazásának összehangolására irányuló törekvések pl.: (Guangming , et al., 2017; Conway, et al., 2017; Alqassemi, et al., 2017; Grivas, et al., 2018), azonban ezek csak részterületekre terjedtek ki. Így fontosnak tartottam, hogy megvizsgáljam a szervezeti kultúra és vezetői szerepek által gyakorolt hatást az információbiztonságra és felhő alapú megoldások alkalmazására. Ezért mutattam be a szakirodalmi részben a szervezeti kultúra és vezetői szerepek vizsgálatával foglalkozó legfontosabb kutatásokat, azok eredményeit. Kiemeltem azokat, amelyek alkalmasak lehetnek az empirikus kutatásomban való felhasználásra, valamint a végén kiválasztottam a ténylegesen használni kívánt megközelítést.

A kutatás megalapozásához áttekintettem az információbiztonsági, valamint felhő alapú megoldásokkal kapcsolatos érettségi modelleket. Azonban fel kellett ismernem, hogy azok döntő hányada még nem alkalmas arra, hogy más tudományágakkal kapcsoljam össze, hiszen túl mélyek, részletesek és csak önálló felmérésükben gondolkoznak. Ezért ezen változtattam és megalkottam az információbiztonsági kiválóságot, melynek fő építő elemeinek a területeket, fenyegetettségek felismerését, felelőségek meghatározását és információbiztonsági menedzsmentet definiáltam. Szükséges volt a felhő alapú megoldások alkalmazását felmérni képes modell kialakítása is, amelyet a felhő modellek, üzemeltetés, szolgáltatások és információbiztonság menedzsment összeseként definiáltam.

3.2 Hipotézisek

A kutatási kérdések segítségével definiáltam a munkám során vizsgálandó területeket. A hipotézisek a vizsgálati modellemben meghatározott változókról, valamint azok kapcsolatáról szólnak, továbbá olyan feltételezések, amelyeknek több elvárásnak is meg kell felelniük:

- a hipotézisek előfeltevések, melyek a kutatói munka végeztével igazolásra vagy cáfolásra kerülnek;
- a feltételezett kapcsolatoknak és azok egymásra gyakorolt hatásának mérhetőnek és igazolhatónak kell lenniük;
- egy-egy jól körülhatárolható problémára fókuszálnak.

Kutatásomban a szervezeti kultúra és a vezetői szerepek által az információbiztonsági kiválóságra, valamint a felhő alapú megoldások alkalmazására gyakorolt hatásokat az alábbi négy hipotézisben fogalmaztam meg.

Az első hipotézisem során építek az irodalomból már megismert tanulmányokra, így az egyes vezetői szerepekre jellemző tulajdonságok és viselkedésminták alapján lehet következtetni arra, hogy azok milyen hatással lehetnek az információbiztonság fejlettségére. Azon vezetői szerepek fognak jól teljesíteni az információbiztonság esetében, ahol a hatékony munkavégzésre, termelékeny környezet megteremtésére fókuszálnak, hiszen ennek egy fontos eleme a termelést kiszolgáló rendszerek védelme is. Tehát a Cameron-Quinn modellben a kontrolláltság félsíkban helyezkednek majd el (Cameron & Quinn, 2000).

1.*hipotézis*

Olyan Cameron-Quinn vezetői szerepek mellett lesz a biztonság fejlett, amelyek a szabályozottságra és stabilitásra törekszenek.

A második hipotézisem esetében úgy gondolom, hogy az egyes kultúrák hatást gyakorolnak az információbiztonsági szintre, hiszen a szervezet működése támogathatja vagy gátolhatja az információbiztonsággal kapcsolatos intézkedéseket. Ha egy szervezet működésének része a szabályok betartása és követése, a stabilitás megteremtésének és fenntartásának igénye, akkor ez igaz lesz az információbiztonsági területekre is, ami pozitívan fog hatni a szervezet biztonsági érettségére.

2.hipotézis

Olyan Cameron-Quinn szervezeti kultúrák esetében várható fejlett biztonsági szint, amelyek számára fontos a kontrolláltság, szabályozottság.

A felhő alapú megoldások alkalmazása olyan vezetők esetében lesz erős, akik szívesen veszik fel az újító szerepet és alkalmaznak olyan technológiákat, amelyek képesek előmozdítani a szervezet termelékenységét és hatékonyságát. Ezen tulajdonságok ugyanis alapját jelentik az új megoldások bevezetésének és az ilyen vezetők a Cameron-Quinn rendszerében a külső fókusz félsíkban lesznek találhatóak (Cameron & Quinn, 2000).

3.hipotézis

Azon Cameron-Quinn vezetői szerepek esetében nagyobb érdeklődést a felhő megoldások iránt, amelyek nyitottabbak az újdonságra és változásokra.

A negyedik hipotézisben megfogalmazottokat arra építem, hogy ha a szervezetet a kreativitás, az új technológiák alkalmazási lehetőségének keresése, a kockázatvállalás és innováció jellemzi, akkor feltételezhetően széles körben fogja alkalmazni az olyan új technológiákat, amelyek előnyhöz juttathatják.

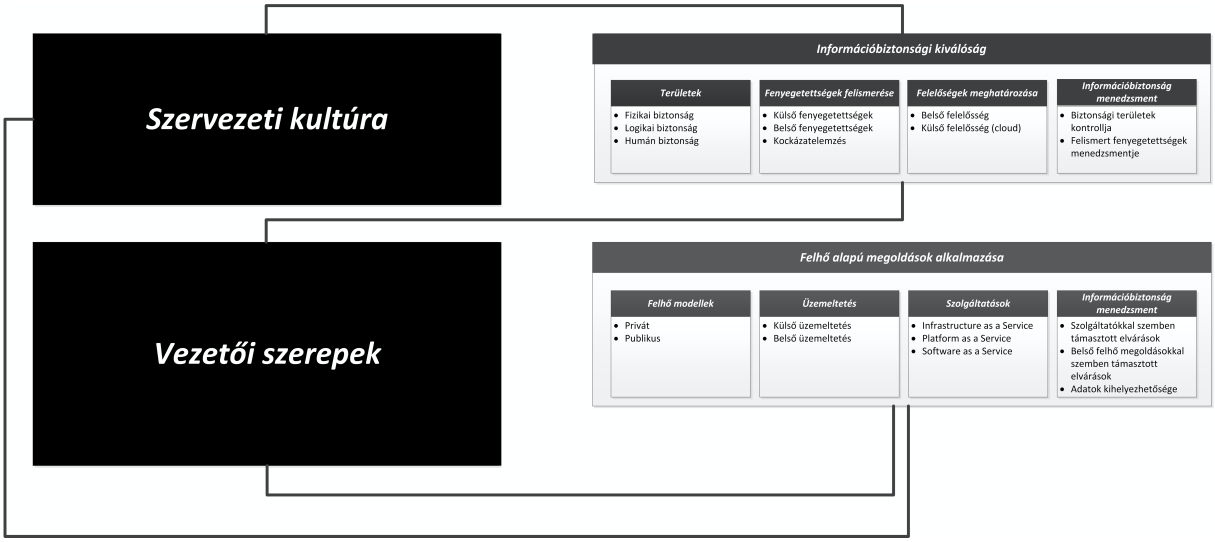
4.hipotézis

A Cameron-Quinn szervezeti kultúrák közül azok esetében aktív a felhő megoldások használata, amelyek fogékonyak az innovációra, az úttörő megoldások bevezetésére.

3.3 A kutatási modell

Az információbiztonsággal és a felhő megoldások alkalmazásával foglalkozó modellek esetében is elmondható, hogy együttes feltérképezésük nem történt meg. Korábbi tanulmányok pl.: (Buecker, et al., 2014; Scholtz , et al., 2016; Sjelin & White, 2016; Bowen & Kissel, 2017; Barrett, 2018) már igyekeztek más tudományágakat (pl.: menedzsment eszközök, tudás megosztás, dokumentum menedzsment) is bevonni vizsgálatukba, de ez csupán apró részterületekre irányult. Kutatásom során olyan modellt alkottam, mely ezt a hiányzó kapcsolatot képes megteremteni a szervezeti kultúra, vezetői szerepek, információbiztonság és felhő megoldások alkalmazása között. Azaz nem csak egy szakmai terület kiegészítése, hanem három egymástól eddig függetlenül kezelt tudományág összefogása valósul meg, melyet a következő modellben jelenítettem meg (1. ábra).

1. ábra: Kutatási modell



A szervezeti kultúrát, valamint a vezetői szerepeket nem bontottam tovább részterületekre, mivel ennek kidolgozását már elvégezték korábban (Cameron & Quinn, 2011), így az általam létrehozott új struktúrára, az információbiztonsági kiválóságra és felhő alapú megoldások alkalmazására helyeztem a hangsúlyt. Továbbá A kultúra és vezető szerepek közötti kapcsolatot számos esetben részletesen vizsgálták az utóbbi években is (Dobi, et al., 2013; Kargas & Varoutas, 2015; Mohelska & Sokolova, 2015; Girma, 2016; Sürücü & Yesilada, 2017; Akanji, et al., 2019), így azok eredményeit elfogadom, munkámban külön vizsgálatukra nem térek ki. A biztonságot azonban négy további területre osztottam fel annak érdekében, hogy vizsgálni tudjam a technikai területeket, fenyegetettséget, felelősséget, valamint menedzsment aspektust is. A felhő vizsgálatát szintén négy részegységre bontottam fel, melyek kitérnek a felhő szolgáltatási modelljére, üzemeltetésre, az igénybevett szolgáltatás típusára és a menedzsmentre. Kutatásom későbbi fázisában arra keresem majd a választ, hogy a szervezeti kultúra és vezetői szerepek milyen hatással vannak az újonnan létrehozott területekre.

3.4 Vizsgálati módszerek

A fejezetben a hipotézisek vizsgálatához kapcsolódó módszereket mutatom be. Kutatásom során mind kvantitatív, mind pedig kvalitatív technikát is alkalmaztam. A kvantitatív kutatás célja objektív, számszerűsíthető, statisztikailag értékelhető adatok gyűjtése, míg a kvalitatív kutatás a problémák azonosítására, hipotézisek felállítására szolgál. Így pedig nem nyújt bizonyító erejű eredményeket, csupán segít megérteni a folyamatokat, rámutat a feltárt viselkedési mintákra. A megfogalmazott kutatási kérdések megválaszolásához, valamint ez alapján meghatározott hipotézisek igazolásához leginkább megfelelő a feltáró jellegű vegyes kutatásmódszertan (Creswell & Plano Clark, 2010).

3.4.1 Kvalitatív felmérés

Kvalitatív kutatást akkor lehet sikeresen alkalmazni, ha a kiváltó okokat és összefüggéseket nem, vagy csak részleteiben ismerjük (Lippert, et al., 2015; Babbie, 2017). Kutatásom során a félig strukturált interjút alkalmaztam. Félig strukturált interjú: melynek kérdéssorát úgy állítottam össze, hogy azokra adott válaszok segítséget nyújtsanak szűkíteni vizsgálatom területeit, valamint a későbbi kérdőíves lekérdezés alapjául szolgálhasson. Célom volt, hogy az interjú egy előre definiált kérdéssor mentén történjen, de megadva a lehetőséget az interjú alany számára a nyitott kérdések révén, hogy válaszát kifejtse, esetleg az érintett témákat kibővítse (Kvale, 2014). További segítséget jelent, hogy a nem egyértelmű válaszok esetén lehetőséget biztosít a további kérdések feltételében így pontosítva a válaszadó által átadni kívánt üzenetet (Jensen & Laurie , 2016). Az esettanulmányomban egy magyarországi telekommunikációs vállalat működését vizsgáltam, valamint dolgoztam fel. Célom volt, hogy feltárjam, milyen változásokat okoz a szervezet kultúrájában és vezetésében egy-egy információbiztonsági kérdés felmerülése és kezelése, valamint milyen hatással van a felhő alapú megoldások alkalmazása, különös tekintettel a privát és publikus felhő jelentette különbségekre. Természtesen nem tekinthettem el attól, hogy feltehetően a kultúrától és a vezetői szerepektől a biztonsági terület fejlettsége, az alkalmazott megoldások, továbbá a felhő szolgáltatásokra való nyitottság is függ. Tehát az egymásra hatás nem egyirányú, így a teljes reláció vizsgálata javasolt. A magyar piacon tevékenykedő, több mint 500 főt foglalkoztató telekommunikációs vállalatok száma alacsony, valamint a meghatározó szereplők mind leányvállalatok, így működésük és felépítésük mutat hasonlóságokat. Elmondható, hogy az esettanulmányom megállapításai nem általánosíthatók teljes mértékben, azonban számos tekintetben igaznak bizonyulnak a szektor egészére.

Esettanulmányomban megfogalmazott kérdések megelőzték a disszertáció kérdéseit, mivel célom volt, hogy az esettanulmány lefolytatását követően az ott megkapott eredményeket felhasználva tovább finomítsam kutatásom irányát. Szerettem volna látni azt, hogy a különböző tudományterületek között mely kapcsolatok azok, amelyeket érdemes mélyebben és szélesebb körben vizsgálni. Továbbá be akartam azonosítani, hogy az információbiztonság témakörét milyen mélyen érdemes vizsgálni egy ilyen komplex modell esetében.

Esettanulmány kutatási kérdései

- EK1: Milyen biztonsági elvárásokat támasztanak a vállalatok a felhő alapú alkalmazásokkal szemben?
- EK2: Hogyan hat a felhő alapú működés az információbiztonság menedzsmentjére?
- EK3: Milyen változásokat okoz a szervezeti kultúrában és a vezetői szerepekben az információbiztonsági kérdés felmerülése és kezelése?
- EK4: Milyen változásokat eredményez a szervezeti kultúrában és a vezetői szerepekben a felhő alapú megoldások alkalmazása?

3.4.2 Kvantitatív felmérés

A változók közti ok-okozati kapcsolatok meglétét és annak erősségét írja le a kvantitatív elemzés (Lippert, et al., 2015; Babbie, 2017). A változók esetében alapfeltevés, hogy mérhetőnek kell lenniük, ezért kérdőívem elkészítése során többnyire eldöntendő kérdéseket, vagy állításokat szedtem össze. Ebből kifolyólag lehetőség nyílt a válaszok mérhetőségének megteremtésére, ezáltal pedig egyszerűsítve a későbbi fázisok végrehajtását. Az adatok gyűjtésére összeállított kérdőívet emailben küldtem ki és a beérkező válaszokat egy excelbe összesítettem. A következő módszereket használtam az adatelemzés során:

- **Főkomponens analízis:** a módszerrel a változókat lineáris transzformáció segítségével egy az eredetinél kisebb számú új változóvá lehet átalakítani. Cél az információ mennyiségének legnagyobb részét megőrizni (Barna & Székelyi, 2008). Munkám során a vezetői szerepek meghatározásánál használtam;
- **Faktoranalízis:** alapja, hogy az eredeti változókat, illetve a vizsgált rendszere vonatkozó adatokat sűrített formában szolgáltatja, kevesebb számú faktor segítségével. Különbsége a főkomponens analízishez képest, hogy a faktorokat az eljárás végén értelmezni kell (Barna & Székelyi, 2008). Fontos, hogy az értelmezhetőség miatt nem tartalmazhat közös indikátorokat. Az információbiztonsági kiválóság és felhő alapú megoldások alkalmazásának érettségi szintjének definiálásához használtam;
- **Varianciaanalízis:** segítségével egy (vagy több) független változó hatása vizsgálható egy (vagy több) függő változóra (Sajtos & Mitev, 2007). A szervezeti kultúra és vezetői szerepek információbiztonságra és felhő alapú megoldások alkalmazására gyakorolt hatásának vizsgálatakor alkalmaztam;
- A megkapott eredményeket hibaoszlop segítségével jelenítettem meg.

4 Empirikus kutatás

Munkám következő részében bemutatom a kutatás folyamatát, az alkalmazott módszereket, melyek segítségével mérhetővé tettem a változókat, valamint azok összefüggéseit. Ismertetem az interjúk és a kérdőíves lekérdezés gyakorlati kivitelezését.

4.1 A kutatás folyamata

Az empirikus vizsgálataimat megelőzte a kutatás céljainak meghatározása, a kutatási kérdések megfogalmazása, valamint a szakirodalmi vonatkozások áttekintést. A modellem szervezeti kultúra és vezetői szerepek dimenzióinak mérési módszere rendelkezésre állt korábbi tanulmányok alapján, azonban az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazása tekintetében ezen mérési eszközök nem voltak elérhetőek megfelelő formátumban, így szükség volt létrehozásuk. Ezt követően interjúkkal kombinált kérdőíves vizsgálatot folytattam le, melynek lépései: (1) empirikus kutatás előkészítése, (2) empirikus kutatás alapjául szolgáló információk összegyűjtése (félig strukturált interjúk, valamint kérdőíves legkérdezés), (3) trianguláció, (4) empirikus információk elemzése és értékelése, (5) kutatási eredmények összefoglalása és általánosítása (korroborácó), (6) kutatási hipotézisek értékelése.

4.1.1 Az empirikus kutatás előkészítése

A kutatás előkészítési szakaszában a kombinált megközelítés értelmében két eltérő előkészítésre volt szükség.

A félig strukturált interjúk esetében célom volt, hogy a vizsgálni kívánt területeket és személyeket a lehető legjobban megismerjem. A kutatás személyes és érzékeny információkat is érint ezért úgy gondoltam, hogy szükséges egy tájékoztatót tartanom a vizsgált személyek számára, ahol ismertettem a kutatás célját, annak menetét. Ezzel kapcsolatosan a felmerült kérdéseket, esetleges aggályaikat tudták megosztani és megnyugtató választ adtam számukra.

A kérdőíves lekérdezés más előkészítő munkát igényelt, mivel ebben az esetben személyesen a vizsgált sokaságot elérni nem tudtam, de mégis szükségesnek tartottam, hogy kommunikáljam a kutatás célját és lehetőséget biztosítsak számukra a későbbi eredmények elérésében. A kérdőív kidolgozását megelőzte és nagyban segítette a félig strukturált interjúk eredményeit felhasználva elkészült esettanulmány.

Mind a félig strukturált interjúkat, mind pedig a kérdőíves lekérdezést megelőzték próba interjúk, mellyel az adatgyűjtés módját kívántam tesztelni. Emiatt egy fővel lefolytattam az interjút, valamint öt fővel a kérdőíves lekérdezést végeztem.

4.1.2 Az empirikus kutatás alapjául szolgáló információk összegyűjtése

A kérdőív létrehozásakor kiemelt figyelmet fordítottam arra, hogy kitöltése ne okozzon nehézséget a válaszadóknak így megelőzve az alacsony kitöltési hajlandóságot. A kérdőívet három részre osztottam, ezáltal a vizsgálni kívánt szervezeti kultúra, vezetői szerepek, információbiztonság és felhő megoldások témakörét is lefedi. Az első részben a szervezeti kultúrával kapcsolatosan a Cameron-Quinn féle Versengő Értékek keretrendszert alkalmaztam (Cameron & Quinn, 2011). A kitöltők feladata volt, hogy a szervezetet jellemző domináns karakterisztikák, a szervezeti irányítás, a vezetési stílus jellemzői, a szervezetet összetartó erő, a stratégiai hangsúlyok és siker kritériumok esetében minden csoportban 100 pontot osszanak szét négy állítás között aszerint, hogy melyik írja le legpontosabban a válaszadó elképzelését, valamint véleményük szerint mely lenne a kívánatos. A vezetői szerepek felméréséhez szintén a Versengő Értékek Keretrendszert alkalmaztam annak érdekében, hogy egységes rendszerben vizsgálhassam a menedzsment tulajdonságokat (Quinn, 1996). A 30 felsorolt vezetői tevékenységgel kapcsolatosan arra voltam kíváncsi, hogy azt milyen gyakorisággal végzik a vezetők és mennyire tartanák kívánatosnak a jövőre nézve a válaszadók.

A kérdőív második részében az információbiztonságon belül vizsgáltam, hogy milyen érettséget mutat a szervezet a területek, fenyegetettségek felismerése, felelőségek meghatározása és információbiztonság menedzsment dimenziókban. A kérdőív létrehozásakor minden dimenziót tovább bontottam, melyekre vonatkozóan kértem meghatározni egy 1-7ig terjedő Likert skálán az adott területen tapasztalt jelenlegi és vállalat jövőben kívánatos értékét.

Harmadik részben a felhő alapú megoldások alkalmazását dolgoztam fel, melynek részeként vizsgáltam az alkalmazott felhő modellt, üzemeltetés formáját, igénybevett szolgáltatások körét és az információbiztonság menedzsmentjét. Az információbiztonsághoz hasonlóan a jelenlegi és kívánatos állapotot kértem értékelni egy 1-7ig terjedő Likert skálán a kérdőívet kitöltőktől Az interjúk során alkalmazott kérdéseket az 1. melléklet tartalmazza..

4.1.3 Trianguláció – az érvényesség többszempontú alátámasztása

Kutatásom során csupán egyetlen vállalaton belül folytatott félig strukturált interjúk túlzott egyszerűsítést tennének lehetővé, így pedig a szervezeti kultúra, vezetői szerepek, információbiztonság és felhő megoldások alkalmazásának vizsgálatát deformálná. Kutatásom esetében azonban fontos, hogy a kapott eredményeket validáljuk, azaz az érvényességet többszempontból is alátámasszuk, melyre számos módszer létezik (Horváth, 2018; Denzin, 2016; Szokolszky, 2004; Sántha, 2017; Sántha, 2015). Kutatásom során az adat és a módszer triangulációt alkalmaztam. Az adatbegyűjtés két szálon történt meg, melynek első fázisában félig strukturált interjúkat folytattam le egy magyarországi vezető telekommunikációs nagyvállalatnál, mely keretében az alkalmazás üzemeltetésért, az alkalmazás fejlesztésért, az infrastruktúra fejlesztés és üzemeltetésért, a végfelhasználói támogatásért, a

szabályozásért és az információbiztonságért felelős vezetőket, valamint közvetlen beosztottjaikkal vontam be a vizsgálatba. Így összesen 92 fővel készültek személyenként 70-80 perces interjúk, melyek célja, hogy megalapozzák a későbbi adatgyűjtési irányokat és a már elkészített kérdőív finomhangolásában is segítséget nyújtsanak. Azért volt szükség ilyen nagy számú elemre az esettanulmány során, mivel a kiválasztott cég esetében szerettem volna a teljes sokaságot lekérdezni, hogy a megkapott eredmény az adott vállalat esetében reprezentatív legyen. Ezen túlmenően, mivel a későbbi kutatásom irányát is a levont következtetésekre kívántam alapozni, így el szerettem volna kerülni, hogy bármilyen aspektus is kimaradjon. Ezen túlmenően a mintában voltak olyan kis csoportok pl. Stratégia és Szabályozás, Információbiztonság, valamint maguk a vezetők, hogy ha a minta csupán egy részét kérdeztem volna le ez a kis szám tovább csökken, így pedig előfordulhatott volna hogy fontos vélemények kimaradnak az értékelésből torzítva a teljes képet.

A kutatásom második szakaszában az adatgyűjtés kiegészült kérdőíves lekérdezéssel, mely a magyarországi telekommunikációs szektort célozta meg és eredményeként 219 fő esetében sikeres adatgyűjtés valósult meg. A kérdőívek kiküldését több csatornán hajtottam végre, mivel célom volt, hogy minél nagyobb számú sikeres kitöltés valósuljon meg. Ezek alapján a kérdéslita kiküldése történt emailt, Linkedin és Facebook csatornákon is, ahol magát a kérdőívet tartalmazó linket a surveymonkey.com-on hoztam létre.

4.1.4 Az empirikus információk elemzése és értékelése

A félig strukturált interjúk során a készített jegyzetek feldolgozásához szövegelemzést alkalmaztam, amelynek során az első lépésként az elemzési egységet határoztam meg, ami esetemben az egyes kérdések voltak. Majd meghatároztam, hogy mire fektetődött a hangsúly, illetve a vizsgálni kívánt területeket milyen gyakran jellemeztek azonos módon.

A kérdőíves lekérdezés eredményeinek elemzése során szervezeti kultúra és a vezetői szerepek, illetve azok komponensei, mint magyarázó változók és az információbiztonsági kiválóság, valamint a felhő megoldások alkalmazásának komponensei, mint magyarázott változók közötti feltételezett kapcsolat vizsgálatát valósítottam meg. A szervezeti kultúra méréséhez az OCAI kérdőívet használtam, amelyet az 5.2.2–es fejezetben tárgyalok bővebben. A kérdőív hat dimenzió alapján vizsgálja a szervezetek kultúráját, minden dimenzió esetében 4-4 állítást határoztak meg, melyek között a kérdőívet kitöltő 100 pontot oszt ki. Ez alapján történik meg a vizsgált szervezet kultúra típusba sorolása. A vezetői szerepek méréséhez a kibővített Cameron-Quinn modell vizsgálatát kellett elvégezni. Az egyes vezetői jellemzőket egy 7 fokú Likert skálán értékelem. Az értékelés történhet számtani átlag, esetleg súlypont meghatározásával. A módszer valamelyest eltér a domináns kultúra meghatározásától, mivel az értékelés során nincsenek összekötve az egyes tulajdonságok. Azaz a minősítés nem egymás rovására

történik *(korábban 100 pontot kellett szétosztani)*. Ennek figyelembevétele azonban rendkívül fontos, mind a két felmérés esetén irányítani kell a kitöltő gondolkodását.

Az információbiztonsági kiválóság méréséhez korábbi kutatásom és a szakirodalomban elérhető felmérési módszerek szolgáltak alapul. A meghatározott négy dimenzió az egyes érettségi szinteknek (Kezdeti/ad-hoc, Szabályozott, Irányított és mérhető, valamint Optimalizált) felelnek meg. A kérdőíves felmérés során megkapott értékek határozzák meg, hogy mely érettségi szint a domináns a szervezetben.

A felhő alapú megoldások alkalmazásának mérési rendszerét az információbiztonsági érettség méréséhez hasonlóan alakítottam ki, azaz meghatározásra kerültek az érettségi szintek (Minimális vagy nem létező, A működésben megjelent, Mindennapi működés részévé vált, valamint a Jövő a felhő megoldás).

4.1.5 A kutatási eredmények megfogalmazása és általánosítása (korroboráció)

A kutatási eredmények elsődleges megfogalmazása az empirikus kutatás eredményeinek értékelését követően történik meg. Azonban ezek még nem nevezhetők véglegesnek és minden esetben érvényesnek. Ahhoz, hogy ezt meg tudjam tenni szükséges a korroboráció módszerének alkalmazása (Plutchik, 1991). Korroboráció a kapott információ helyességének ellenőrzése, mely történhet a kutatásba bevont személyek visszajelzései alapján vagy ismétlődő tesztelések keretében (Tashakkori & Teddlie , 2002). A kutatás során a korroboráció lebonyolításába a teljes sokaság bevonása megtörtént két lépésben. Első körben a félig strukturált interjúban részt vett alanyok segítségével a szélsőséges eredmények kiszűrését végeztem el, majd pedig a kérdőíves felmérésben részt vett válaszadók is bevonásra kerültek az eredmények megosztása révén, ahol szintén lehetőség nyílt a visszajelzésre. Az így kiszűrt értékek törlését követően nyílt lehetőség a kutatási eredmények általánosítható megfogalmazására, majd a kutatási hipotézisek végső értékelésére.

4.2 A változók operacionalizálása

Az empirikus elemzés során olyan adatokra van szükség, amelyeket mérhetővé tudom tenni annak érdekében, hogy később értékelésük megtörténhessen. A kérdőíves vizsgálat esetében is szükség van az operacionalizálásra, hiszen ennek hiányában nem tudnám elvégezni a hipotézisek tesztelését sem.

A kérdőíves technikai használatakor háromféle módon számszerűsítettem az adatokat, annak függvényében, hogy mire szeretném őket felhasználni. Az első kategória a tulajdonságok voltak, ahol olyan nominális változókhoz jutottam, amelyek az adatállomány szűrését, csoportosítását tették lehetővé, valamint különféle leíró statisztikák előállítására adtak lehetőséget.

A kérdőíves felmérés további részénél törekedtem arra, hogy magas mérési szintű változókhoz jussak, ezért az információbiztonsági kiválóság és a felhő alapú megoldások esetében 1-7-ig skálázott, hétfokú Likert skálán végeztem el. A Likert skála esetében egyenlő szakaszokra osztott intervallum skáláról beszélhetünk, így a különbségek összehasonlíthatóvá vállnak (Sajtos & Mitev, 2007; Lippert, et al., 2015).

A szervezeti kultúra és vezetői szerepek felmérése a Cameron-Quinn Versengő értékek keretrendszerének segítségével történ meg, ahol követtem a módszer kidolgozóinak az útmutatását (Cameron & Quinn, 2006; Cameron & Quinn, 2011). A szervezeti kultúra esetén a kérdőív létrehozásakor minden kultúra típus esetében 4-4 állítást szerepel, melyek között a kérdőívet kitöltő 100 pontot oszt ki. Ez a 100 pont kiosztása történhet a 4 állítás között (bizonyos súlyok meghatározásával), de akár egyetlen állítás is minősíthet 100 ponttal. A meghatározott négy dimenzió az egyes kultúra típusoknak (A = klán, B = adhokrácia, C = piac, D = hierarchia) felelnek meg. A módszer magas mérési szintű változót eredményez.

A vezető szerepek esetén szintén egy 7 fokú Likert skálát alkalmaztam, ahol 32 kérdésre válaszolva kellett meghatározni, hogy vezető a megkérdezett tevékenységet milyen gyakorisággal végzi el. A módszer szintén magas mérési szintű változót eredményez.

4.3 A kutatás alapjául szolgáló sokaság

4.3.1 Vizsgált iparág bemutatása

Kutatásom során olyan iparágat kívántam kiválasztani, amely élen jár a modern technológiák alkalmazásában, valamint működése és nyújtott szolgáltatásai erősen építenek ezen megoldásokra.

Az iparág kiválasztása során figyelembe vett kritériumok:

- Havi díjas szolgáltatást biztosítsanak ügyfeleiknek a szervezetek, mivel így nem befolyásolja a szervezet működését a szezonalitás, valamint az évente változó méretű megrendelési állományból fakadó szervezeti hatások. Ezért egy konstans, működésében állandónak tekinthető szervezet vizsgálata történhet meg.
- Dinamikusan változó, kiélezett piaci verseny jellemzi, mely elengedhetetlen ahhoz, hogy az új technológiákra való nyitottságot vizsgálhassam, mivel egy ilyen környezet rákényszeríti és egyben ösztönzi a vállalatokat arra, hogy folyamatosan olyan új megoldásokat keressenek és vezessenek be.

Ezen elvárások figyelembevétele mellett úgy döntöttem, hogy a magyarországi telekommunikációs szektort vizsgálom, mely révén egy olyan iparág működésébe nyertem betekintést, mely élen jár a modern technológiák alkalmazásában, valamint működése és nyújtott szolgáltatásai erősen építenek ezen megoldásokra. A telekommunikációs iparág az egyik legdinamikusabban változó szektor, így szervezeti struktúrájuk és működésük gyakran átalakításra kerül, ezáltal pedig ideális vizsgálati területet biztosítanak.

Esettanulmány során kiválasztott szervezet esetében figyelembe vett további kritériumok:

- Szervezeti átalakulás előtt vagy alatt álló, esetlegesen az átalakulást már lezárt szervezet legyen, de a végső struktúra még nem idősebb, mint fél év. Ezen kritérium hozzásegített ahhoz minket, hogy ne csak egy már meglévő struktúrát és viszonyokat legyünk képesek vizsgálni, hanem annál egy jóval izgalmasabb, változó környezetben történhessen meg felmérésünk. Az így szerzett adatok későbbi kutatásunk során is felhasználhatók és segítik megérteni a szervezetek részletesebb működését.

A fenti kritérium lehetőséget teremt továbbá arra, hogy egy átalakulási folyamat részeseként vizsgálni tudjam a korábbi és az új szervezeti struktúra közötti különbségeket, annak hatásait a mindennapi működésre. Ezáltal pedig kitágítva az esettanulmány időbeliséget elérve, hogy nem csak a jelenlegi állapot felmérésére alkalmas.

4.3.2 Választott minta

Kvalitatív kutatás (esettanulmány) során választott minta

Az adatgyűjtés során kvalitatív módszert használtam, mivel célom volt, hogy az IT szervezet gondolkodásmódját és várható reakcióit mélyebben megértsem. A strukturált interjúkat az IT és az információbiztonság menedzsmentjéért felelős területeket irányító összes menedzserrel és direkt riportjukkal (92 interjú alany) lefolytattam annak érdekében, hogy teljes képet kapjak a szervezet állapotáról. A vizsgálatot 2018. május – augusztus között végeztem el és vizsgálati egységnek az IT egyes részterületeit tekintettem. Az 5. táblázatban összefoglaltam a kutatásba bevont területeket, azok felelőségi körét, valamint a csapat méretét.

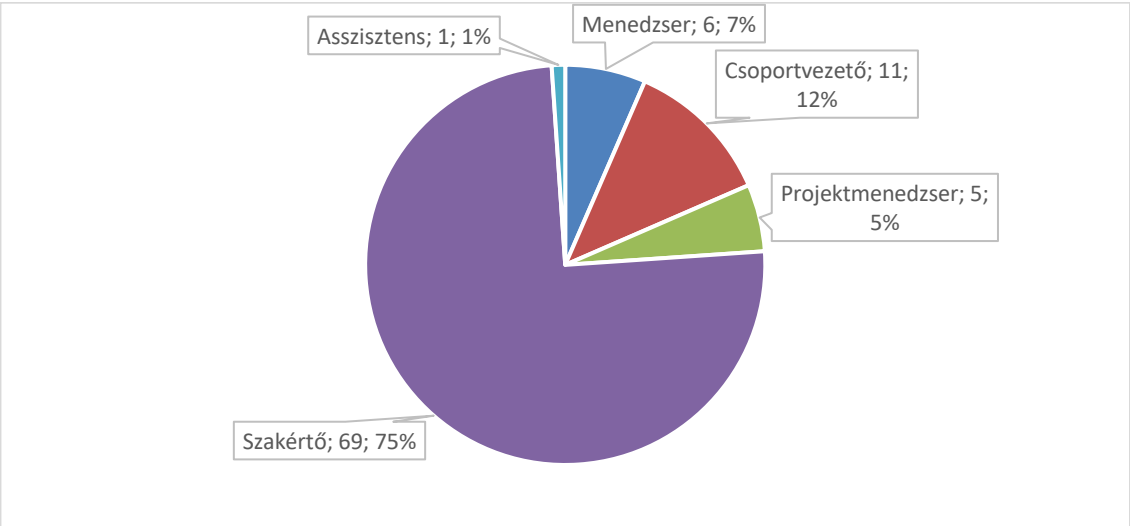
5. táblázat: A kvalitatív strukturált interjú minta jellemzői (N=92)

Azonosító	Terület	Felelőség	Terület mérete
VA1	Alkalmazás üzemeltetés	A vállalatnál működő alkalmazások üzemeltetése, támogatása mind belső, mind pedig külső erőforrások igénybevétele mellett.	15 fő + külső szállítók
VA2	Infrastruktúra fejlesztés és üzemeltetés	A vállalat hálózat, tűzfal, szerver, storage, adatbázis, middleware mentési rendszereinek üzemeltetése és bővítések, új rendszerek üzembe helyezése.	25 fő + külső szállítók
VA3	Alkalmazás fejlesztés	Üzleti területek és alkalmazás üzemeltetés által támasztott fejlesztési igények priorizálása és kiszolgálása.	25 fő + külső szállítók
VA4	Végfelhasználó támogatás	L1 helpdesk feladatok ellátása, beleértve a beérkező hibajegyek az érintett alkalmazás és infrastruktúra L2-L3 szintek felé történő továbbítása.	20 fő
VA5	Stratégia és Szabályozás	Pénzügyi koordináció, szabályozási és audit feladatok ellátása.	5 fő
VA6	Információbiztonság	Sérülékenységi vizsgálatok lefolytatása, feltárt hiányosságok menedzsmentje az alkalmazás és infrastruktúra csapatokkal közösen. Megjelenő biztonsági kockázatok vizsgálata, értékelése és indokoltság esetén az érintett területekkel védelmi megoldás kidolgozása, bevezetése.	2 fő

Az alapsokaság méretének megállapításakor célom volt, hogy ne csupán az IT szervezet egy részét mérjem fel. Ezért a teljes 92 fős mintán folytattam le a strukturált interjúkat. A vizsgálatban összesen 18 nő és 74 férfi vett rész, akik átlagéletkora 38,82 év.

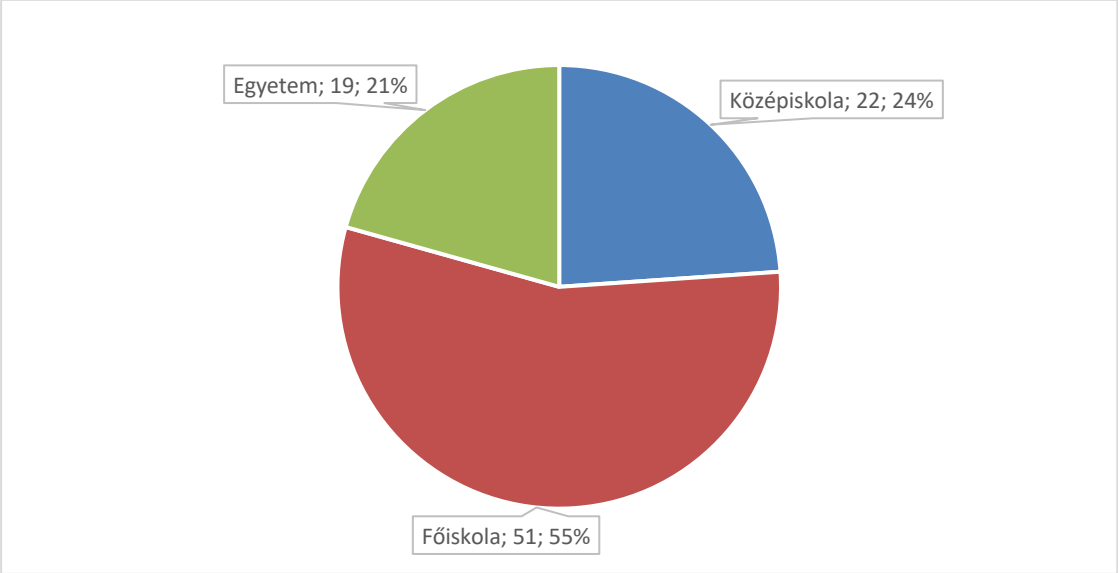
Jelenlegi pozíciójuk szerint 6 fő, mint menedzser, 11 fő, mint csoportvezető, 5 fő, mint projektmenedzser, 69 fő, mint szakértő és 1 fő asszisztensként dolgozik.

2. ábra: A minta munkakör szerinti megoszlása



A vizsgált mintában a végzettség eloszlása változatos. 24% fejezte be tanulmányait középiskolát követően, 55% főiskolai, míg 21% egyetemi diplomát is megszerezte.

3. ábra: A minta végzettség szerinti megoszlása



Az esettanulmány során vizsgált minta részletes adatait a 2. melléklet tartalmazza.

Kvantitatív kutatás (kérdőív) során választott minta

A minta meghatározása során már az esettanulmány megválasztásakor alkalmazott megközelítést követtem, azaz minél nagyobb számú IT szakember és vezető megkérdezése volt a célom szervezetenként. A statisztikai számításhoz szükséges, hogy a lehető legnagyobb mintán hajtsam végre az összefüggések vizsgálatát. A magyarországi telekommunikációs szektor jellemzője, hogy néhány

nagy vállalat mellett még mindig sok kis kábelszolgáltató működik, akik pár ezer vagy tízezer lakossági ügyféllel rendelkeznek egyenként. Valószínű azonban, hogy öt év múlva nem lesz ennyi kis szereplő a piacon. Ezt a folyamatot támasztják alá a nemzetközi trendek is, melynek fő oka, hogy az iparágban magas a folyamatos beruházási igény, melynek költséghatékonyságához és megtérüléséhez szükséges a megfelelő ügyfélállomány birtoklása.

Az egész országra kiterjedő felmérésben minden olyan vállalat szakértőit és vezetőit megkerestem, amelyek elérték a minimum 500 fő foglalkoztatási határt. Erre azért volt szükség, mivel ezen méret alatt azt tapasztaltam, hogy nem volt kiterjedt IT szervezet, így pedig nehéz lett volna mérni az egyes vizsgálni kívánt területek közötti hatásmechanizmust. Az anonimitás megtartása mellett is elmondható, hogy minden, a magyar piacot meghatározó szereplő esetében sikerült adatgyűjtést megvalósítani (minimum 20 munkavállaló cégenként), továbbá a teljes vizsgálat során 219 sikeresnek tekinthető kérdőíves lekérdezést hajtottam végre. A KSH 2019-es adatai alapján infokommunikációs és kommunikációs szektorban 132.000 munkavállaló volt foglalkoztatva, melynek csupán egy része (átlagosan kb. 5-10%) dolgozik IT területen, ami így 13.200 főt jelentene (Központi Statisztikai Hivatal, 2019). Azonban ezek egy jó része kis és középvállalatok, valamint IKT-feldolgozóipar és egyéb IKT szolgáltatások alkotják, amelyek nem része a telekommunikációs szektornak. Ezért a fenti számot tovább kell csökkenteni, ha csupán a telekommunikációs vállatokra vagyok kíváncsi. Így azt feltételezem, hogy kb. 2.000-2.500 fő dolgozhat IT területen a vizsgált szektoron belül.

5 Vizsgálati eredmények

A fejezetben bemutatom a kvalitatív vizsgálat eredményeként létrehozott esettanulmányomat, rendszereztem a megkapott adatokat és választ adtam az esettanulmány keretében feltett kérdésekre. Ezt követően a kvantitatív vizsgálattal folytattam, ahol kitértem a szervezeti kultúrákkal, majd a vezetői szerepekkel kapcsolatos eredményekre. Meghatároztam a vizsgált sokaság érettségi szintjeit az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazásának területeire vonatkozóan. Feltártam a változók közötti kapcsolatokat, ellenőriztem a hipotézisek helytállóságát és kimondtam a kutatási téziseimet.

5.1 Kvalitatív vizsgálat

A vizsgálat során félig strukturált interjút választottam az összefüggések feltárása, valamint kutatási irányok pontosítása és szűkítése érdekében. Az interjú során használt kérdéseket a 11. melléklet tartalmazza.

5.1.1 Esettanulmány értékelése

Felhő alapú megoldások információbiztonsági követelményei és szervezeti hatásai (EK1, EK2, EK4)

A szakirodalomban fellelhető, a felhő megoldások használatát alátámasztó előnyök, azaz a könnyű skálázhatóság, rugalmasság, jó automatizálhatóság, magas rendelkezésre állás fontossága a kvalitatív eredményeimben is megjelennek. A költséghatékonyságot azonban nem emelték ki a válaszadók, ami arra enged következtetni, hogy a rugalmasság és a stabilitás iránti igény elsődleges szempontot képvisel.

> „A könnyebb működtetés, egyszerűbb számonkérés, rugalmas skálázhatóság és számos automatizálási lehetőség olyan előnyök, melyek szervezetünk számára kritikusak. A felhő megoldások lehetőséget biztosítanak a homogén működésre és működtetésre.” (VA2)
>
> „Központilag egyszerűbb menedzselésük és elosztott kialakításukból fakadóan stabilitásuk is kimagasló tud lenni.” (VA1)

Az előnyök mellett kritikus kérdés volt számukra a megfelelő felhő modell (privát, publikus, hibrid, közösségi), a szolgáltatás típus (IaaS, PaaS, SaaS, etc), a szolgáltató kiválasztása, továbbá az üzemeltetési modell tisztázása (külső, belső).

> „A piacon rengeteg megvalósulással találkozni attól függően, hogy a felhőt házon belül építik fel, vagy pedig külső szolgáltatótól vásárolják meg. Mi ennek ötvözését biztosító hibrid megoldásban látjuk az IT jövőjét.” (VA2)
>
> „Így lehetőség nyílik arra, hogy a kritikus adatokat házon belül tartsuk, de a szabadon hozzáférhető, rugalmas kapacitások elérésében rejlő előnyöket is kihasználhassuk.” (VA6)

Az információbiztonság menedzseléséért felelős terület feladatai azonban átalakultak, amikor a felhő alkalmazásának lehetőségét kezdték el vizsgálni. Már nem volt ugyanis elég egy belső ellenőrző

szervezetként való megjelenésük. Ehelyett tanácsadó, ellenőrző, jogi megfelelésben aktívan részvevő és folyamatos kontrollt gyakorló szervezetté kellett válnia egy olyan környezetben, ahol nem minden esetben képes hatni a külső szolgáltatókra. A korábbi kontroll szerep tehát egy használható megoldást javasló működés felé kezdett elmozdulni, de természetesen korábbi funkciójuk sem tűnt el.

> „Az információbiztonság fókusza arra irányult a külső felhő szolgáltatók megjelenése előtt, hogy rendszereinket a külvilágtól a lehető legjobb módon elzárjuk és megvédjük." (VA6)
>
> „A menedzsment és üzemeltetés által generált új igények azonban rákényszerítettek minket a változásra, mivel a publikus felhőből kiszolgált megoldások használata számos előnyt hordozott magában, így használatuk elkerülhetetlenné vált." (VA5)
>
> „Ahhoz, hogy meg tudjunk felelni az új szervezeti igényeknek, merőben új kompetenciák felépítésére volt szükség. Belső ügyfeleink számára segítséget kellett nyújtanunk, hogy melyek azok a felhő alkalmazások, amiket használhatnak, és melyek azok, amelyek problémát jelenthetnek hosszú távon. Ennek meghatározása önmagában azonban nem elég. Definiálni kellett ugyanis azon adatköröket, amelyek a publikus felhőbe ideiglenesen vagy véglegesen „kihelyezhetők" és azokat, amelyek csak a belső privát megoldásban tárolhatók." (VA6)

A megjelenő új feladatok ellátása azonban indokolttá tette a létszám növelését az információbiztonság területén. Ehhez a folyamathoz azonban időre volt szükség, mivel a menedzsment nem minden esetben látta, vagy fogadta el ennek szükségességét.

> „Csapatunk létszámát csak azután tudtuk növeli, hogy a belső üzleti ügyfelek önállóan olyan felhő megoldásokat kezdtek el használni mindennapi munkájukhoz, melyekről nem volt tudomásunk. Nem gyakoroltunk kontrollt, valamint üzletileg kritikus adatok kerültek ki szervezeten kívülre. Ezen esetek egyre gyakoribb felbukkanása ösztönözte arra a vezetőket, hogy újra pozícionáljak az információbiztonság területét és annak szerepét a vállalati struktúrában." (VA6)

A külső felhő szolgáltatás igénybevételének feltétele volt, hogy megfeleljen a belső biztonsági elvárásoknak, jogi és szabályozási környezetnek. Nehézséget jelentett, hogy ez csak a belső szolgáltatásokra állt korábban rendelkezésre. Ezért ki kellett dolgozni azon feltételeket, sztenderdeket, biztonsági elvárásokat, amelyek mellett használhatóak a publikus megoldások. Fontos figyelembe venni, hogy ezen szolgáltatások esetében Európai Unión kívüli és belüli adattárolás GDPR szempontjából jelentősen eltérhet. A meghatározott elvárások között szerepelt:

- Biztosítson egy elkülönített, a vállalat számára fenntartott felhő szeletet (tenant);
- Történjen meg mikroszegmentáció;
- Lehessen meghatározni és korlátozni az adatok tárolásának földrajzi helyét;
- Legyen lehetőség arra, hogy a felhőben futó saját alkalmazások biztonsági tesztelése megvalósulhasson, kitérve a felhő szolgáltatási rétegre is.

Az ENISA 2016-os Exploring Cloud Incidents tanulmánya a standardok jelentőségét hangsúlyozta, amire való törekvés a vizsgált szervezetnél is megjelenik. Definiálásra kerültek un. „building block"-ok, biztonsági ajánlások és elvárások, melyek használata kötelező a saját privát felhő építése, bővítése során. Az információbiztonság menedzselésért felelős terület számára minden publikus felhő alapú szolgáltatás igénybevétele előtt kötelező ellenőrizni azok megfelelőségét, és jóváhagyásuk nélkül alkalmazásuk nem lehetséges. Annak érdekében, hogy ne csak szabályozási szint valósuljon meg, ezért belső hálózatból minden, korábban még nem engedélyezett felhő alapú megoldás elérése tiltásra került, így biztosítva a kontroll meglétét.

> „Meghatároztunk három biztonsági szintet az üzemeltetési, információbiztonsági, jogi területekkel együttműködve, annak érdekében, hogy adatainkat bizalmasságuknak megfelelő rendszerben tudjuk kezelni:
>
> 1. Magyarországról kiszolgált, privát felhő. Ebben az esetben az adatok nem hagyják el a vállalat adatközpontjait;
> 2. Nemzetközi privát felhő. A kiszolgáló infrastruktúra több országban (pl.: Magyarország, Hollandia, Németország, Anglia) található, de a vállalat adatközpontjaiban;
> 3. Nemzetközi hibrid felhő. A belső erőforrásokon túl külső publikus felhő szolgáltatókat használ a terhelés és igények függvényében." (VA5, VA6)
>
> „Olyan korlátozásokat építettünk a belső rendszereinkbe, melyek megakadályozzák belső ügyfeleinket abban, hogy publikusan működő szolgáltatásokat vegyenek igénybe jóváhagyásunk nélkül. Erre azért volt szükség, mivel az üzleti területek esetében számos esetben tapasztaltuk, hogy a belső szabályozást megszegve használnak külső szolgáltatásokat (p.: Google Drive, Slack, stb)" (VA2)

Az interjúk során kiemelték, hogy Magyarország csak korlátozottan vesz igénybe publikus felhő szolgáltatásokat, mivel azt biztonsági és jogi oldalról aggályosnak tartják, azonban a nemzetközi privát felhő felhasználásában, valamint kiszolgálásában nagy lehetőségeket látnak.

> „A GDPR-nak való megfelelésre történő felkészülésünk része, hogy megvizsgáljuk mélyebben a publikus megoldások használatának lehetőségét, de jelenleg az a döntés született, hogy nem képezik részét a magyarországi szervezet 2019-es céljainak. Azonban a nemzetközi privát felhő számos előnyt képes jelenteni számunkra. Az üzemeltetési csapatunk a nemzetközi rendszer építésének második fázisába már aktívan bekapcsolódott és stratégiailag is fontos lépést tett, mivel a bővítés részeként Magyarország biztosítja a már működő rendszer erőforrás kiterjesztésének egyik színhelyét." (VA2)

A felhő megoldások egyértelmű hatást gyakorolnak nem csak az információbiztosági szervezetre, hanem megváltoztatják az üzemeltetési csapatok feladatkörét. Az on-site infrastruktúra biztosítása során szükség van a rendszerek fizikai üzemeltetését ellátó személyzet fenntartására, valamint saját adatközpontok és az azokhoz tartozó kiszolgáló szolgáltatások biztosítására (p.: áramellátás, UPS, hűtés stb). Erre egy publikus felhő esetében – legyen az akár IaaS, PaaS, SaaS stb – nincs szükség. Így pedig terjedésükkel negatívan fognak hatni az üzemeltetési létszámra. Az, hogy ez csupán az adatközpont, az infrastruktúra, vagy az alkalmazás üzemeltetőkre gyakorol hatást, szoros kapcsolatban van az igénybevett szolgáltatással. Az IaaS esetében az adatközponti, a PaaS során az infrastruktúra, míg a SaaS már az alkalmazás üzemeltetőket is képes érinteni.

> „Be kell látnunk, hogy a publikus felhő szolgáltatások használata negatívan fog hatni a belső IT feladataira. Sok közülük feleslegessé fog válni, mivel a külső szolgáltató fogja elvégezni." (VA1)
>
> „Nem gondolom, hogy a belső IT teljes mértékben megszűnne, mivel a felhő szolgáltatások igénybevételének számos feltétele van. Ezért abban hiszek, hogy a hibrid megoldásoké a jövő, amikor van helye egy belső szakértői csapatnak is. Azonban azt el kell fogadni, hogy az újonnan kialakult helyzethez a szakembereknek is alkalmazkodnia kell, ha versenyképességüket fenn akarják tartani." (VA2)

Olyan munkakörök fognak felértékelődni, amelyek már sok szervezetben jelen vannak, de eddig a belső folyamatokra fókuszáltak (pl.: szolgáltatás menedzserek). Így a vezetői szint biztosan nem fog eltűnni, azonban szerepe átalakul. Azon túl, hogy számonkérni és ellenőrizni fogja a külső szolgáltatókat, koordináló szerepet is el fog látni a belső ügyfelek és a külső szolgáltatók között.

> „Az igénybevett SaaS megoldásokat azonos módon kezeljük, mintha belső csapat biztosítaná, annyi különbséggel, hogy nem minden esetben tartoznak közvetlen az üzemeltetési vezetők alá, hanem ún. szolgáltatás menedzser felel értük. Annak meghatározása, hogy mely vezetőhöz kerül a felelősség, függ attól, hogy IaaS, PaaS vagy SaaS modellt veszünk igénybe. De a hibakezelés és KPI-ok követése azonos azzal, amit jelenleg is alkalmazunk." (VA5)

Az OCAI kérdőív segítségével összegyűjtött adatok alapján és az értékelést követően megállapítható, hogy a szervezetben adhokrácia a domináns kultúra, mely előny egy a telekommunikációs szektorban működő vállalat esetében. Sikeréhez elengedhetetlen ugyanis a dinamikus és kreatív munkakörnyezet. Tapasztalataim alapján az alkalmazottak bátran vállalnak kockázatot annak érdekében, hogy kiemelkedő eredményeket érjenek el, valamint az innováció és kísérletezés lehetősége fontos számukra. A felhő megoldások alkalmazásának egyik alappillére a vállalatnál tapasztalt ezen jellemzők megléte.

A kapott eredmények (N=92) alapján kimondható, hogy egy, a telekommunikációs szektorban működő meghatározó vállalatnál a felhő alapú megoldásokat aktívan használják. Vállalatonként és működési

környezettenként eltérő lehet azonban, hogy publikus, privát, hibrid vagy közösségi megoldást választanak a szervezetek. Az információbiztonság menedzseléséért felelős területeknek – annak érdekében, hogy meg tudjanak felelni a felhő által támasztott új kihívásoknak – változáson kell keresztülmenniük, melyhez hozzá tartozik funkciójuk újradefiniálása is.

Szervezeti információbiztonság (EK3)

Az interjúk eredményei alapján az IT szervezet tudatában van, valamint körültekintően tervezi a biztonsági intézkedéseket, de számos hiányosság tapasztalható vezetői és kulturális szempontból a vállalat egészét tekintve.

> „Egy telekommunikációs vállalat számára elengedhetetlen, hogy ne csak saját rendszereit, hanem ügyfelei otthoni hálózatát is legyen képes megvédeni." (VA5)
>
> „Nem engedhetjük meg azt, hogy mint internet szolgáltató veszélyeztessük előfizetőink saját gépeit és adatait, ezért a fejlesztés során minden elkövetünk azért, hogy a kihelyezett eszközeinket folyamatosan biztonsági aspektusból teszteljük, és a feltárt réseket azonnal befoltozzuk." (VA3)
>
> „De be kell ismernünk azt is, hogy a felsővezetés és az üzleti területek nem minden esetben partnerek a biztonsági kérdésekben. Nem érzik annak jelentőségét és a versenyképességet befolyásolni képes hatásait." (VA4)

A szervezet erős a fizikai biztonság területén és ehhez kapcsolódó intézkedéseket proaktívan végzi. Logikai biztonság témakörében számos védelmi megoldást vezettek be (tűzfalak, szeparált hálózati szegmensek, IPS, IDS eszközök). Az intézkedések egy része nem proaktív módon történik, hanem audit megfelelés céljából, vagy az audit során feltárt hiányosságok kezeléseként. A humán biztonsági oktatások vannak, de a szervezet egyes területeinek a biztonság tudatossága ennek ellenére elmarad az elvárt szinttől.

> „Számos beruházást eszközöltünk az elmúlt években annak érdekében, hogy megújítsuk határvédelmünket. Ezt indokolta, hogy egyes audit vizsgálatok megállapították, hogy a korábbi megoldásaink esetében számos olyan kockázattal rendelkeztünk, amelyek nem voltak felvállalhatók." (VA2)
>
> „Készítünk belső oktatási anyagokat, melyek célja, hogy felhasználóink biztonsági tudatosságát fejlesszék és segítsenek számukra kiszűrni a feléjük irányuló vagy rajtuk keresztül végrehajtani kívánt támadásokat. Ez egy nem könnyű folyamat, mivel a tudatosságot kiépíteni energiaigényes, azonban a megfelelő szint fenntartása még ennél is több energia befektetését követeli meg." (VA6)

A válaszadók a tervezett és rendszeresen lefolytatott, biztonsági vizsgálatokat elengedhetetlennek tartják annak érdekében, hogy a meglévő védelmi szintet fenn lehessen tartani, illetve javítása megtörténhessen.

Kiemelték, hogy több alkalmazás esetében tapasztalták, hogy már nem képesek működni a támogatás alatt levő operációs rendszereken, így rákényszerítve az üzemeltetési csapatokat a nem biztonságos, elavult környezetek fenntartására.

> „Alkalmazásaink egy része elavult és támogatással már nem rendelkező rendszereken képesek csak futni (pl: Windows Server 2003).” (VA2)
>
> „Ez olyan üzemeltetési kockázatokat rejt magában, amely akár egy kritikus alkalmazás megállásához is vezethet. Ezzel a felsővezetés tisztában van, azonban az új fejlesztések, új szolgáltatások bevezetése minden esetben elsőbbséget élveznek a „karbantartó” fejlesztésekkel szemben.” (VA3)

A felmérés során kiderült, hogy a szervezet végez saját vizsgálatokat, bevon külső cégeket, valamint az auditok során is történnek biztonsági tesztelések. Megkülönböztetett figyelmet fordítanak az újonnan bevezetendő alkalmazások biztonsági tesztelésére, ami nélkül nem kerülhetnek éles üzembe.

> „Elengedhetetlen, hogy rendszereinket folyamatosan teszteljük, külsős, független szervezetek bevonásával annak érdekében, hogy a belső kollégák által fel nem tárt hiányosságokat, biztonsági réseket fel tudjuk ismerni és kidolgozzuk rájuk a megfelelő válasz lépéseket.” (VA6)

Kiemelték, hogy tapasztalatuk alapján a szervezet akkor veszi komolyan a biztonsági fenyegetettségeket, ha korábban már átesett valamilyen krízis helyzeten (biztonsági incidensen, pl. SONY). Addig a biztonsági intézkedések és kezdeményezések alacsony prioritással rendelkeznek. Ezt a viselkedésmintát már az irodalmi áttekintés során is megerősíteni láttuk. Természetesen ez a megállapítás nem általánosítható minden szervezetre, mivel vannak kiemelkedő biztonság tudatossággal rendelkezők, de a hozzáállást nagyban befolyásolja a vezetés.

> „Az információbiztonsággal kapcsolatos fejlesztésekre és intézkedésekre mindig korlátozott keretösszeggel rendelkezünk. A költések szintjét a korábbi évekkel azonos szinten kell tartanunk annak ellenére, hogy a kihívások és fenyegetettségek nem minden évben azonosak ezen a területen.” (VA1, VA2)
>
> „Olyan esetben, mikor egy támadás, vagy tényleges incidens történt, mindenkit aktívan érdekelni kezd a Senior Vezetői szinten, hogy javítsunk a kialakult helyzeten, akár extra erőforrások (emberi, anyagi) bevonásával.” (VA5)

Az információbiztonság menedzsment az üzemeltetési csapatoktól független, önálló szervezet kell, hogy legyen az interjúalanyok elmondása szerint, amely egybevág az irodalmi kutatásunk során tapasztaltakkal.

> „A kontrollt és ellenőrzést gyakorló szervezet minden esetben teljes függetlenséggel kell, hogy rendelkezzen az üzemeltetést és fejlesztést végző csapatoktól. Ellenkező esetben nem valósulna meg az őszinte és megbízható kontroll.” (VA5)

Az elmúlt két évben számos szervezeti átalakuláson ment át a vizsgált vállalat, melynek egyik fókusza volt a biztonsági kihívásokra történő hangsúly helyezése. Egyértelművé vált, hogy lokálisan nincs elég erőforrás a napjainkban felmerülő biztonsági kihívások felismerésére és a szervezet időben való felkészítésére. Ezért az új fenyegetettségek azonosítását, annak követését központosították egy nemzetközi csapat formájában, és az ezzel foglalkozó személyek számát növelték.

> „Nem tudtuk megvalósítani az összes rendszerünkkel kapcsolatosan felmerült új biztonsági hibák követését, monitorozását, a szervezeten belüli kommunikációját, és ami a legfontosabb, az ellenőrzését. Ennek egyrészt oka volt a kis létszámú biztonsági és governance csapat, másrészt a lokális vezetés ezirányú érdeklődésének hiánya." (VA5)
>
> „Az információbiztonsági kérdések kezelése korábban mindig másodlagos volt. A felsővezetésen nehéz volt átvinni azokat az intézkedéseket, amelyek a belső felhasználókat korlátozták a biztonság fenntartásának érdekében." (VA4)

A vizsgált szervezetnél az átalakítással elérték, hogy a kontroll elvételével a korábban ellenállást tanúsító felsővezetői réteg már csak végrehajtó szintre került. Nem volt joguk módosítani a biztonsági elvárásokat és intézkedéseket, amelyet korábban lokális szinten meg tudtak tenni. Ellentétben a korábbi gyakorlattal, amikor az igazgatósági egyeztetéseken ebben a kérdésben az IT vezető mindig egyedül maradt. Ez merőben új megközelítést jelentett, így lehetőség nyílt arra, hogy egységes biztonsági elvárásokat lehessen támasztani egy több országban működő nemzetközi szervezeten belül.

> „A biztonsági kérdéseknek központosítása merőben új helyzetet teremtett a vezetés számára. A korábban „mi megmondjuk mit nem lehet megcsinálni" attitűdből a „hogyan tudjuk ezt megoldani" felfogásba fordultunk át." (VA6)

A szervezeti kultúra lassan tud csak változni, de az elmúlt két évben a válaszadók elmondása alapján észlelhetővé vált az információbiztonsággal kapcsolatosan, hogy a korábbi adhokrácia típusú működésből elindult a hiearchikus irányba a központosított vezetést követően. Azt feltételezem, hogy az információbiztonsági intézkedések a változás egyik okozói voltak. Természetesen a szervezet teljes egészét tekintve nem történt szignifikáns változás a kultúra szemszögéből, azonban biztonsági kérdésekben szabályozottabbá és kiszámíthatóbbá vált a vállalat.

> „Alkalmazkodnia kellett a szervezetnek az újonnan kialakult működési formához. Ez nem csak az emberekre, hanem a szervezetünk viselkedésére is hatott. Voltak azonban olyanok, akik nem tudtak azonosulni ezzel az új megközelítéssel, mivel számukra elfogadhatatlan volt, hogy a döntéseket a jövőben központilag és nem az országban hozzák meg." (VA2)

A feltárt eredmények igazolják azt a feltételezésemet, hogy egy, a telekommunikációs szektorban működő vállalat esetében kiemelt hangsúlyt fektetnek az információbiztonságra és aktívan tesznek azért,

hogy szavatolják és fejlesszék, azonban lehetőségeik nagyban függenek a felsővezetés biztonság iránti elhivatottságától.

Következtetések

Az esettanulmány eredményeképpen megállapítható, hogy az információbiztonság csak akkor kap kellő hangsúlyt, ha korábban valamilyen kritikus biztonsági esemény következett be. Ez alól a vizsgált telekommunikációs vállalat sem kivétel, azonban azt tapasztaltuk, hogy működése során már megjelent az információbiztonság javítása iránti igény és elvárás. Azonban ennek tényleges megvalósulására hatással van a felsővezetés biztonság iránti elkötelezettsége (EK3). Az információbiztonság menedzseléséért felelős szervezet független a fejlesztést és üzemeltetést biztosító csapatoktól, az interjúalanyok elmondása szerint ez alapvető feltétele, hogy a valós kontroll megvalósulhasson (EK3). A biztonsági szervezet hatékonyságának feltérképezése során érdekes meglátás volt, hogy amíg lokális szervezeti egységként működött, nem volt meg a kellő ereje ahhoz, hogy a szükséges lépéseket kikényszerítse és betartassa. Ezt felismerve a funkciót központosították, így pedig megváltoztak a korábbi vezetői szerepek, mivel már nem a helyi irányítás határozta meg a biztonsággal kapcsolatos irányokat, hanem azokat mint elvárás kapták (EK3). Munkám rávilágított, hogy a szervezet adhokrácia típusú kultúrája elengedhetetlen ahhoz, hogy a kiélezett piaci versenyben képes legyen helytállni. Az eredményorientáltság, valamint a komparatív előnyök megszerzésének vágya arra ösztönzik a vállalatot, hogy a legújabb, innovatív, hatékonyságot javítani képes, vagy költség csökkentésére alkalmas megoldásokat, mint „early adapter" igyekezzen bevezetni (pl.: felhő alapú szolgáltatások) (EK4). De az elmúlt években érezhetővé vált a kultúra változása is annak ellenére, hogy ez egy hosszú folyamat (EK3). Az információbiztonság menedzseléséért felelős terület feladatai nagyban átalakultak, aktívan részt kell venniük a felhő megoldások értékelésében, kiválasztásában és a szolgáltatások biztonságának folyamatos ellenőrzésében, valamint a felhőbe kihelyezendő adatok körének meghatározásában (EK2). A felhő rendszerekkel szemben támasztott biztonsági elvárások meghatározása megtörtént (EK1) a vizsgált szervezetnél, továbbá definiáltak olyan sztenderdeket, ami ahhoz szükséges, hogy saját privát felhő megoldásuk egységes és biztonságos legyen. A felhő megoldások hatást gyakorolnak a belső üzemeltetési feladatkörökre (EK4). Néhányuk eltűnik, mások át fognak alakulni, mely folyamatban az alkalmazkodás és az új feladatok ellátásának képessége fogja meghatározni, hogy mely szakemberek és vezetők lesznek alkalmasak az új környezetben is működni (EK4). Természetesen lesznek olyan feladatkörök, amelyek ezért akár teljesen eltűnhetnek egy-egy vállalat esetében, míg másikaknál (felhő szolgáltatók) koncentrálódni fognak (EK4).

A lefolytatott félig strukturált interjúk és kiértékelésük során szerzett tapasztalatok alapján úgy döntöttem, hogy a kutatási kérdéseimet szűkítem. Erre azért volt szükség, mivel a szervezeti kultúra és vezetői szerepek kölcsönhatása nagyobb mértékben befolyásolta a felhő megoldások alkalmazását, mintsem azon biztonsági elvárások köre, amelyet a szervezet támaszt ilyen szolgáltatásokkal szemben.

Természetesen igazolásra került, hogy ez egy nagyon fontos terület, de csak másodlagos szerepet játszik. Ezért ezt a kérdést már elhagytam az esettanulmányt követő kutatásom során:

- EK1: Milyen biztonsági elvárásokat támasztanak a vállalatok a felhő alapú alkalmazásokkal szemben?

Hasonlóan tettem az információbiztonság menedzsmenttel kapcsolatos kérdéskörrel is, mivel úgy gondolom, hogy ezt nem kezelhetem elszeparáltan, így modellemben is részévé tettem az információbiztonság és a felhő megoldások dimenziónak. Ezáltal pedig nem szükséges vizsgálni a következő kérdésben önállóan:

- EK2: Hogyan hat a felhő alapú működés az információbiztonság menedzsmentjére?

Az esettanulmányom során azonban a szervezeti kultúrával és vezetői szerepekkel kapcsolatos kérdések számos eredményt hoztak, melyek szélesebb körű vizsgálata és igazolása volt szükséges. Arra a következtetésre jutottam, hogy a korábban két kérdésbe sűrített területeket azok szerteágazósága miatt tovább bontom, így létrehozva a disszertáció 1.3Kutatási kérdések fejezetében található kutatási kérdéseket.

5.2 Kvantitatív vizsgálat - A változók esetében

5.2.1 Kvantitatív kutatás bemutatása

A kutatás során kérdőíves vizsgálatot választottam az összefüggések feltárása érdekében és a Magyarországon működő telekkommunikációs vállalatokat kerestem meg. A kérdéseket tartalmazó kérdőív az 1. mellékletben található. Az így begyűjtött adatokat kvantitatív kiértékelési módszerek és SPSS statisztikai szoftver segítségével elemeztem.

5.2.2 A szervezeti kultúrára vonatkozó eredmények

Kiértékelésem első szakaszában a szervezeti kultúra vizsgálatát végeztem el annak érdekében, hogy későbbiekben feltárjam kapcsolatát az információbiztonsági kiválósággal és a felhő alapú megoldások alkalmazásával.

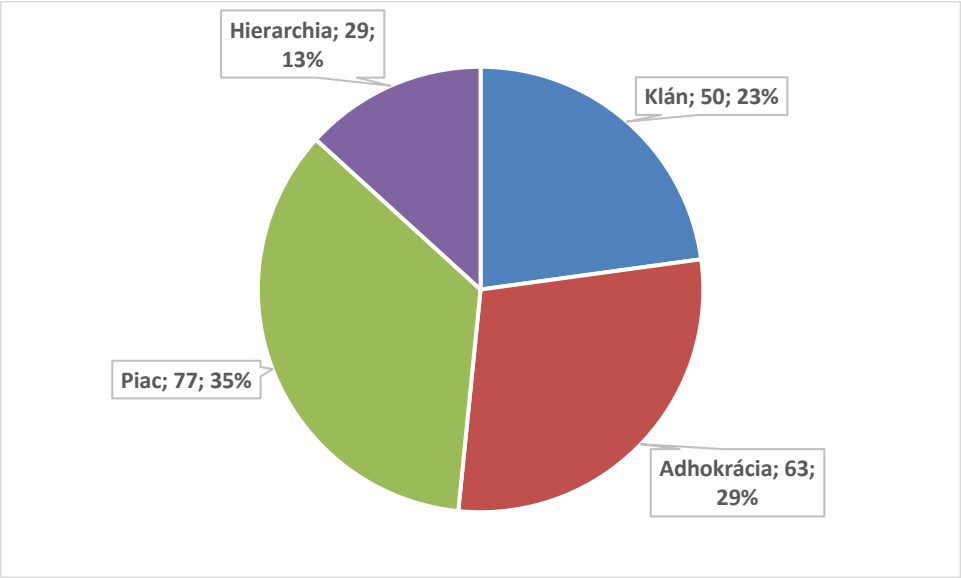
A vizsgált mintában mind a négy domináns szervezeti kultúra típust megtaláltam és az összefoglaló statisztikai adatokat a 6. táblázat tartalmazza. Az egyes kultúra típusok terjedelme közel azonos képet mutat. A legnagyobb távolságot a kapott válaszok között az Adhokrácia kultúra típus mutatja.

6. táblázat: Szervezeti kultúra felmérés statisztikai eredményei

Domináns szervezeti kultúra	Terjedelem	Minimum	Maximum	Átlag	Szórás	Gyakoriság a teljes mintában
Klán	34,17	10,00	44,17	23,34	6,55	50
Adhokrácia	38,33	11,67	50,00	27,25	8,53	63
Piac	36,67	9,17	45,83	26,49	8,95	77
Hiearchia	22,50	13,33	35,83	22,93	4,03	29

A kiértékelés eredményeként a Piac szervezeti kultúra jelenik meg legtöbbször (34%), míg 29%-ban Adhokrácia és 23%-ban Klán szervezeti forma volt a meghatározó. Legkisebb gyakorisággal a Hierarchia szervezet volt tapasztalható, de még így is jelentős, 13%-os ért el (4. ábra).

4. ábra: A domináns szervezet kultúra megoszlása



A kutatási kérdéseim domináns szervezeti kultúrát érintő részei esetében lefolytatott elemzés során a megkapott eredményeket, mint alacsony értékelési szintű nominális változó viszem be a varianciaanalízis során.

5.2.3 A vezetői szerepekre vonatkozó eredmények

A kiértékelés során az egy-egy szerephez tartozó kérdéseket faktorelemzéssel kell összevonni, így a négy kérdésből egy főkomponens alakítható ki. Az összevonások során több indikátor kihagyására volt szükség, mivel a KMO érték és kommunalitási indikátor nem volt megfelelő, így egyes változók nem tartoztak ahhoz a főkomponenshez, melyhez a módszer sorolta volna őket. A kapott eredmények minden esetben az eredeti információtartalom min. 50%-át tartalmazzák (7. táblázat).

7. táblázat: Vezetői szerepek főkomponens statisztikai eredményei

Dominán vezetői szerep	KMO-érték	Bartlett-teszt szignifikanciája	Megőrzött variancia
Bróker	0,500	0,010	60,989
Innovátor	0,779	0,000	62,176
Mentor	0,760	0,000	58,815
Facilitátor	0,779	0,000	60,875
Koordinátor	0,725	0,000	50,003
Direktor	0,825	0,000	71,108
Producer	0,726	0,000	53,770
Monitor	0,771	0,000	57,472

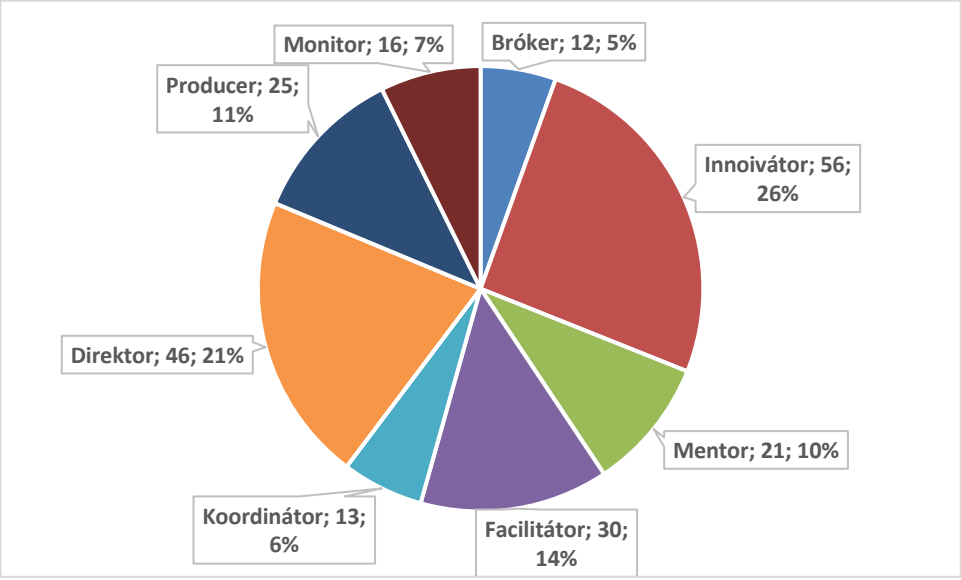
A létrehozott főkomponensek kialakításánál a Cameron-Quinn Versengő értékek keretrendszere által meghatározott főkomponenseket alkalmaztam, de annak érdekében, hogy a főkomponensek közötti kapcsolatot ki tudjam zárni elvégeztem Pearson féle korrelációs elemzésüket, melynek eredményeként elmondható, hogy egyetlen kapcsolat se szoros, továbbá ahol szignifikáns lenne ott is 0,25 alatt van az értéke (8. táblázat).

8. táblázat: Vezetői szerepek főkomponensek közötti korreláció

Főkomponens	Bróker	Innovátor	Mentor	Facilitátor	Koordinátor	Direktor	Producer	Monitor
Bróker	1	0,068	0,066	0,035	0,099	-0,033	0,044	-0,032
Innovátor	0,068	1	-0,124	-0,228	-0,028	0,001	-0,209	0,047
Mentor	0,066	-0,124	1	-0,146	-0,062	-0,18	-0,113	-0,019
Facilitátor	0,035	-0,228	-0,146	1	-0,126	-0,235	-0,17	-0,045
Koordinátor	0,099	-0,028	-0,062	-0,126	1	-0,014	-0,142	0,074
Direktor	-0,033	0,001	-0,18	-0,235	-0,014	1	-0,077	-0,103
Producer	0,044	-0,209	-0,113	-0,17	-0,142	-0,077	1	-0,01
Monitor	-0,032	0,047	-0,019	-0,045	0,074	-0,103	-0,01	1

A főkomponensek meghatározását követően szükséges volt meghatározni a domináns vezetői szerepet. Dominánsnak azt a szerepet tekintettem, ahol a faktorhoz tartozó érték a legnagyobb (12. melléklet). A domináns vezetői szerepek eredményeiből látható (12. melléklet), hogy minden vezetői szerep megjelenik a mintában. Ezek közül a Bróker (5%), Koordinátor (6%), Monitor (7%) típusú vezetők képviselik a legalacsonyabb reprezentáltságot, míg az Innovátor (26%) és a Direktor (21%) dominánsként jelennek meg. A Mentor, Producer és Facilitátor vezetői szerepek pedig 10-14% gyakorisággal jelennek meg (5. ábra).

5. ábra. Domináns vezető szerepek megoszlása



A domináns vezetői szerepekkel kapcsolatosan lefolytatott elemzés során a megkapott eredményeket, mint alacsony értékelési szintű nominális változó használom a varianciaanalízis során.

5.2.4 Az információbiztonsági kiválóság érettségre vonatkozó eredmények

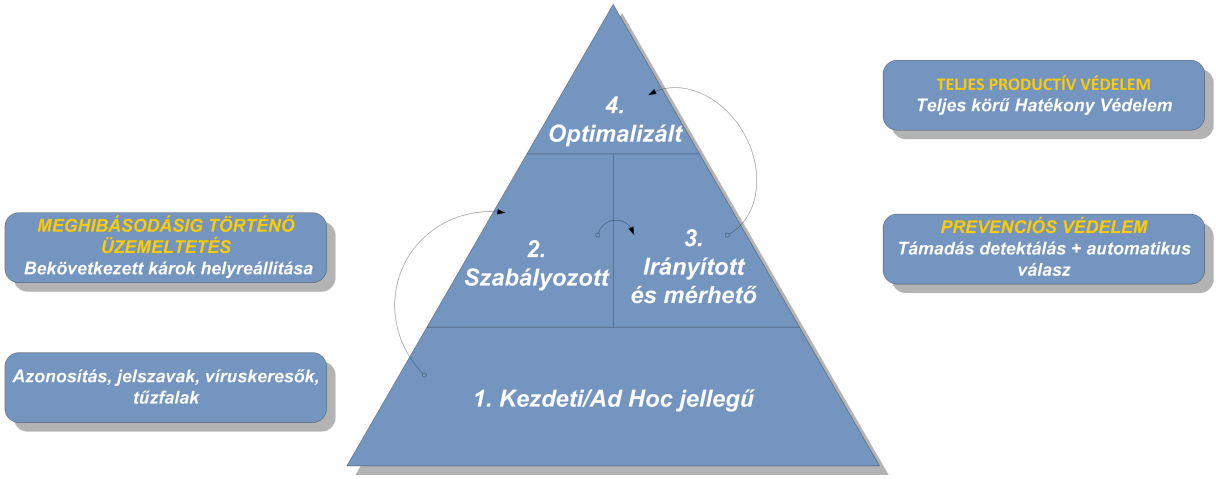
Az információbiztonsági kiválóság és annak érettsége több tényezőből tevődhet össze figyelembe véve a vizsgálat modelleket (3. táblázat). Fontos volt munkám során, hogy elkerüljem a csupán információbiztonságra fókuszáló megközelítést és szélesebb, már a menedzsment és kontroll aspektusát is beépítsem a kérdőíves lekérdezés során. Természtesen figyelembe kellett vennem, hogy mély, minden területre kiterjedő vizsgálat nem volt lehetséges, mivel annak bonyolultsága és részletgazdagsága megakadályozta volna, hogy feltárjam az összképet és kutatásom során nem releváns információt tartalmazó adatgyűjtésbe végződött volna.

Áttekintve a korábbi érettségi modelleket és azok által vizsgált területeket, olyan indikátorokat választottam, amikkel jellemezni tudom a vállalatok információbiztonsági helyzetét, működését és összetételét.

Az adatokat kérdőíves lekérdezés segítségével gyűjtöttem össze, mely kitér a fizikai, logikai és humán biztonságra. Figyelembe veszi a fenyegetettségek forrását, annak kezelését, továbbá magának az információbiztonságnak a kontrollját is. Az adatgyűjtés 11 állítást tartalmaz, melyek értékelése egy 7 fokú Likert-skála segítségével történik meg. Az állításokat tartalmazó kérdőív az 1. mellékletben található.

A szervezetek információbiztonsági kiválóságát a korábbi modellek alapján meghatározott érettségi szintekbe soroltam (6. ábra).

6. ábra: Információbiztonsági kiválósági piramis



Az információbiztonsági kiválóság főkomponenseinek meghatározása

Az összegyűjtött adatok elemzésének és értelmezésének feltétele volt, hogy a változók számát redukálni tudjam, erre faktorelemzést, azon belül főkomponens analízist (Principal Component Analysis) alkalmaztam. Így a válaszok mögötti látens struktúra feltérképezésére is lehetőségem nyílt. A faktorelemzés alapja, hogy az eredeti változókat és a kvantitatív adatokat sűrített formában szolgáltatja, számottevően csökkentett számú úgynevezett faktor segítségével (Barna & Székelyi, 2008). Az átalakítás után létrehozott új változókat főkomponenseknek nevezzük, melyek nem mutatnak korrelációt egymással és a kiinduló adatok lehető legnagyobb százalékát (varianciát) megőrzik (Barna & Székelyi, 2008).

Az elemzés első lépése annak vizsgálata, hogy a kapott adatok teljesítik-e a faktorelemezés feltételeit. Ennek eszköze a változók közötti korreláció (Pearson-féle linerási korreláció) vizsgálata, mely megléte nélkül nem lehetséges a változókat faktorba összevonni. A vizsgálat lefuttatása után megállapítható, hogy a változók közötti kapcsolat közepesen erős (3. melléklet), ezáltal megfelel a faktorelemzés követelményeinek.

Második lépésként az anti-image mátrixot (4. melléklet) vizsgáltam meg, mely abból indul ki, hogy a változók szórás négyzete felbontható nem magyarázott (anti-image) és magyarázott (image) részre, melyet a kovariancia és korrelációs mátrixok mutatnak. Az anti-image korrelációs mátrixban elsődlegesen az átlóban található értékek vizsgálata szükséges, mivel ezek tartalmazzák az egyes változókra vonatkozó MSA-értéket. Az MSA-értéke 0 és 1 között változhat és azt adja meg, hogy az adott változó mennyire szoros kapcsolatban áll más változókkal (Csallner, 2015). Ha egy változó MSA

értéke 0,5 alatti, abban az esetben a változót nagy valószínűséggel ki kell venni az elemzésből, míg ha 1 az értéke, akkor a többi változó ezt a változót hiba nélkül becsli. A kapott eredmények alapján a főátló értékei 0,717 és 0,915 közöttiek, a többi kapott eredmény pedig a megfelelő tartományban alacsony, így ez a feltétel is teljesül.

Harmadik kritérium a Barlett-teszt nullhipotézis teljesülésének szükségessége, mely alapján a kiinduló változók között nincs korreláció. Az információbiztonsági kiválósággal kapcsolatos kérdéseket egy főkomponensbe rendezve (9. táblázat) a Barlett-teszt nullhipotézisét el lehet vetni, mivel a szignifikancia szint kisebb, mint 0,05. Így kijelenthető, hogy a kiinduló változók az elemzésre alkalmasak, ugyanis van közöttük korreláció.

Negyedik feltétel a Kaiser-Meyer-Olkin (KMO) érték vizsgálata, mely az egyik legfontosabb mérőszám annak meghatározására, hogy a változók mennyire alkalmasak az elemzésre. Ha az érték 0,5 alatt van, akkor nem fogadható el, míg 0,8 felett nagyon jó. A 9. táblázat értéke alapján a KMO érték = 0,793, így megfelelőnek minősíthető.

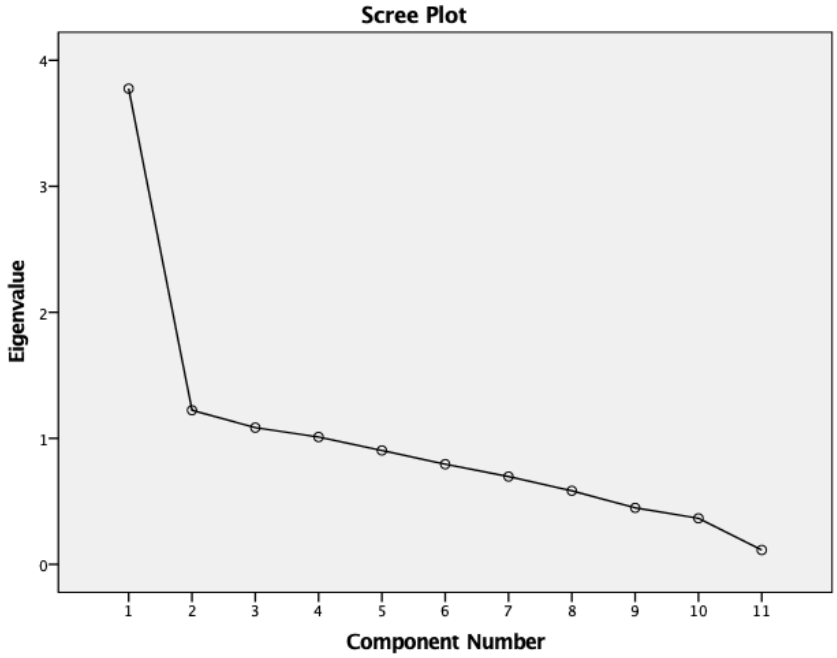
9. táblázat: Információbiztonsági kiválóság főkomponens Barlett-teszt és KMO eredménye

Kaiser-Meyer-Olkin érték		**0,793**
Barlett teszt	Szabadsági fok	55
	Szignifikancia	0,000

A fenti kritériumok teljesülése biztosítja, hogy a változók alkalmasak a faktoranalízisre. Így pedig tovább léptem a faktorok meghatározására, mely folyamat során több felétételnek is teljesülnie kell. Elsődleges kritériumként egyetlen faktor létrehozását végeztem el. A faktorok számának meghatározásakor figyelembe kell venni a Kaiser-kritériumot, mely alapján azon faktorokat kell számításba venni, melyek saját értéke minimum 1. Kaiser kritérium alapján 4 faktor meghatározása a javasolt.

Lehetőség van a Scree-teszt futtatására is, amely szintén a faktordimenziók megállapításában nyújt segítséget.

7. ábra: Információbiztonsági kiválóság Scree-teszt eredménye



A Scree-plot (7. ábra) segít meghatározni hány látens dimenzió használata szükséges. A faktorok számát ott érdemes meghúzni, ahol a görbe meredeksége megváltozik (Barna & Székelyi, 2008). A 7. ábra alapján 2, viszonylag nagy információ tartalmú faktorra számíthatunk.

A faktor elemzést folytatva 2 faktorra is elvégeztem alapozva a Scree-plot által mutatott értékekre. Ennek eredményeként azonban kevesebb információ őrizhető meg 2, mint 4 faktor esetében. A megőrzött variancia 45,435% 2 faktor esetében, míg 64,483% 4 faktor mellett.

A faktorkiválasztás során kiemelten fontos a rotáció (faktorok elforgatása), melynek célja azon változók korrelációjának a felszámolása, amelyeknek egymáshoz nincs köze, így problémát okozva az elemzés során. Az elforgatástól azonban nem változik meg a modell illeszkedése, az egyes változók végső információtartalma, melyet a faktorok együttesen őriznek meg. Változást az jelenti, hogy az egyes faktorok milyen mennyiségét őrzik meg az információnak (Barna & Székelyi, 2008). Az elemzés során a Varimax rotációt használtam Principal component módszer mellett. Természetesen megvizsgáltam a Maximum likelihood lehetőségét is, azonban előző jobb eredményekkel szolgált. A 6 iteráció után kialakult 4 faktor az eredeti információtartalom 64,483,%-át őrizte meg (10. táblázat).

10. táblázat: Információbiztonsági érettség főkomponensek megőrzött varianciája

Főkomponens	Eredeti saját érték		Varimax rotáció utáni érték	
	Megőrzött variancia %	Kommulatív %	Megőrzött variancia %	Kommulatív %
1	34.320	34.320	22.910	22.910
2	11.115	45.435	20.669	43.579
3	9.864	55.299	11.026	54.605
4	9.184	64.483	9.878	64.483

A modell javításának módszere, ha megvizsgáljuk a kommunalitási értéket, mely segít meghatározni, hogy van-e olyan változó, amelyet ki kell zárni, azaz értéke 0,25 alatt van. Az ilyen változóknak nincs elég magyarázó ereje (Barna & Székelyi, 2008). Ilyen változót nem találtam.

Ezen túl szükséges, hogy egy változó csak egyetlen faktorhoz tartozzon. Ezért elvárás volt, hogy a faktorsúly jelentősen nagyobb, legalább kétszerese, vagy különbsége minimum 0,25 legyen, mint a többi faktor esetében. Ez szintén teljesült vizsgálatom során.

Továbbá azokat a változókat is el kell hagynom, amelyeket nem lehet magyarázni, vagy egyáltalán nem illenek bele a létrejött modellbe, de erre nem volt példa a faktorelemzés során.

A válaszok, valamint a faktorelemzés eredménye alapján 4 egymástól független faktor jött létre, melyek magas mérési szintűek, így további elemzést tesznek lehetővé.

Az információbiztonsági kiválóságra jellemző dimenziók

A dimenziócsökkentés eredményeként megállapítható, hogy az információbiztonsági érettséget 4 fő tényező határozza meg:

- Információbiztonsági területek
- Információbiztonság menedzsment
- Külső információbiztonságot befolyásoló tényezők
- Belső információbiztonságot befolyásoló tényezők

11. táblázat: Információbiztonsági kiválóság komponens mátrix

Változók	Inf.bizt területek	Inf.bizt menedzsment	Külső Inf.bizt befolyásoló tényezők	Belső Inf.bizt befolyásoló tényezők
Fizikai biztonság fejlettsége jelenlegi	0,726			
Logikai biztonság fejlettsége jelenlegi	0,92			
Humán biztonság fejlettsége jelenlegi	0,898			
Külső fenyegetettségek felismerése jelenlegi			0,763	
Belső fenyegetettsége felismerése jelenlegi				0,802
Tudatos kockázatelemzés jelenlegi		0,732		
Belső felelőségek tisztázottak jelenlegi				-0,634
Külső szolgáltatás/üzemeltetés esetén a felelőségek tisztázottak jelenlegi			-0,647	
Biztonsággal kapcsolatos területeket kontrolálják jelenlegi		0,624		
Felismert fenyegetettségeket kezelik jelenlegi		0,766		
Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés jelenlegi		0,604		

Az **információbiztonsági területek magukba foglalják a biztonsággal kapcsolatos összes intézkedést**. Első dimenziója a fizikai biztonság, mely az illetéktelen fizikai hozzáférést hivatott kiküszöbölni. Második dimenzió a logikai biztonság, ami az informatikai biztonsági intézkedéseket öleli fel, megakadályozva a virtuális térben történő nem engedélyezett hozzáféréseket. Harmadik elem a humán biztonság, mely az emberi tudatlanságból, hiszékenységből eredő kockázatokat kiküszöbölni képes módszereket tömöríti.

Az információbiztonsági menedzsment főkomponensbe olyan tevékenységek tartoznak, amelyek célja, hogy **az információbiztonsággal kapcsolatos alapvető feladatokat összefogják**, irányítsák, ezzel hozzájárulva a biztonsági szint kialakulásához és egyben szavatolásához is. Ennek első pillére a tudatos kockázatelemzés, mivel anélkül egy vállalat nem ismerné, hogy az egyes fenyegetések milyen valódi kockázatot jelentenek működésére. Szervesen rá épülő tevékenység a már felismert fenyegetettségek kezelése, ugyanis nem elég csupán feltárni a veszélyt, elengedhetetlen annak kiküszöbölése, vagy olyan mértékű kezelése, mely a már elfogadható szintre képes csökkenteni annak negatív hatásait. Ha mindezek ellenére mégis bekövetkezne egy biztonsági esemény, akkor mint harmadik pillérként a számonkérés jelenik meg, mely már reaktív tevékenység, de kiemelten fontos annak érdekében, hogy a jövőben a hasonló eseteket el lehessen kerülni. A biztonsági területek kontrolja, mint egy keretrendszer jelenik meg, ami az előző három pillér megfelelő működéséért felel.

Harmadik és negyedik főkomponensek a külső és belső információbiztonságot befolyásoló tényezőket, fenyegetettségeket tömörítik magukba, melyek kockázatot jelentenek a szervezet működésére.

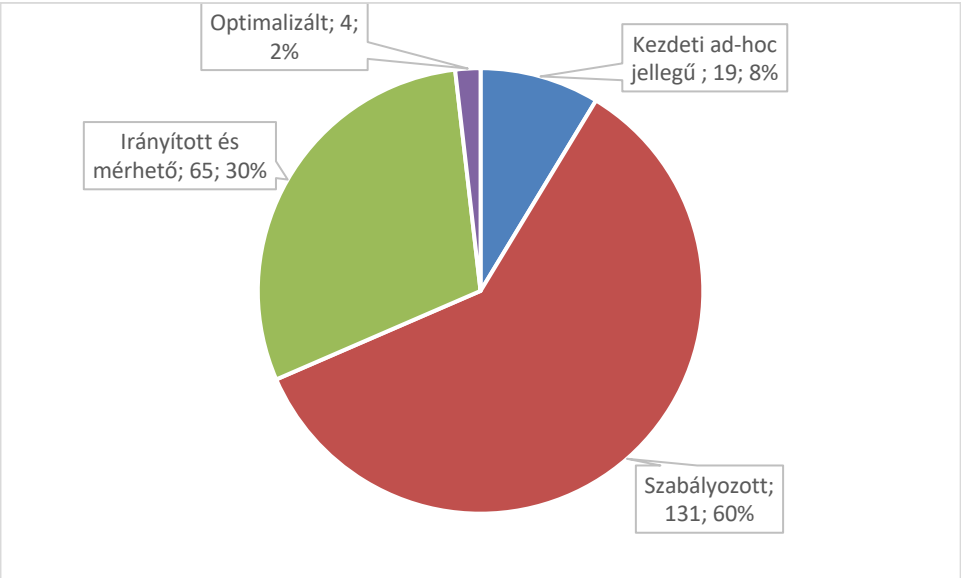
Az információbiztonsági kiválósági érettség meghatározása

A megkapott főkomponensek segítségével lehetőség nyílik az érettségi szint meghatározására, mely során a 6. ábra alapján meghatározott szintekbe soroltam be a szervezeteket. Az érettség meghatározásának menete:

1. Kiszámoltam az egyes főkomponensek első, második, harmadik kvartilisét (=KVARTILIS(vizsgált tartomány;kvart) (13. melléklet)
2. Ezt követően a megkapott értékek alapján meghatároztam, hogy az egyes főkomponensek esetében a vizsgált szervezet milyen érettségi szintbe tartozik (6. melléklet)
3. A megkapott érettségi szintek segítségével kiszámoltam egy adott válaszadóhoz tartozó főkomponens érettségi értékek geometriai átlagát, mely így megadta a szervezet információbiztonsági kiválósághoz kapcsolódó összesített érettségét (6. melléklet)

A fenti módszerrel meghatározott érettségi szintek vizsgált mintán belüli összetételét a 8. ábra tartalmazza.

8. ábra: Információbiztonsági kiválóság érettségi szintek szerinti megoszlása



Az információbiztonsági kiválósági érettséggel kapcsolatos eredmények összefoglalása

A jelenlegi fejezetben a beérkezett adatok alapján bemutattam az elemzés menetét, a változók mérhetővé tételét és főkomponsekbe történő sorolásuknak folyamatát. Az így megkapott eredmények alapján a változókat 4 főkomponensbe lehetett csoportosítani, melyek között megjelent az informcáióbiztonsági területek, információbiztonsági menedzsment, külső és belső információbiztonságot befolyásoló tényezők is.

Ismertettem annak módszerét, hogy miként képződnek a főkomponensek értékéből az egyes érettségi szintek, melynek végeredményeként összefoglaltam az egyes érettségi szintek megoszlását a teljes vizsgálati mintán belül.

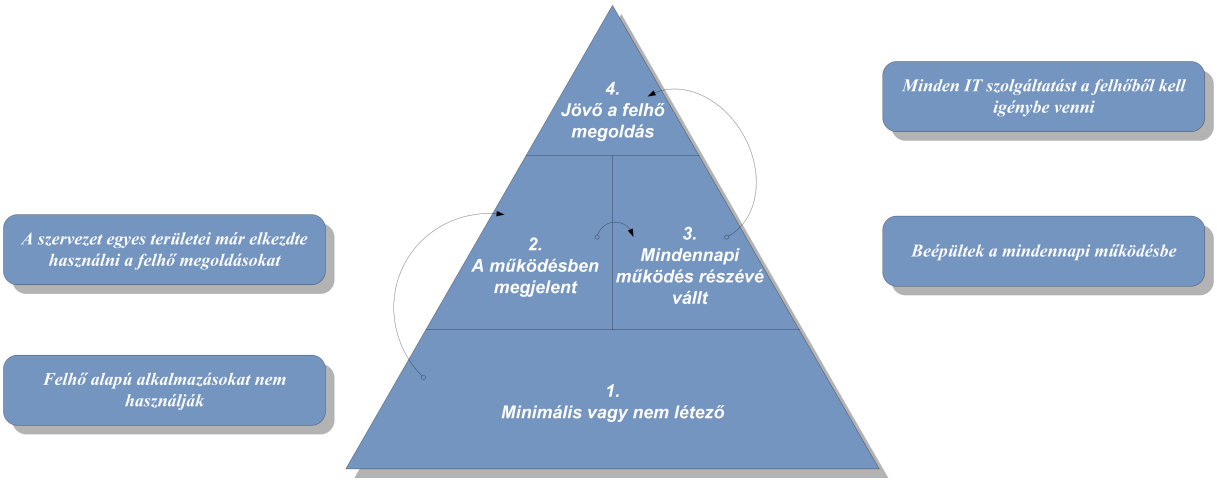
5.2.5 A felhő alapú megoldások alkalmazására vonatkozó eredmények

A felhő alapú megoldások alkalmazása és annak érettsége számos tényezőből tevődik össze. Áttekintve a korábbi érettségi modelleket és azok által vizsgált területeket, olyan indikátorokat választottam, amelyekkel jellemezni tudom a vállalatok által alkalmazott felhő alapú megoldásokat. Figyelembe vettem azokat a tapasztalatokat, amelyeket korábban a strukturált interjúk során szereztem.

Az adatokat a vizsgált mintán lefolytatott kérdőíves lekérdezés eredményekét gyűjtöttem be, mely kitért a privát, publikus megoldások értékelésére, az üzemeltetéshez kapcsolatos kulcskérdésekre, a szolgáltatási szintekre, továbbá vizsgálta az adatok szemszögéből is a felhő alapú megoldásokat. A kérdőívem ezen része 10 állítást tartalmaz, melyek értékelése egy 7 fokú Likert-skála segítségével történt meg. Az állításokat tartalmazó kérdőív az 1. mellékletben található.

A felhő alapú megoldások alkalmazásának érettségét a korábbi modellek alapján meghatározott érettségi szintekbe soroltam (9. ábra).

9. ábra: Felhő alapú megoldások alkalmazása érettségi piramis



A felhő alapú megoldások alkalmazására vonatkozó főkomponensek meghatározása

A felhő alapú megoldások vizsgálatakor szintén feladatom volt, hogy a változók számát redukáljam, erre faktorelemzést, azon belül főkomponens analízist (Principal Component Analysis) használtam. Szükséges volt megvizsgálni, hogy a felhő alapú megoldásokhoz tartozó változók alapján kapott adatok megfelelnek-e a faktorelemzés feltételeinek.

Első lépésként a Pearson-féle lineáris korreláció vizsgálatára volt szükség. Az eredmények alapján kijelenthető, hogy a változók közötti kapcsolatok közepesen erősek (7. melléklet), ami azt jelenti, hogy megfelel a faktorelemzés követelményének.

Következő feltétel vizsgálatát az anti-image mátrix segítségével tettem meg, ahol elsődlegesen az átlóban található értékek elemzése szükséges, mivel ezek tartalmazzák az egyes változókra vonatkozó MSA-értékeket. Ha az MSA értéke 0,5 alatti, abban az esetben a változót nagy valószínűséggel ki kell venni az elemzésből, ha 1 az értéke, akkor a többi változó ezt a változót hiba nélkül becsli (Csallner, 2015). A kapott eredmények alapján a főátló értékei 0, 724 és 0, 836 közöttiek, a többi kapott eredmény pedig a megfelelő tartományban alacsony, így ez a feltétel is teljesül (8. melléklet).

Harmadik kritérium a Barlett-teszt nullhipotézis teljesülésének feltétele. A felhő alapú megoldásokkal kapcsolatos kérdéseket egy főkomponensbe rendeztem (12. táblázat). A szingifikancia szint kisebb, mint 0,05. Így kijelenthető, hogy a kiindulási változók között van korreláció, így alkalmasak az elemzésre.

Negyedik és egyben utolsó kritériumként Kaiser-Meyer-Olkin (KMO) vizsgálatát kellett elvégeznem. Nem fogadható el értéke, ha 0,5 alatt van, azonban 0,8 felett nagyon jónak mondható. Vizsgálatom során KMO=0,762, mely szintén megfelel érték.

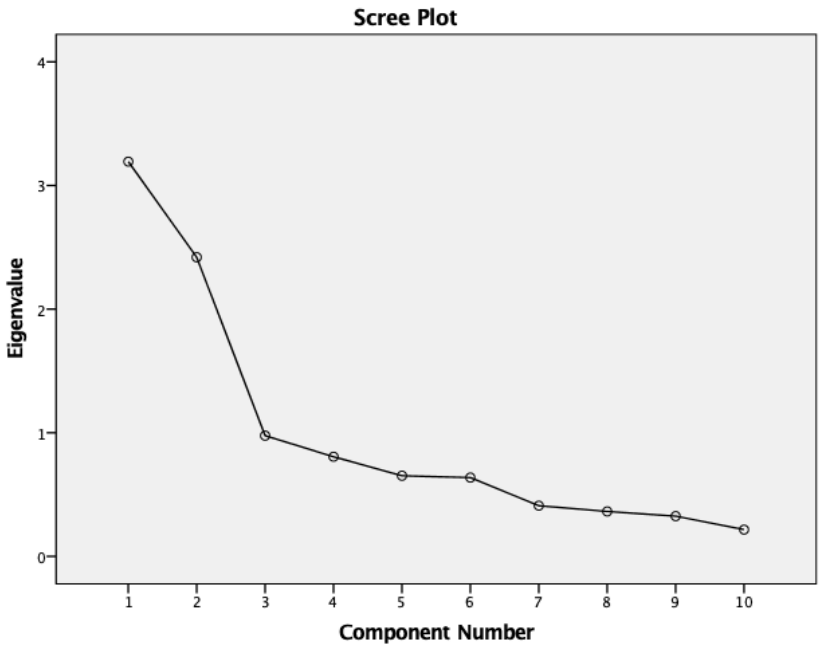
12. táblázat: Felhő alapú megoldások főkomponens Barlett-teszt és KMO eredménye

Kaiser-Meyer-Olkin érték		**0,762**
Barlett teszt	Szabadsági fok	45
	Szignifikancia	0,000

Következő lépésként a faktorok meghatározása következett és először egyetlen faktor létrehozását végeztem el. A Kaiser-kritérium alapján, azokat a faktorokat vehetem figyelembe, melyek saját értéke legalább 1. A kapott eredmények alapján 2 faktor esetében kaptam nagyobb értéket, mint az elvárt szint (2.419 és 3.19). Azonban folytatni kell az elemzést, mivel 1faktorra történő átalakítás esetén csupán az eredeti információ tartalom 31,9%-a lenne megőrizve.

A Scree-teszt a teljes varianciát veszi figyelembe és segítséget nyújt a faktorok számának meghatározásában, ezért ennek eredményét is megvizsgáltam.

10. ábra: Felhő megoldások alkalmazása Scree-teszt eredménye



A Scree-plot (10. ábra) esetében a faktorok számát ott érdemes meghúzni, ahol a görbe meredeksége megváltozik (Barna & Székelyi, 2008). Az ábra alapján 2, viszonylag nagy információ tartalmú faktorra számíthatunk.

A Kaiser-kritérium és a Scree-plot eredményei alapján 2 faktor létrehozásával haladtam tovább és vizsgáltam a változók korrelációját az egyes faktorokkal. A faktorkiválasztás során kiemelten fontos a rotáció (faktorok elforgatása), melynek célja azon változók korrelációjának a felszámolása, amelyeknek egymáshoz nincs köze, így problémát okozva az elemzés későbbi szakaszában. A forgatás során Varimax rotációt használtam Principal component módszer mellett. A 3 iteráció után kialakult 2 faktor az eredeti információtartalom 60,70%-át őrizte meg (13. táblázat).

13. táblázat: Felhő alapú megoldások alkalmazás főkomponensek megőrzött varianciája

Főkomponens	Eredeti saját érték		Varimax rotáció utáni érték	
	Megőrzött variancia %	Kommulatív %	Megőrzött variancia %	Kommulatív %
1	35,374	35,374	30,488	30,488
2	25,296	60,670	30,183	60,670

A modell javításának módszere, ha megvizsgáljuk a kommunalitási értékeket, mely segít meghatározni, hogy van-e olyan változó, amelyet ki kell zárni, azaz értéke 0,25 alatt van. Az ilyen változóknak nincs elég magyarázó ereje (Barna & Székelyi, 2008). Ilyen volt a "Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak" változó, mivel értéke 0,235 mutatott.

Ezen túl szükséges, hogy egy változó csak egyetlen faktorhoz tartozzon. Ezért elvárás, hogy a faktorsúly jelentősen nagyobb, legalább kétszerese, vagy különbsége minimum 0,25 legyen, mint a többi faktor esetében. Ez teljesült vizsgálatom során.

Továbbá azokat a változókat is el kell hagynom, amelyeket nem lehet magyarázni, vagy egyáltalán nem illettek bele a létrejött modellbe, de erre nem volt példa a faktorelemzés során.

A válaszok, valamint a faktorelemzés alapján 2 egymástól független faktor jött létre, melyek magas mérési szintűek, így további elemzést tesznek lehetővé.

A felhő alapú megoldásokra jellemző dimenziók

A dimenziócsökkentés eredményeként megállapítható, hogy a felhő alapú megoldásokkal kapcsolatos változók 2 fő tényező köré csoportosíthatóak:

- Publikus felhő szolgáltatások
- Privát felhő szolgáltatások

14. táblázat: Felhő alapú megoldások alkalmazásának komponens mátrix

Változók	Publikus felhő szolgáltatások	Privát felhő szolgáltatások
Privát felhő szolgáltatásokat használ		0,889
Publikus felhő szolgáltatásokat használ	0,824	
Külső üzemeltetés felel a felhő alapú megoldásokért	0,796	
Belső üzemeltetés felel a felhő alapú megoldásokért		0,838
Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)		0,787
Platform szolgáltatást vesz igénybe/biztosít (PaaS)	0,697	
Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	0,649	
Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak		0,608
Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem)	0,569	

A publikus felhő szolgáltatások főkomponens magába foglalja a külső szolgáltatókat jellemző területeket. Így az első dimenzió maga a publikus felhő használata, mely meghatározza, hogy az adott szervezet milyen mértékben épít a külső erőforrásokra. Második dimenzió az üzemeltetés felelősége és feladata, mely ebben az esetben a külső szolgáltatóra hárul. Harmadik és negyedik dimenzió maga a szolgáltatás típusa. A publikus szolgáltatások esetében döntő részben a platform és szoftver szolgáltatások igénybevétele a jellemző. Ötödik és egyben kritikus témaköre a publikus felhő szolgáltatásoknak annak meghatározása és értékelése, hogy mely adatok azok, amelyek kihelyezhetőek külső szolgáltatóhoz.

A privát felhő szolgáltatások főkomponens tartalmazza a belső szolgáltatások területeit, így magát a privát felhő használatának mértékét, mely meg fogja mutatni, hogy a szervezeten belül mennyire elterjedt a felhő alapú megoldások alkalmazása. A privát felhő üzemeltetése esetében két megközelítés, valamint ezek ötvözése van jelen. Azaz külső, vagy belső, vagy ezek kombinációjával biztosítják a napi feladatok ellátását. A privát felhő szolgáltatások főkomponenshez belső üzemeltetési feladatok dimenziója került elemzésem alapján. A privát megoldás esetében döntő többség az infrastruktúra szolgáltatások jelennek meg és kiemelt figyelmet kapnak ezen szolgáltatásokkal szemben támasztott biztonsági elvárások is.

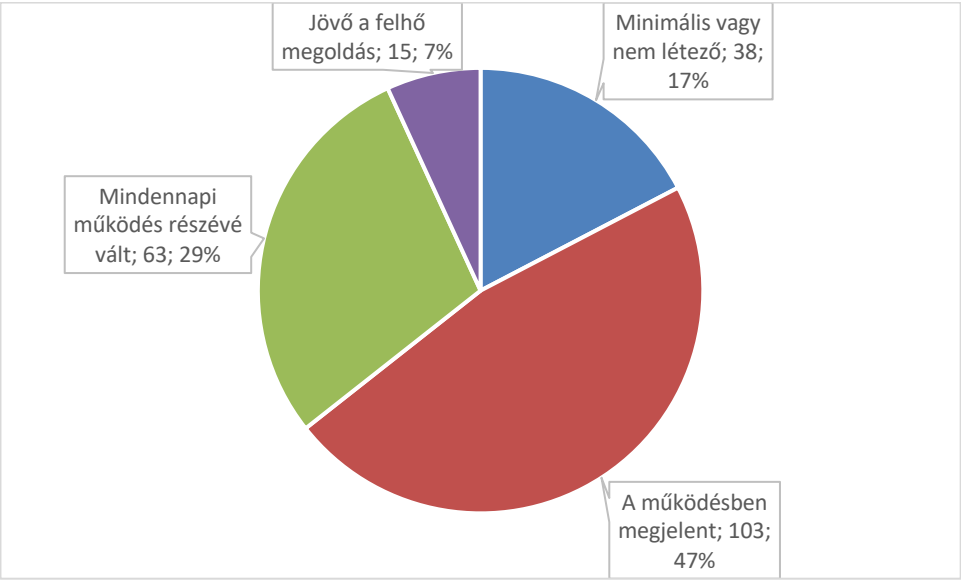
A felhő alapú megoldások alkalmazásának érettség meghatározása

Az érettség meghatározásához szükséges a megkapott főkomponens értékek felhasználása a következő folyamat mentén:

1. Kiszámoltam az egyes főkomponensek első, második, harmadik kvartilisét (=KVARTILIS(vizsgált tartomány;kvart) (14. melléklet)
2. Az így kapott értékek alapján meghatároztam, hogy az egyes főkomponensek esetében a vizsgált szervezet milyen érettségi szintbe tartozik (9. melléklet)
3. A meghatározott érettségi szintek segítségével kiszámoltam egy adott válaszadóhoz tartozó főkomponens érettségi értékek geometriai átlagát, mely így megadta a szervezet felhő alapú megoldások alkalmazásához kapcsolódó összesített érettségét (9. melléklet)

Az így meghatározott érettségi szintek összetételét a vizsgált mintára vetítve a 11. ábra tartalmazza.

11. ábra: Felhő alapú megoldások alkalmazásának érettségi szintek szerinti megoszlása



A felhő alapú megoldások alkalmazásával kapcsolatos eredmények összefoglalása

A beérkezett adatok alapján elvégeztem a faktoranalízis alkalmazhatósági feltételeinek vizsgálatát, majd folytattam a változók főkomponensekbe történtő sorolásával. Az elemzés végeredményeként 2 főkomponens jött létre, melyeket a publikus és privát felhő szolgáltatások alkották.

Ismertettem annak módszerét, hogy miként képződik a főkomponensek értékéből az egyes érettségi szintek, melynek végeredményeként összefoglaltam az egyes érettségi szintek megoszlását a teljes mintán belül.

5.3 Kvantitatív vizsgálat - A változók közti kapcsolatok esetében

A munkám ezen fejezetében célom, hogy vizsgáljam a szervezeti kultúra és vezetői szerepek hatását az információbiztonsági kiválóságra és a felhő alapú megoldások alkalmazásának érettségére. Arra voltam kíváncsi, hogy milyen különbségek mutatkoznak szervezeti kultúránként és vezetői szerepenként.

A modell magyarázott oldalán az információbiztonsági kiválóság és a felhő alapú területek állnak, melyeket az érettséggel jellemzem. A megkapott válaszok mérhetővé tételét az 5.2.4 és az 5.2.5 fejezetekben fejtettem ki. A magyarázó változók a modell tekintetében a szervezeti kultúra és a vezetői szerepek állnak, melyeket a domináns karakterisztikával jellemeztem és elemzésüket az 5.2.2 és az 5.2.3 fejezet tartalmazza. A vizsgálat során azt kerestem, hogy melyek azok a domináns tulajdonságok, amelyek esetében az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazása esetében magas érettségi szintet lehet tapasztalni.

A függő változók magas, míg a magyarázó változók minden esetben alacsony mérési szintű nominális változók, így a kapcsolat vizsgálatára varianciaanalízist fogok használni. A variancia elemzésnél tisztában kell lennünk a kapcsolat irányával, azaz tudunk kell, melyik változó befolyásolja a másikat, illetve a változók mérési skálája eltérő kell, hogy legyen. A varianciaanalízist arra használjuk a gyakorlatban, hogy feltárjuk egyes tényezők milyen hatással vannak más tényezőkre (Sajtos & Mitev, 2007).

5.3.1 Szervezeti kultúra hatása az információbiztonság kiválóságra

Az elemzés során magyarázó változóként a domináns szervezeti kultúrát használom, ami alacsony mérési szintű nominális változó. Magyarázott változónak pedig az információbiztonsági kiválóság érettségi szintet tekintem, mely magas mérési szintű, így a mérési szintre vonatkozó feltételek teljesülnek.

A varianciahomogenitás, vagy más néven szóráshomogenitás azt jelenti, hogy a függő változónak megegyező szórással kell rendelkeznie a függő változó különböző szintjei mellett. Ennek ellenőrzése a

Levente-teszt segítségével történik. Ahogy a 15. táblázatban látható, a teszt eredménye szignifikáns lett (Sig=0,000) így annak nullhipotézisét el kell fogadnom. A varianciahomogenitás feltétele nem teljesül, azaz Post-Hoc analízis során Tamhane kontrasztot kell alkalmaznom.

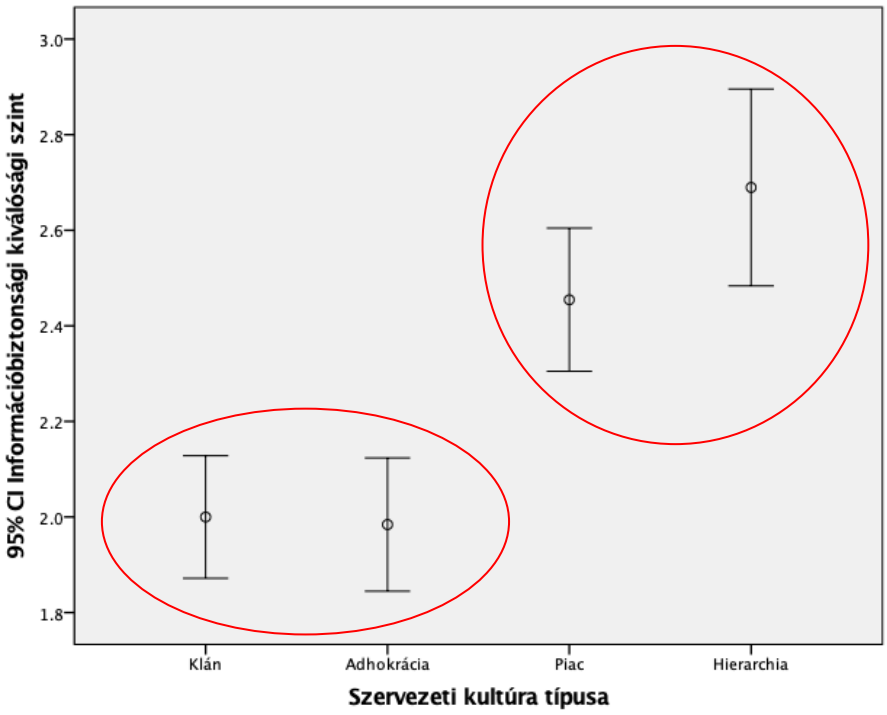
15. táblázat: Levene teszt eredménye (szervezeti kultúra és információbiztonsági kiválóság)

Levene statisztika	*Szabadsági fok*	*Szignifikancia*
13,275	3	0,000

Az ANOVA teszt lefuttatásakor (15. melléklet) látható az F hányad, amely a csoportok közötti és a csoporton belüli eltérésnégyzetének az aránya (5,468/0,327=16,726). Az F próbához tartozó valószínűség szignifikanciája (Sig=0,000), ami arra utal, hogy a független változó szignifikáns részt magyaráz a függő változó heterogenitásából, azaz a szervezeti kultúra szignifikánsan befolyásolja az információbiztonsági kiválóságot (15. melléklet). Mivel a modell 4 szervezeti formát foglal magába, ezért az F próba csak a kapcsolatok meglétét tudja bizonyítani. A Post-Hoc elemzés használata szükséges, mely segít meghatározni, hogy az egyes szervezeti kultúrák milyen hatással vannak az információbiztonsági kiválóságra. A 15. melléklet az egyes kultúrák közötti különbségekre vonatkozó Tamhane statisztika azon eredményeit mutatja, ahol szignifikáns a kapcsolat (Sig<0,05).

A 12. ábra alapján elmondható, hogy a Piac és Hierarchia szervezeti kultúra érettebb képet mutat információbiztonsági kiválóság tekintetében, mint a Klán és Adhokrácia szervezetek. A Versengő Értékek modelljében mind a két, információbiztonság területén jól szerepelő kultúra típusról elmondható, hogy a kontrolláltság és flexibitás tengelyén a kontrolláltság oldalán foglalnak helyet. A Post-Hoc elemzést megvizsgálva elmondható, hogy az érettebb biztonsági szint elérésének kedvez a szabályozottság, elszámolhatóság, valamint a kontrol megléte, amely területeken a Hierarchia kultúra erős. A Piac szervezeti kultúrára szintén jellemző ez a működés, azonban a kontroll inkább a piaci/gazdasági szükségszerűség által meghatározott. Az ilyen szervezetek törekednek a piaci előnyök megszerzésére, ezáltal pedig kiemelten fontos számukra az adataik védelme is.

12. ábra: Domináns szervezeti kultúra és az információbiztonsági kiválóság kapcsolata



Az Adhokrácia típusú szervezetek esetében elmondható, hogy a fókusz az állandó változó kihívásoknak való megfelelés kerül előtérbe, amely miatt a szervezet mindennapi működésének részévé vált az újítások bevezetése. Egy ilyen környezet azonban beláthatóan nem fog kedvezni az információbiztonsági területeknek, mivel az erőforrások a folyamatos kihívásokra történő válaszadásra összpontosítódnak. A Klán kultúrára jellemző a csapatmunka, a kölcsönös elkötelezettség. A szervezetet összetartó erő a hagyományok, melyek akár gátat is jelenthetnek az információbiztonság fejlődésének, mint ahogy az a 12. ábrán is látható.

5.3.2 Vezetői szerepek hatása az információbiztonsági kiválóságra

Folytatva vizsgálatomat a magyarázó változóként a domináns vezetői szerepeket választottam, ami alacsony mérési szintű nominális változó. Magyarázott változónak pedig az információbiztonsági kiválóság érettségi szinteket tekintem, mint azt tettem a szervezeti kultúrával kapcsolatos vizsgálatkor is.

A varianciahomogenitás ellenőrzését Levente-teszt segítségével hajtottam végre. Ahogy a 16. táblázat látható, a teszt eredménye szignifikáns (Sig=0,000) így a varianciahomogenitás feltétele nem teljesül.

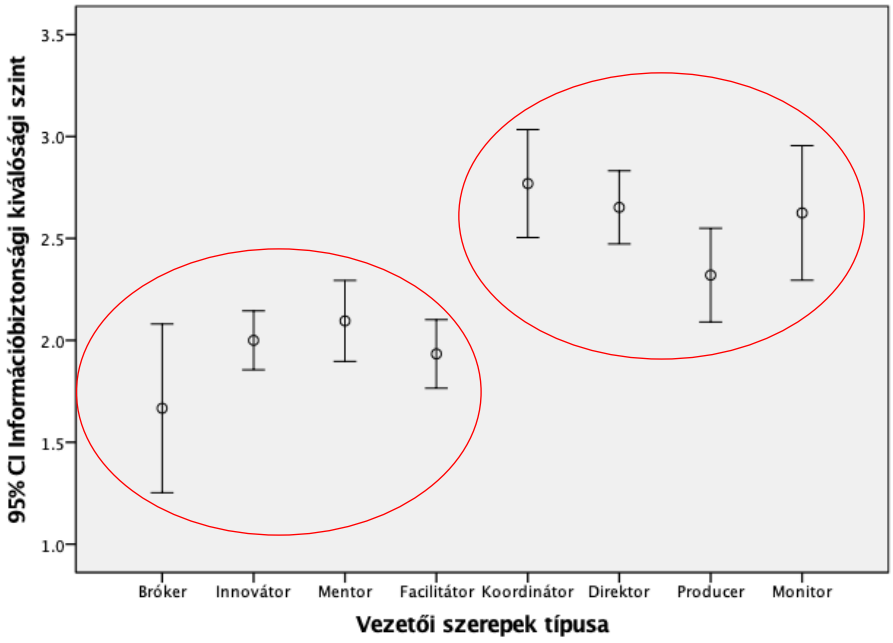
16. táblázat: Levene teszt eredménye (vezetői szerepek és információbiztonsági kiválóság)

Levene statisztika	*Szabadsági fok*	*Szignifikancia*
4,313	7	0,000

Az ANOVA teszt lefuttatásakor (16. melléklet) megkaptam az F hányadot, amely a csoportok közötti és a csoporton belüli eltérésnégyzetének az aránya (3,487/0,295=11,815). Mivel az F próbához tartozó valószínűség szignifikanciája kisebb, mint 0,05, ezért a nullhipotézist elutasítom. Ezáltal a kategóriaátlagok szignifikánsan különböznek, vagyis az egyes vezetői szerepek, más és máshogy hatnak az információbiztonsági kiválóságra. A szervezeti kultúrához hasonlóan itt is elvégeztem a Post-Hoc elemzést (16. melléklet), hogy feltérképezzem, hogy az egyes vezetői szerepeknek milyen hatása van az információbiztonságra. A Levene teszt szignifikáns eredménye miatt a Tamhane kontrasztot használom, ami nem követeli meg a függő változó varianciahomogenitását, azaz a vezetői szerepek szignifikánsan befolyásolják az információbiztonsági kiválóságot.

A 13. ábra alapján elmondható, hogy a Koordinátor, Direktor, Producer és Monitor vezetői szerepeknél fejlettebb információbiztonságot tapasztaltam, mint a Bróker, Innovátor, Mentor és Facilitátor vezetői szerepek esetében. A biztonsági szempontból jó értékeket mutató Koordinátor jellemzője a stabilitás, funkcionális területek összehangolása, valamint a munka tervezése. Direktor szerep az irányításra, célok kitűzésére és szervezésre, a Producer a hatékonyságra, termelékeny környezet biztosítására, a Monitor vezető pedig a dokumentálásra, teljesítmények figyelésére összpontosít. Ezek mind olyan tényezők, amelyek az információbiztonság megteremtésében és annak szavatolásában képesek döntő szerepet játszani, ezt igazolják vissza a 13. ábrán láthatóak.

13. ábra: Domináns vezetői szerepek és az információbiztonsági kiválóság kapcsolata



A Bróker, Innovátor, Mentor és Facilitátor esetében látható, hogy információbiztonsági szempontból elmaradottabbak az ilyen vezetőkkel rendelkező szervezetek. Ez visszavezethető arra, hogy esetükben

az innováció, a rugalmasság, valamint a részvéten alapuló döntéshozatal kerül előtérbe. Ezek ugyanis olyan tényezők, amelyek túlsúlya képes hátráltatni olyan területek fejlődését, amelyek elengedhetetlenek pl. az információbiztonság folyamatos fejlesztéséhez.

5.3.3 Szervezeti kultúra hatása a felhő alapú megoldások alkalmazására

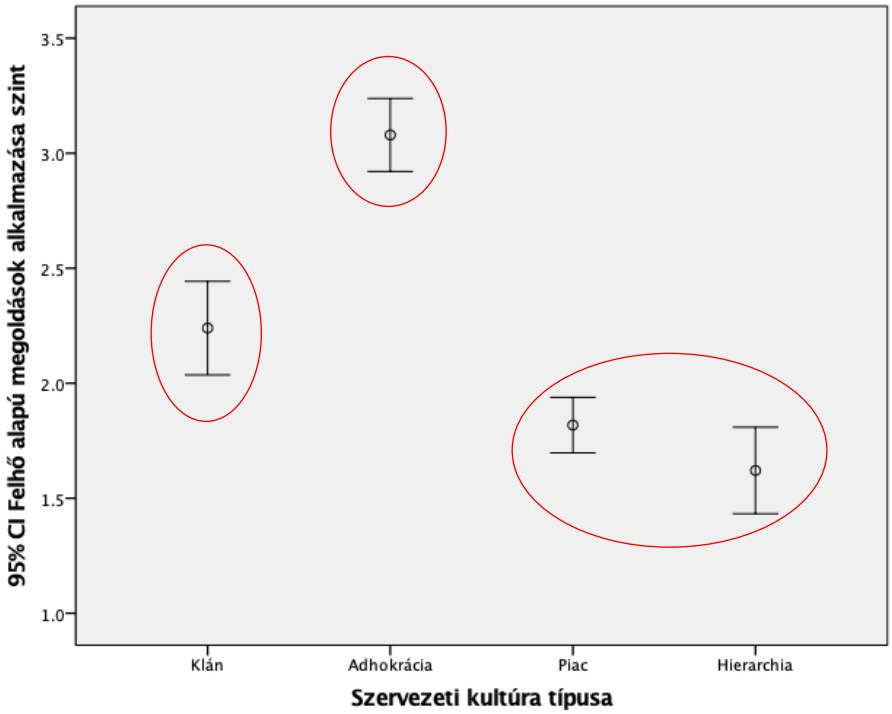
Következő lépésként áttértem a felhő alapú megoldások vizsgálatára, ahol magyarázó változó esetében maradtam a domináns szervezeti kultúránál, ami alacsony mérési szintű nominális változó. Magyarázott változónak pedig a felhő alapú megoldások alkalmazásának érettségi szintjét tekintettem. A varianciahomogenitás ellenőrzését szintén Levene-teszt segítségével valósítottam meg. A 17. táblázat alapján a teszt eredménye szignifikáns lett (Sig=0,018). Mivel a varianciahomogenitás feltétele nem teljesül, a Post-Hoc analízis során Tamhane kontrasztot kell alkalmaznom.

17. táblázat: Levene teszt eredménye (vezetői szerepek és felhő alapú megoldások alkalmazása)

Levene statisztika	*Szabadsági fok*	*Szignifikancia*
3,410	3	0,018

Az ANOVA tesztet szintén le kellett futtatnom, mint az információbiztonság vizsgálata során, ennek eredményeként (17. melléklet) látható az F hányad, amely a csoportok közötti és a csoporton belüli eltérésnégyzetének az aránya (23,061/23,061=23,061). Mivel az F próbához tartozó valószínűség szignifikanciája 0,000, vagyis kisebb, mint 0,05, ezért a nullhipotézist elutasítom. Ezáltal a kategóriaátlagok szignifikánsan különböznek, vagyis az egyes szervezeti kultúrák, más és máshogy hatnak a felhő alapú megoldások alkalmazására. Post-Hoc elemzést végeztem, annak érdekében. hogy feltérképezzem a szervezeti kultúra hatását a felhő alapú megoldások alkalmazására (17. melléklet). A 14. ábra alapján megállapítható, hogy az Adhokrácia szervezeti kultúra kiemelten támogatja a felhő alapú megoldások előtérbe kerülését. Ezen szervezeti típusra jellemző ugyanis az innováció iránti elkötelezettség, mely elengedhetetlen ahhoz, hogy a versenyképessége fenntartható és javítható legyen egy szervezetnek. Az elmúlt időszakban a felhő, mint költséghatékonysági és rugalmassági megoldás jelent meg az információs technológiák között, ezért is képes lehet egy szervezet piaci potenciáljának javítására azáltal, hogy működésére hat költség vagy rugalmassági aspektusból. A Klán típusú szervezetek közepesen érett képet mutatnak felhő alapú megoldások alkalmazásának tekintetében. Ez visszavezethető a fejlődés iránti nyitottságra, azonban láthatóan a hagyományok, azaz a már jól bevált és megszokott megoldások előtérbe helyezése még akadályozza az ilyen innovatív szolgáltatások széles körű bevezetését.

14. ábra: Domináns szervezeti kultúra és a felhő alapú megoldások alkalmazáságnak kapcsolata



Az előző két szervezeti típushoz képest elmaradott képet mutat mind a Piac, mind pedig a Hierarchia típusú szervezeti kultúra is. Azt gondolom, hogy ennek oka a Piac típusú szervezet esetében, hogy az ügyfélre, azok igényeire fókuszálnak és cél az ennek való megfelelés. A szervezet ez alá helyez mindent. A felhő, mint egy eszköz tud ebben segíteni, de hasznosságát és a benne rejlő lehetőségeket még csak kevés ilyen szervezet fedezte fel a túlzott ügyfél fókusz miatt. A Hierarchikus szervezeteknél a szabályozottság, a stabilitás, a folyamatos minőség javítás kerül a előtérbe. A felhő megoldások alkalmazásához azonban inkább arra van szükség, hogy egy szervezet az újítások irányába legyen nyitott, ezzel pedig hajlandó legyen akár kockáztatni a stabilitás és a minőség csökkenése árán is.

5.3.4 A vezetői szerepek hatása a felhő alapú megoldások alkalmazására

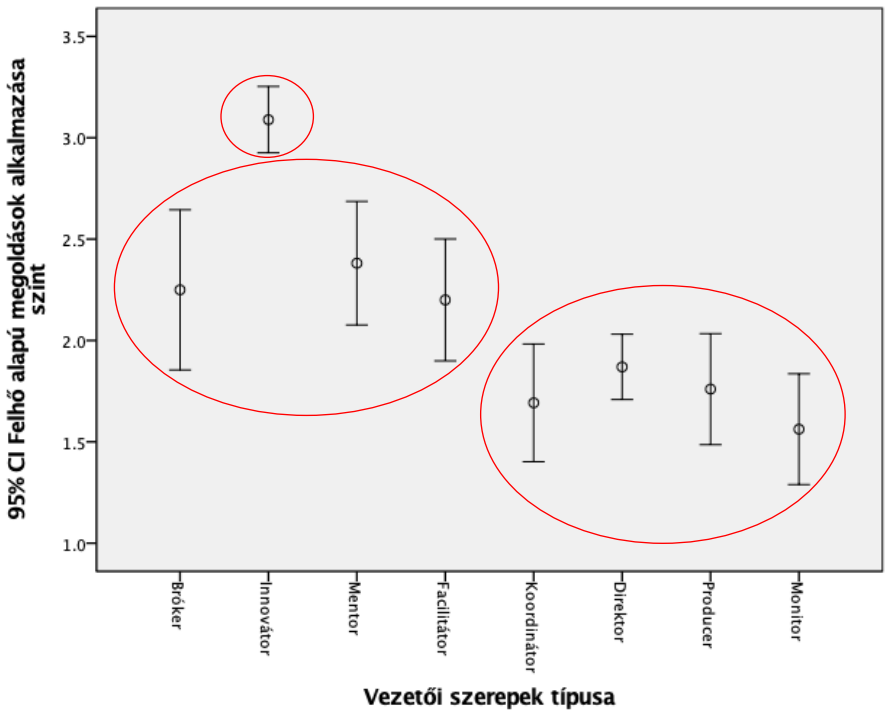
Utolsó lépésként a magyarázó változónak a domináns vezetői szerepeket választottam, míg magyarázott változónak pedig a felhő alapú megoldások alkalmazásának érettségi szintjét. A varianciahomogenitás ellenőrzését, mint korábban most is a Levente-teszt segítségével valósítottam meg, ahol a nullhipotézis azt jelenti, hogy a szórások nem egyenlők, amelynek az elvetése azt jelenti, hogy a szóráshomogenitás teljesül (Sajtos & Mitev, 2007). A 18. táblázat megmutatja, a teszt eredménye nem szignifikáns (Sig=0,089) így a szóráshomogenitás teljesül.

18. táblázat: Levene teszt eredménye (vezetői szerepek és felhő alapú megoldások alkalmazása)

Levene statisztika	*Szabadsági fok*	*Szignifikancia*
1,796	7	0,089

A vizsgálatot az ANOVA teszttel folytattam, ahol (18. melléklet) az F hányad (17,180 / 0,708= 24,262). A vezetői szerepek által a felhő alapú megoldások alkalmazására gyakorolt hatás feltérképezéséhez Post-hoz elemzést kellett végeznem. A Levene teszt nem lett szignifikáns, ezért részletesebb feltárása érdekében az LSD (Least Significant Difference = legkisebb szignifikáns különbség) alkalmazható, mely t-próbával ellenőrzi a kezelésátlagok (between groups) közötti különbséget. A legengedékenyebb feltételekkel rendelkezik a Post-Hoc tesztek közül, azaz ezzel lehetséges a leghamarabban kezelésátlagok közötti különbségeket kimutatni (Sajtos & Mitev, 2007). A 18. melléklet az egyes kultúrák közötti különbségekre vonatkozó LSD statisztika azon eredményeit mutatja, ahol szignifikáns a kapcsolat (Sig<0,05). A vizsgálat eredményét a 15. ábra foglalja össze, azaz az Innovátor vezetői szerephez tartozó eredmény kiemelkedő fejlettségi szintet mutat a felhő alapú megoldások alkalmazásának terén. Azt gondolom, hogy ennek egyik fő oka, hogy az ilyen vezetőkre jellemző a változások támogatása és előmozdítása. Működésüknek fontos alapköve a változással történő együttélés és alkalmazkodás.

15. ábra: Domináns vezetői szerepek és a felhő alapú megoldások alkalmazáságnak kapcsolata



A többi vezetői szerepet figyelembe véve elmondható, hogy további két nagy csoportra lehet osztani őket. Első csoportba a Bróker, Mentor és Facilitátor vezetői szerepek kerültek, melyek már mutatnak komolyabb érdeklődést a felhő alapú megoldások alkalmazása iránt, azonban még nincsenek olyan érettségi szinten, hogy nagyobb mértékben alkalmazzák azokat. Azonban azt gondolom, hogy közép vagy hosszú távon fejlődni fognak, ha nem éri őket valamilyen negatív "élmény" a felhő szolgáltatások

kapcsán. A második csoportba a Koordinátor, Direktor, Producer és Mentor vezetők kerültek. Esetükben a felhő megoldások még csak kezdetlegesen jelennek meg, ha egyáltalán használják őket.

5.3.5 Az információbiztonsági kiválóság hatása a felhő alapú megoldások alkalmazására

Kutatásom elemzési szakaszában lettem figyelmes arra, hogy az információbiztonsági kiválóság egyes szintjei összefüggést mutatnak a felhő alapú megoldások alkalmazásának érettségével, ezért kapcsolatuk részletesebb feltárása mellett döntöttem.

A varianciahomogenitás ellenőrzését, mint korábban most is a Levente-teszt segítségével valósítottam meg. A 19. táblázat megmutatja, hogy a teszt eredménye szignifikáns lett (Sig=0,000) így annak nullhipotézisét el kell fogadnom.

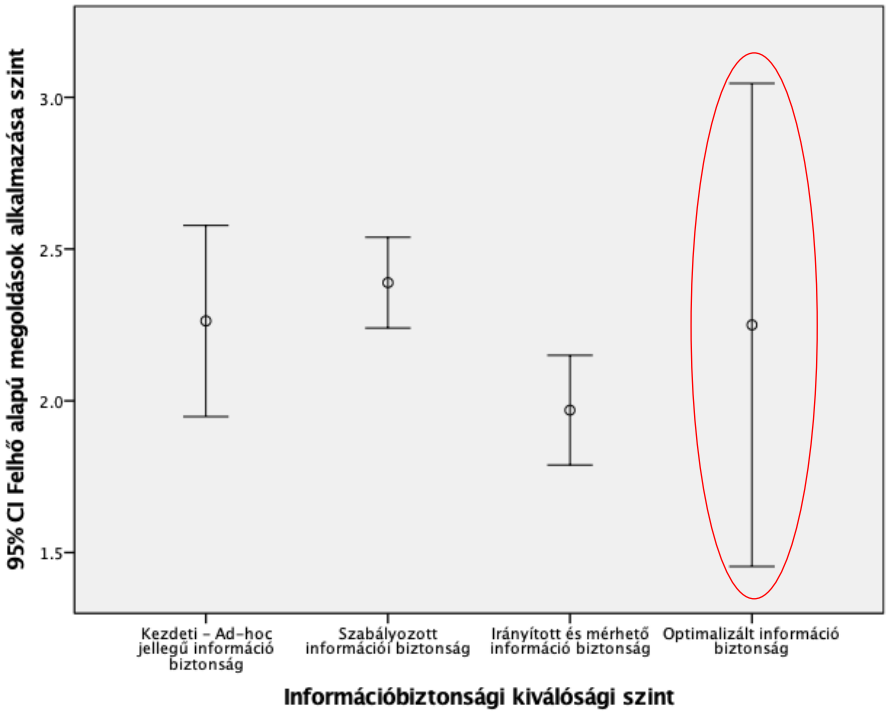
19. táblázat: Levene teszt eredménye (információbiztonsági kiválóság és a felhő alapú megoldások alkalmazása)

Levene statisztika	*Szabadsági fok*	*Szignifikancia*
6,308	3	0,000

A vizsgálatot az ANOVA teszttel folytattam, ahol (19. melléklet) az F hányad (2,557/0,649=3,994). A Levene teszt szignifikáns eredménye miatt a Tamhane kontrasztot használom, ami nem követeli meg a függő változó varianciahomogenitását, azaz a vezetői szerepek szignifikánsan befolyásolják a felhő alapú megoldások alkalmazását.

Az elemzés eredményét a 16. ábra foglalja össze, mely alapján elmondható, hogy a Kezdeti - Ad-hoc és a Szabályozott információbiztonsági kiválósági szint esetében a felhő alapú megoldások használata magas érettséget mutat, azonban haladva az Irányított és mérhető információbiztonsági kiválóság felé csökken alkalmazásuk.

16. ábra: Az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazáságnak kapcsolata



Azonban a legérettebb kiválósági szinten szignifikáns változás látható, hiszen újra megjelennek olyan vállalatok, akik előszeretettel használják a felhő alapú megoldásokat. Természtesen nem meglepő az sem, hogy ezen az érettségi szinten találhatók a felhő biztonságával szemben leginkább szkeptikus szervezetek, akik még nem nyitottak ilyen szolgáltatások irányába.

5.4 Hipotézisek helytállóságának elemzése és tézisek megfogalmazása

Kutatásom kezdeti fázisában négy hipotézist határoztam meg. Az első és második az egyes vezetői szerepek és szervezeti kultúra információbiztonságot befolyásoló képességének feltárását kívánta meghatározni.

A harmadik és negyedik hipotézisek szintén a Cameron-Quinn féle vezetői szerepek és szervezeti kultúra hatásait vizsgálják, azonban már a felhő alapú megoldások alkalmazásának előmozdítása, vagy mellőzése szempontjából.

1. hipotézis

Olyan Cameron-Quinn vezetői szerepek mellett lesz a biztonság fejlett, amelyek a szabályozottságra és stabilitásra törekszenek.

Az első hipotézisem új szemszögből közelítette meg a vezetői szerepeket és információbiztonságot. Korábban a két tudományterületet külön-külön vizsgálták a kutatók, azonban mélyreható összevetésük nem történt meg. A létrehozott, mind a két tudományágat tartalmazó kutatási modell lehetőséget biztosított arra, hogy a két terület együttes vizsgálat megtörténhessen. Ezzel nem csupán az egyik vagy másik szakterület részlet részleteiben merültem el, hanem azokat egy közös, új szemüvegen keresztül szemléltem, törekedve arra, hogy megértsem együttes működésüket.

A kapcsolódó irodalom áttekintését követően a Cameron-Quinn féle Versengő Értékek keretrendszerét választottam, melyben nyolc vezetői szerepet különböztetnek meg. A vizsgált mintán a Bróker (5%), Koordinátor (6%), Monitor (7%) típusú vezetők képviselik a legalacsonyabb reprezentáltságot, míg az Innovátor (26%) és a Direktor (21%) dominánsként jelennek meg. A Mentor, Producer és Facilitátor vezetői szerepek közepes, 10-14% közötti értéket mutatnak a mintán belül.

A korábbi tanulmányokat elemezve azonosítottam az információbiztonsági elemeket, melyek között legtöbb esetben megjelentek a biztonsági területek, fenyegetettségek és felelőségek. Ezek alapján meghatároztam az információbiztonsági kiválóság definiálásához szükséges tényezőket és egy közös modellbe foglaltam őket. A vizsgált mintán belül az egyes kiválósági szintek a következő megoszlásban voltak jelen: a Kezdeti/Ad-hoc (8%), a Szabályozott (60%), az Irányított és mérhető (30%) és az Optimalizált (2%).

A domináns vezetői szerepekhez tartozó információbiztonsági kiválósági szinteket megvizsgálva kijelenthető, hogy az egyes vezetői szerepek között szignifikáns különbség van. Az ANOVA vizsgálat F statisztikája valószínűség szignifikanciája 0,000, vagyis kisebb, mint 0,05, ami csak a kapcsolat létezését igazolta. Így Post-Hoc elemzésre volt szükségem ahhoz, hogy meghatározzam melyik vezetői szerep hogyan befolyásolja az információbiztonsági kiválóságot. A Levene teszt szignifikáns lett (Sig=0,000), ezért feltárása érdekében Tamhane statisztikát kellett alkalmaznom. A Koordinátor, Direktor, Producer és Monitor vezetői szerepekhez tartozó információbiztonsági kiválóság érettségi szintek szignifikánsan magasabbak, mint a Bróker, Innovátor, Mentor, Facilitátor esetében.

A vizsgálat eredményei alapján meghatározott 1. tézis:
Szignifikáns kapcsolat mutatható ki a Versengő Értékek Keretrendszere szerinti domináns vezetői szerepek és az információbiztonsági kiválósági szintek között. A Koordinátor, Direktor, Producer és Monitor vezetői szerepekhez tartozó kiválósági szintek szignifikánsan magasabbak, mint a Bróker, Innovátor, Mentor, Facilitátor esetében.

2. hipotézis

Olyan Cameron-Quinn szervezeti kultúrák esetében várható fejlett biztonsági szint, amelyek számára fontos a kontrolláltság, szabályozottság.

A szervezeti kultúra esetében is a Cameron-Quinn modelljét alkalmaztam, így segítve, hogy a szervezeti kultúrákat és vezetői szerepeket egységes rendszerben tudjam szemlélni. A kiválasztott minta lekérdezése során a módszerhez tartozó OCAI kérdőívet használtam és mind a négy domináns szervezeti kultúrát azonosítani tudtam. A vizsgált szervezetek körében a Piac kultúra jelenik meg legtöbbször (34%), míg 29%-ban Adhokrácia és 23%-ban Klán szervezeti forma volt a meghatározó. Legkisebb számosságban a Hierarchikus szervezet jelent meg, de még így is jelentős, 13%-os penetráció volt tapasztalható.

A domináns szervezeti kultúrához tartozó információbiztonsági kiválósági szinteket megvizsgálva kijelenthető, hogy az egyes szervezeti kultúrák között szignifikáns különbség van. Az ANOVA teszt az F próbához tartozó valószínűség szignifikanciája 0,000, vagyis kisebb, mint 0,05, ezért a nullhipotézist elutasítom. Ezáltal a kategóriaátlagok szignifikánsan különböznek, vagyis az egyes szervezeti kultúrák, más és máshogy hatnak az információbiztonsági kiválóságra. A Levene teszt szignifikáns (Sig=0,000) lett, ezért a Tamhane statisztikát kellett használnom. A teszt eredményei azt bizonyítják, hogy a Piac és a Hiearchia szervezeti kultúrához szignifikánsan magasabb információbiztonsági kiválósági értékek tartoznak, mint a Klán és Adhokrácia szervezetek esetében.

A vizsgálat eredményei alapján meghatározott 2. tézis:

A tézis kimondja, hogy szignifikáns kapcsolat mutatható ki a Versengő Értékek Keretrendszere alapján meghatározott domináns szervezeti kultúrák és az információbiztonsági kiválóság eredményei között. A domináns Piac és Hierarchia szervezeti kultúrákhoz tartozó információbiztonsági kiválóság értékek szignifikánsan magasabbak, mint a domináns Klán és Adhokrácia szervezetek esetében.

3. hipotézis

Azon Cameron-Quinn vezetői szerepek esetében nagyobb érdeklődést a felhő megoldások iránt, amelyek nyitottabbak az újdonságra és változásokra

Harmadik hipotézisem esetében szintén a Cameron-Quinn féle Versengő értékek Keretrendszerét alkalmaztam, mint vezetői szerepek meghatározásának eszközét. Áttekintve a korábbi érettségi modelleket és azok által vizsgált területeket, olyan indikátorokat választottam, amelyek képesek a vállalatok által alkalmazott felhő alapú megoldások érettségét jellemezni. Figyelembe vettem azokat a tapasztalatokat, amelyeket korábban a strukturált interjúk során szereztem. A vizsgált mintán belül az egyes felhő alapú megoldások alkalmazásának érettségi szintjei a következő megoszlásban jelentek

meg: Minimális, vagy nem létező (33%), a Működésben megjelent (44%), a Mindennapi működés részévé vált (0%) és a Jövő a felhő megoldás (23%).

A domináns vezetői szerepekhez tartozó felhő alapú megoldásik érettségi szinteket megvizsgálva kijelenthető, hogy az egyes vezetői szerepek között szignifikáns különbségek vannak. Az ANOVA vizsgálat F statisztikája valószínűség szignifikanciája 0,000, vagyis kisebb, mint 0,05, a Levente teszt pedig nem lett szignifikáns (Sig=0,089), így az LSD eljárást kell alkalmaznom. A vizsgálat eredményei azt bizonyítják, hogy az Innovátor szerephez szignifikánsan magasabb felhő érettségi szint tartozik, mint a Bróker, Mentor, Facilitátor, Koordinátor, Direktor, Producer és Monitor szerepekhez. A domináns Bróker, Mentor és Facilitátor szerepekhez tartozó felhő alapú megoldások alkalmazásának érettségi szintje szintén magasabb értéket kaptak, mint a Koordinátor, Direktor, Producer és Monitor szerepek.

A vizsgálat eredményei alapján meghatározott 3. tézis:
Szignifikáns kapcsolat mutatható ki a Versengő Értékek Keretrendszere szerinti domináns vezetői szerepek és a felhő alapú megoldások alkalmazásának érettségi szintjei között. A domináns Innovátor szerephez tartozó felhő érettségi szint szignifikánsan magasabb, mint a Bróker, Mentor, Facilitátor, Koordinátor, Direktor, Producer és Monitor szerepekhez. A domináns Bróker, Mentor és Facilitátor felhő alapú megoldások alkalmazásának érettségi szintje szintén szignifikánsabb magasabb értéket mutatnak, mint a Koordinátor, Direktor, Producer és Monitor szerepek.

4. hipotézis

A Cameron-Quinn szervezeti kultúrák közül azok esetében aktív a felhő megoldások használata, amelyek fogékonyak az innovációra, az úttörő megoldások bevezetésére.

A negyedik hipotézisem szervezeti kultúra szintjét azonosan közelítettem meg, mint a második hipotézisem esetében. A domináns szervezeti kultúrához tartozó felhő alapú megoldások alkalmazásának érettségi szintjeit megvizsgálva kijelenthető, hogy az egyes szervezeti kultúrák között szignifikáns különbség van. Az ANOVA teszt az F próbához tartozó valószínűség szignifikanciája 0,000, vagyis kisebb, mint 0,05, ezért a nullhipotézist elutasítom. Ezáltal a kategóriaátlagok szignifikánsan különböznek, vagyis az egyes szervezeti kultúrák, más és máshogy hatnak a felhő alapú megoldások alkalmazására. A Levene teszt eredménye szignifikáns (Sig=0,000), ezért a Post-Hoc elemzés során újra a Tamhane eljárást használtam. Az eredmények alátámasztják, hogy az Adhokrácia szervezeti kultúra kiemelten támogatja a felhő alapú megoldások előtérbe kerülését, a Klán típusú szervezetek közepesen érett képet mutatnak felhő alapú megoldások alkalmazása során, míg a Piac és Hiearchia szervezetek kevéssé támogatják ezen új technológiát.

A vizsgálat eredményei alapján meghatározott 4. tézis:

Szignifikáns kapcsolat mutatható ki a Versengő Értékek Keretrendszere alapján meghatározott domináns szervezeti kultúrák és a felhő alapú megoldások alkalmazásának érettsége között. A domináns Adhokrácia szervezeti kultúrákhoz tartozó felhő alapú megoldások alkalmazásának érettségi értéke szignifikánsan magasabb, mint a domináns Klán, Piac és Hierarchia szervezetek esetében. A domináns Klán szervezeti kultúra szignifikánsan magasabb érettségi szint jellemzi a felhő alapú megoldások érettségét tekintve, mint a domináns Piac és Hierarchia szervezeti formák.

6 A kutatás eredményeinek értékelése

Ebben a fejezetben a kutatás eredményeinek áttekintésével, értelmezésével, valamint a tézisek megfogalmazásával és a kutatási kérdések megválaszolásával foglalkozok. Ezen túlmenően ismertetem a vizsgálatom újszerűségét és gyakorlati alkalmazhatóságát. Bemutatom, hogy a jövőben milyen továbbfejlesztési lehetőségeket látok.

6.1 Eredmények értelmezése és kutatási kérdések megválaszolása

Kutatásom fő célja volt, hogy korábban egymástól teljesen önállóan vizsgált tudomány területeket egymáshoz közelebb hozzam és létrehozzam a közös vizsgálatuk lehetőségét úgy, hogy közben megtartsam azonos súlyukat. Ehhez azonban ki kellett választanom egy olyan, magyarországi piaci szektort, mely alkalmas szereplőinek számossága, mérete és fejlettségét tekintve a vizsgálat elvégzésére. Az irodalom feldolgozása mellett létrehoztam az eltérő tudományterületek vizsgálatának lehetőségét biztosító modellt. Ezt követően interjúkat és kérdőíves adatgyűjtést folytattam le a magyarországi telekommunikációs szektor szereplőin.

Első lépésként áttekintettem a szervezeti kultúrával és vezetői szerepekkel foglalkozó szakirodalmakat és modelleket. Azonosítottam azokat a megközelítéseket, amelyek lehetőséget biztosítanak az információbiztonság és a felhő megoldásokkal történő közös vizsgálatra, azaz létezik olyan kapcsolódási területük, amely segíti egységes modellbe rendezni őket. Kutatásom első szakaszában nem a teljes telekommunikációs szektorra, hanem csupán annak egy meghatározó szereplőjére fókuszáltam. Ennek részeként elvégeztem egy 92 főt magába foglaló strukturált interjút és a kapott eredmények segítségével elkészítettem esettanulmányomat. Ennek eredményeképpen kimondható volt, hogy az információbiztonság tényleges megvalósulására hatással van a felsővezetés biztonság iránti elkötelezettsége. A vizsgált szervezet esetében Adhokrácia típusú kultúrából a Hierarchikus irányba mozdult el a működés, mely az információbiztonság jelentőségének felértékelődésére vezethető vissza, ugyanis ezen kultúra esetében olyan működési sajátosságok tapasztalhatóak, amelyek kedveznek az információbiztonságnak pl.: szabályozottság, elszámolhatóság.

A kapott válaszok alapján megállapítható volt továbbá, hogy az információbiztonság menedzseléséért felelős terület feladatai átalakultak, aktívan részt kell venniük a felhő megoldások értékelésében. A felhő rendszerekkel szemben támasztott biztonsági elvárások meghatározása megtörtént. Kimutatásra került, hogy a felhő megoldások hatást gyakorolnak a belső üzemeltetési feladatkörökre. A strukturált interjúk tapasztalatait felhasználva pontosítottam a kutatási kérdéseket, az esettanulmányban meghatározottak közül kettőt később elhagytam:

- EK1: Milyen biztonsági elvárásokat támasztanak a vállalatok a felhő alapú alkalmazásokkal szemben?
- EK2: Hogyan hat a felhő alapú működés az információbiztonság menedzsmentjére?

Ehelyett inkább a szervezeti kultúrával és vezetői szerepekkel kapcsolatos kérdésekre összpontosítottam és bontottam tovább őket annak érdekében, hogy jobban megértsem hatásukat az információbiztonsági kiválóságra és felhő alapú megoldások alkalmazására.

Kvantitatív kutatásom során a Cameron-Quinn Versengő Értékek keretrendszerét alkalmaztam. Ennek segítségével meghatároztam az egyes interjú alanyok által adott válaszok alapján a domináns szervezeti kultúrákat, melyek között legnagyobb számban a Piac és Adhokrácia típus volt jelen. A vezetői szerepek azonosítása során faktoranalízis lefolytatására volt szükség. Az összevonások során több indikátor elhagyása történt meg, mivel a KMO érték és kommunalitási indikátor nem volt megfelelő, így nem tartoztak az egyes főkomponensekhez. A kapott eredmények alapján minden típusú vezetői szerep megjelent a mintában, de az Innovátor (26%) és a Direktor (21%) volt a legjellemzőbb.

Az információbiztonság és felhő alapú megoldások alkalmazása területén szintén vizsgáltam a már létező érettségi modelleket, melyeket szintetizálva létrehoztam egy olyan új érettségi megközelítést, ami lehetőséget biztosít arra, hogy mind a két terület felmérését el tudjam végezni. Azonban fontos volt, hogy az elemzés ne legyen túl mély hiszen cél egy átfogó kép megszerzése és annak összevetése a szervezeti kultúra és vezetői szerepekkel. Az információbiztonsági kiválóságot vizsgálva meghatároztam 4 faktort, melyek az eredeti információtartalom 64,483,%-át őrizték meg. Ez alapján a szervezet érettségi szintjét az információbiztonsági területek, a külső és belső információbiztonságot befolyásoló tényezők, valamint az információbiztonság menedzsment adják. Ez részben eltér az irodalomi feldolgozás alapján meghatározott kutatási modelltől, ahol úgy véltem, hogy a biztonság dimenzióit a területek, a fenyegetettségek felismerése és meghatározása, valamint az információbiztonság menedzsmentet alkotja. A mintán belül mind a négy érettségi szintben volt található szervezet, de a legmagasabb értéket csupán 5%-a érte el. Nem várt eredményként jelent meg, hogy a minta 36%-ában a legalacsonyabb érettségi szintet kaptam eredményként annak ellenére, hogy mára az információs rendszerek által tárolt adatok és üzletmenetet biztosító funkciók nélkül a szervezet működése lehetetlenülhet el.

A felhő alapú megoldások alkalmazásának területén 2 fő tényező köré csoportosíthatók a változók. Ezek közül az egyik a publikus, míg a másik a privát felhő szolgáltatásokat jellemző elemeket tartalmazza. Ezen eredmény nagyobb mértékben tért el az irodalmi feldolgozás követő modell meghatározásomtól, mint az az információbiztonsági kiválóság esetében tapasztaltam. Hiszen itt úgy gondoltam, hogy a felhő modellek, az üzemeltetés, a szolgáltatások és az információbiztonság menedzsment együtteséből fog összetevődni a felhő alapú megoldások alkalmazásának érettsége. Az SPSS elemzés során tapasztalható volt, hogy ezen tényezők mind részt vesznek az érettségi szint kialakításában, azonban teljesen eltérő módon csoportosulnak, mint azt korábban gondoltam. A vizsgált minta eredményei alapján kimondható,

hogy a válaszadók 33%-a olyan szervezetnél dolgozik, ahol a felhő alapú megoldások még nem, vagy csak minimálisan jelentek meg, 44%-uknál már igénybe veszik, de még nem képezi a mindennapi működés szerves részét az ilyen szolgáltatások. 23%-uk gondolja úgy azonban, hogy a felhő a jövő technológiája és használata elengedhetetlen.

A varianciaanalízis segítségével bizonyításra került, hogy minden magyarázó változó (szervezeti kultúra és vezetői szerepek) szignifikánsan befolyásolja a magyarázott változókat (információbiztonsági kiválóság és felhő alapú megoldások alkalmazása). A Piac és Hierarchia típusú szervezetekhez szignifikánsan magasabb információbiztonsági kiválóság tartozik, mint a Klán és Adhorkácia esetében. Ez arra vezethető vissza, hogy a szabályozottság, elszámolhatóság, valamint a kontrol megléte alapja az információbiztonságnak, amely területeken a Hierarchia kultúra erős. A Piac szervezeti kultúrára szintén jellemző a kontrolláltság, ami inkább a piaci/gazdasági szükségszerűség által meghatározott. Az ilyen szervezetek törekednek a piaci előnyök megszerzésére, ezáltal pedig kiemelten fontos számukra az adataik védelme is. Ezáltal pedig választ adtam a 2. kutatási kérdésemre, mellyel a következőre kerestem a választ: ***K2: Milyen szervezeti kultúra kedvez az információbiztonsági kiválóság érettségének?***

A vezetői szerepeket vizsgálva a Koordinátor, Direktor, Producer és Monitor vezetői szerepeknél fejlettebb információbiztonságot tapasztaltam, mint a Bróker, Innovátor, Mentor, Facilitátor esetében. A biztonsági szempontból előnyös jellemzőket mutat a Koordinátor a stabilitás, funkcionális területek összehangolása, valamint a munka tervezése révén. A Direktor szerep az irányításra, célok kitűzésére és szervezésre, a Procuder a hatékonyságra, termelékeny környezet biztosítására, a Monitor vezetői szerep pedig a dokumentálásra, teljesítmények figyelésére összpontosít. Ezek mind olyan kompetenciák, amelyek az információbiztonság fejlesztéséhez és fenntartásához elengedhetetlenek. Az így kapott eredmények segítségével az 1. kutatási kérdésemre adtam választ, azaz: ***K1: Milyen vezetői szerepek mellett fejlett információbiztonsági kiválóság?***

A felhő alapú megoldásokat vizsgálva már eltérő képet kaptam szervezeti kultúra és vezetői szerepek szempontjából. Az Adhokrácia szervezeti kultúra szignifikánsan magasabb érettségi értéket ért el a felhő alapú megoldások alkalmazása szempontjából, mint más kultúra típusok. Erősségei közé tartozik az innováció iránti elkötelezettség, azaz új megoldások és technológiák minél előbbi bevezetése. Közepesen érett, de még mindig fejlett képet mutatott a Klán típusú kultúra is. Megállapítható ez alapján, hogy a rugalmasság síknegyedében található szervezeti kultúrák nyitottak az új megoldásokra, így pedig a felhő alapú szolgáltatások szignifikánsabban jelennek meg esetükben. Ezen információk segítségével egyben választ adtam a 4. kutatási kérdésemre: ***K4: Milyen szervezeti kultúra nyitott a felhő alapú megoldások alkalmazására és bevezetésére?***

A vezetői szerepeket tekintve az Innovátor típusú vezető mutatta a legmagasabb értékeket a felhő alapú megoldások alkalmazásának tekintetében, amely nem meglepő, hiszen az Adhokrácia kultúrához tartozó vezetői szerep, így a korábbi eredmények előre vetítették, hogy jól fog teljesíteni. Azonban meglepő, hogy Bróker vezetői szerep nem teljesített annyira jól, annak ellenére, hogy szintén Adhokrácia kultúra egyik jellemző vezetési stílusa. Ez az ellenmondás azonban megengedett, mivel adott vezetői szituációban az egyik vagy másik megközelítés előnyösebb. Ahogy a Klán típusú kultúra kevésbé volt érett, mint az Adhokrácia típusú felhő alapú megoldások alkalmazásának tekintetében, úgy a hozzá tartozó jellemző vezetői szerepeket, mint a Mentor és Facilitátor szintén alacsonyabb érettség jellemez. Így pedig a 3. egyben utolsó kutatási kérdésem megválaszolása is megtörtént: ***K3: Milyen vezetői szerepek jelenléte támogatja a felhő alapú megoldások alkalmazását?***

Összefoglalva az eredményeket a magas információbiztonsági kiválósági szint eléréséhez szükséges a szabályozottság, elszámolhatóság, valamint a kontrol megléte egy szervezet működésében. Vezetői irányból történő megközelítés esetében pedig a stabilitás, funkcionális területek összehangolása, a munka tervezése, a célok kitűzése és szervezése, valamint a termelékeny környezet biztosítására történő összpontosítás kedvezően fog hatni az információbiztonságra. Kimondható az is, hogy ha egy szervezet számára fontos ezen terület fejlesztése, vagy a már elért érettségi szint megtartása szervezeti tulajdonságok tekintetében törekednie kell a Piac vagy Hierarchia szervezeti kultúra megteremtésére, vezetői szerep szerinti jellemzőit leginkább a Koordinátor, Direktor, Producer vagy Monitor irányába kell fejlesztenie. A felhő alapú megoldások alkalmazásának előmozdításához szükséges az innováció, azaz új megoldások és technológiák minél előbbi bevezetése iránti szervezeti elkötelezettség, míg vezetői szempontból a változások támogatása és előmozdítása iránti hajlam megléte szükséges. Ahhoz, hogy ezen tulajdonságok megjelenjenek egy szervezet működésében szükséges, hogy Adhokrácia vagy Klán kultúra irányába mozduljon el a mindennapi működés és vezetői szerepek jellemzőit leginkább az Innovátor típusú vezetői jellemzők irányába kell elmozdítani.

6.2 Önálló, újszerű eredmények

Munkám során mind szervezeti, mind pedig technológiai oldalról is vizsgáltam a vállalatok működését. Megközelítésemben újszerű, hogy nem önálló rendszerként tekintek az egyes tudományterületekre, hanem azt a célt tűztem ki, hogy együttes vizsgálatukat végzem el. Ilyen szintű összevonása eltérő tudományágaknak korábban nem történt meg. Találhatóak olyan törekvések, ahol az információbiztonság területek vizsgálata során igyekeztek a menedzsment aspektust bevonni, de ez csak részleteiben történt meg. Hiányzott az a megközelítés, mely a technikai területeket ne részleteiben és mélyen kívánja vizsgálni, hanem csak olyan mértékben, amely még alkalmas a kultúrához és vezetői szerepekhez kapcsolódás lehetőségének megteremtésére. Számos kutatás érhető el ma, amelyek egy-egy tématerületre mély és hasznos elemzéseket hajtottak végre, de kutatásommal célom volt, hogy ezeket tovább gondolva, átfogó képe és egyfajta iránymutatást tudjak biztosítani a menedzsment

számára. A vezetőknek ugyanis az őket érő terhelés miatt nincs idejük hosszú tanulmányok részletes megértésre. Mindennapi munkám során én is tapasztalom, hogy már egy hosszabb, túl részletes email elolvasása is problémát jelenthet és a vezető azt hajlamos "majd később elolvasom" címkével ellátni. Azonban mindannyian tudjuk, hogy ezek egy jó része sose kerül feldolgozásra. Úgy gondolom, hogy nincs ez másképp sok kutatási eredménnyel, tanulmánnyal sem. Ezért létrehoztam egy olyan útmutatót, amely gyors áttekintéshez, az összefüggések megértéséhez ad segítséget anélkül, hogy a vezetőknek el kéne mélyedniük az adott tudományágakban.

Azért, hogy ezt elérjem már magát az információbiztonságot és felhő alapú megoldások felmérését is máshogy közelítettem meg, mint korábban tették. Az útmutató elkészítéséhez nem volt szükség részletes, mély elemzésre, hiszen abban az esetben rengeteg olyan információt tartalmazott volna felmérésem, melyek a modell és a kívánt összefüggések szempontjából nem lettek volna relevánsak. Munkám kiemelkedő eredménye továbbá, hogy nem csak egy vállalat mély vizsgálatát hajtottam végre, hanem törekedtem arra, hogy egy teljes iparágat felmérjek, a megkapott eredményeket pedig képes legyek más, hasonló jellemzőkkel bíró iparágakra is érvényessé tenni.

6.3 A kutatás eredményeinek gyakorlati alkalmazása

A létrehozott információbiztonsági kiválóság, valamint a felhő alapú megoldások alkalmazásának felmérésére kialakított módszer és kérdőív hasznos minden olyan vezető számára, aki szeretne egy átfogó képet kapni arról, hogy szervezete milyen szinten áll ezen technológiai területeken, valamint azon belül mely pontok az erősségeik és gyengeségeik. Ha elvégzik kérdőívem alapján a felmérést nem csak azt tudják meghatározni, hogy milyen szervezeti kultúra és vezetői szerepek a dominánsak jelenleg, hanem arra is kaphatnak visszajelzést, hogy a dolgozók szerint, melyek lennének a kívánatosak. Ugyanezt az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazása során is el lehet végezni a létrehozott kérdőívem segítségével. Így a vezetés saját elképzeléseit össze tudja hasonlítani a teljes szervezet véleményével, akik a mindennapi működésről a legtöbb információval rendelkeznek. Ez pedig óriási segítség tud lenni a szervezet stratégiájának megalkotásakor. Továbbá úgy gondolom, hogy ez a magas szintű rávilágítás képes támogatni, hogy a vezető a megfelelő területre irányítsa figyelmét és megtegye a szükséges beavatkozásokat. Ezáltal pedig növelve a beruházások hatékonyságát, mivel azok pontosan oda tudnak érkezni, ahol a fejlesztés szükséges. Ez azért is jelentős előrelépés, mivel korábban a szervezeti és a technológiai változtatások pontos hatásmechanizmusa nem volt ismert a felsővezetés számára, így egy-egy beavatkozással akár a kívánt fejlődéssel ellentétes irányú eredményt érhetnek el. De a létrehozott kérdőívvel és modellel már képes egy szervezet könnyen és egyszerűen felmérni működését és nem szükséges csupán iparági ajánlásokra hagyatkoznia. Ennek fontossága abban rejlik, hogy saját területeinek egymásra hatása akár nagyban el is térhet az iparágban tapasztaltaktól, így pedig egy olyan eszközhöz jutnak, amelyet felhasználva az iparági javaslatokat testreszabhatják.

Kidolgoztam egy felsővezetői útmutatót, mely általános segítséget nyújt a vezetők számára, ha nem szeretnének mélyebb vizsgálatot végezni, de mégis kíváncsiak arra, hogy az egyes szervezeti kultúrák és vezetői szerepek miképp hatnak magára az információbiztonsági kiválóságra és a felhő alapú megoldások alkalmazására a technológia intenzív iparágakban.

A 20. táblázat segítséget nyújt abban, hogy megértsék, mely szervezeti kultúra és vezetői szerep képes az információbiztonsági kiválóságot, vagy a felhő alapú megoldások alkalmazását előremozdítani.

20. táblázat: Információbiztonsági kiválóság és felhő alapú megoldások alkalmazását előmozdító szervezeti kultúrák és vezetői szerepek

	Szervezeti kultúra	Vezetői szerep
Információbiztonságot kíván javítani	Piac	Producer Direktor
	Hiearchia	Monitor Koordinátor
Felhő alapú megoldások alkalmazását kívánja előmozdítani	Adhokrácia	Innovátor Bróker
	Klán	Mentor Facilitátor

Azonban, ha figyelembe vesszük, hogy a szervezeti kultúra egy lassan változó tényező szükséges az előző javaslatot finomhangolni annak érdekében, hogy csupán a vezetői szerep megváltoztatásával pozitív hatást lehessen gyakorolni a fent említett technológiai területekre. A 21. táblázatban az egyes szervezeti kultúrákhoz tartozó vezetői szerepek közül azt emelem ki, amely információbiztonsági kiválóságot és a felhő alapú megoldások alkalmazását a legnagyobb mértékben tudja előremozdítani.

21. táblázat: Az egyes szervezeti kultúrákhoz tartozó ideális vezetői szerepek figyelembe véve az információbiztonsági kiválóság és a felhő alapú megoldások szintjét

Szervezeti kultúra	Információbiztonsági kiválóság	Felhő alapú megoldások alkalmazása
Klán	Facilitátor	Mentor
Adhokrácia	Innvoátor	Innovátor
Piac	Direktor	Direktor
Hierarchia	Koordinátor	Koordinátor

Az elkészült útmutató alapján felismerhető, hogy az Adhokrácia, Piac és Hierarchia estében egyértelműen meghatározható, hogy mely vezetői szerep alkalmas egyszerre az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazása terén is pozitív hatást elérni.

6.4 További kutatási irányok kijelölése

A vizsgálat során összegyűjtött adatok számos további elemzésre adnak lehetőséget, azonban magát az adatgyűjtés spektrumát és idősíkját is tovább lehet szélesíteni. Ez alapján lehetőség van a vizsgált iparágból történő kilépésre (pl.: bankszektor, autóipar). Azt gondolom erre azért is van szükség, mert ezen iparágak tevékenységének alapját ugyancsak az informatika jelenti, azonban működésük hatékonysága a teljes magyarországi gazdaság stabilitására sokkal nagyobb hatással lehet.

Fontosnak tartom az idő bevonását is a modellbe, mivel eddig csak a szervezetek jelenlegi helyzetét mértem fel, azonban a kívánatos állapot feltárása egyrészt segítséget nyújtana megismerni és szintetizálni a jövőben elérni kívánt működést. Másrészt lehetőséget adna arra, hogy egy olyan, változtatásokból álló utat rajzoljunk fel a szervezeti kultúra, vezetői szerepek, információbiztonság kiválóság és felhő alapú megoldások alkalmazásának bevonásával, amely segít megérteni és elérni a vállalatvezetés számára a kívánt működést.

Meggyőződésem, hogy a modellbe bevont tudomány területek körét is szükséges lenne bővíteni, annak érdekében, hogy a szervezeten belül uralkodó erőviszonyokat jobban megértsük és befolyásolni legyünk képesek, a felrajzolt relációs adatmodell segítségével. Ilyen potenciális, bevonásra alkalmas területként tekintek a humán erőforrásra, valamint a projektmenedzsmentre.

Mivel kutatásomban csupán egy irányú hatást vizsgáltam, azaz csak a szervezeti kultúra és vezetői szerepekre tekintettem, mint magyarázó változó azt gondolom szükséges a jövőben az információbiztonság, a felhő alapú megoldások alkalmazásának hatásait is megvizsgálni a szervezeti kultúrára és vezetői szerepekre.

A fent felsorolt bővítési lehetőségekkel létrehozható egy a szervezeti kultúrára, vezetői szerepekre, humán erőforrásra, projektmenedzsmentre, információbiztonságra, információs technológiák (ilyen pl. a felhő) használatára kiterjedő modell, melyben már nem csak a szervezeti kultúra és vezetői szerepek hatását vizsgálnám az egyes területekre, hanem egy olyan mátrixot lehetne megalkotni, amelynek csomópontjait az egyes vizsgált tudományterületek alkotnák, míg a köztük lévő relációkat pedig az őket összekötő élek. Az így létrehozott megközelítést tovább bővíteném az idővel, mint egy plusz dimenzióval ezáltal pedig létrehozva egy 3D-ós mátrixot, ezáltal képesek lennék a szervezetek teljes működését leképezni beleértve a területeket és az idő faktort is.

7 Összefoglalás

Kutatásom az a gazdasági/társadalmi probléma indokolta, hogy a vezetők még mai is sok esetben az IT-ra, mint fekete dobozra tekintenek. Nem értik annak működését és minden beruházási és üzemeltetési költséget, amelyet ez a terület igényel felesleges pénzkidobásnak tartanak. Mára azonban többen felismerték, hogy az információbiztonság kritikus, valamint a felhő megoldások segítségével akár költségeik is csökkenthetőek, de azzal végképp nincsenek tisztában, hogy miképp is kellene ezeket a területeket kezelni. Gyakran még a saját szervezetük kultúráját se mérik fel, hanem csak "működnek", holott, ha a fenti témákban fejlődést kívánnak elérni nem elég csupán beruházni. Sok esetben tapasztalható az, hogy óriási pénzek elköltése után sem történik radikális előrelépés. De vajon mi lehet ennek a hátterében? A fejlesztésekért felelős vezetők, az alattuk lévő dolgozók, vagy maguk a projekt menedzserek a hibásak? Kutatásom alapján elmondható, hogy a hibát sokszor magában a szervezeti kultúrában, a menedzsment vezetési stílusában kell keresni. Hiszen hiába tudjuk, hogy előnnyel járhat egy felhő alapú megoldás alkalmazása, ha azt a szervezet maga nem fogadja el és "bojkottálja" az ilyen irányú törekvéseket.

Azért, hogy a problémák mélyére lássak kutatásom célja volt, hogy megismerjem a kultúra dimenziók és vezetői szerepek által az információbiztonságra és felhő alapú megoldások alkalmazására gyakorolt hatásait. Ehhez szükségem volt az információbiztonsági kiválóság és felhő alapú megoldások alkalmazását vizsgáló olyan új modell létrehozására, mely megteremti a különböző tudományágak összekapcsolásának lehetőségét is.

A kutatás megalapozásának érdekében áttekintettem a hazai és nemzetközi szakirodalmakat. A szervezeti kultúra és vezetői szerepek területén létező modelleket megismertem és a kutatási kritériumoknak legmegfelelőbbet, a Cameron-Quinn Versengő Értékek keretrendszerét választottam ki. Az információbiztonság és felhő érettségi modellek áttekintése és szintetizálását követően fel kellett ismernem, hogy azok csupán részben lennének alkalmasak kutatási kérdéseim megválaszolására, ezért építve rájuk, de új megközelítést hoztam létre.

Az empirikus kutatás során mind kvalitatív, mind pedig kvantitatív módszert is felhasználtam. Kvalitatív vizsgálat során strukturált interjúkat folytattam le az IT és információbiztonsági területeken dolgozókkal. Kvantitatív vizsgálat során az egész országra kiterjedő felmérésben minden olyan telekommunikációs vállalat szakértőit és vezetőit kerestem meg, amelyek elérték a minimum 500 fő foglalkoztatási határt.

A statisztikai és ökonometriai elemzések során létrehoztam az információbiztonsági kiválóság, valamint felhő alapú megoldások alkalmazásának faktorjait és ezek segítségével megállapítottam a vizsgált

szervezetek érettségét. Ezt követően összefüggéseket kerestem a szervezeti kultúra, vezetői szerepek és a feljebb említett érettségi szintek között.

Megállapítottam, hogy a domináns szervezeti kultúra és vezetői szerepek szignifikáns hatást gyakorolnak az információbiztonsági kiválóságra és a felhő alapú megoldások alkalmazására. Azon szervezetek esetében, ahol a domináns szervezeti kultúra Piac és Adhokrácia, az információbiztonsági kiválóság értékek szignifikánsan magasabbak. A vezetői szerepek esetén pedig a Koordinátor, Direktor, Producer és Monitor vesznek fel szignifikánsan magasabb értékeket információbiztonsági kiválóság szempontjából. A felhő alapú megoldások alkalmazása esetében szervezeti kultúra szempontjából az Adhokrácia, míg a vezetői szerepek közül az Innovátor esetében tapasztalható szignifikánsabb magasabb érettségi szint.

Az eredmények áttekintése során ellenőriztem a hipotézisek helytállóságát, valamint ezek alapján megfogalmaztam a téziseimet. A kutatási kérdések megválaszolása megtörtént, továbbá meghatároztam a gyakorlati alkalmazás lehetőségét, mivel azt gondolom, hogy egy kutatás alapvető célja kell, hogy legyen a mindennapi értékteremtés. A vizsgálat során összegyűjtött tapasztalatok alapján definiáltam a kutatás folytatásának lehetőségét is.

8 Irodalomjegyzék

1. Agrawal, D., Das, S. & Abbadi, A. E., 2012. *Data Management in the Cloud: Challenges and Opportunities (Synthesis Lectures on Data Management).* London: Morgan & Claypool Publishers.
2. Akanji, B. és mtsai., 2019. The influence of organisational culture on leadership style in higher education institutions. *Personnel Review,* pp. 1-26.
3. Ali, M., Khan, S. U. & Vasilakos, A. V., 2015. *Security in cloud computing: Opportunities and challenges.* North Dakota State: Information Sciences.
4. Alqassemi, S., Ever, Y. K. & Rajan, A. V., 2017. *Maturity Level of Cloud Computing at HCT.* Dubai, Institute of Electrical and Electronics Engineers .
5. Alvesson, M. & Sveningsson, S., 2007. *Changing Organizational Culture..* hely nélk.:Routledge.
6. Angyal, Á., 2009. *Vállalatok társadalmi felelőssége, felelős társaságirányítás.* Budapest: Kossuth Kiadó.
7. Ansoff, I. H., 1991. Critique Of Henry Mintzberg's 'The Design School: Reconsidering The Basic Premises Of Strategic Management. *Strategic Management Journal,* pp. 449-461.
8. Argyris, C. & Schön, D. A., 1978. *Organizational learning: A theory of action perspective.* hely nélk.:Reading, Mass: Addison Wesley .
9. Babbie, E., 2017. *A társadalomtudományi kutatás gyakorlata.* Budapest: Balassai Kiadó.
10. Bakacsi, G., 2004. *Szervezeti magatartás és vezetés.* hely nélk.:AULA KIADÓ Kft..
11. Bakacsi, G., 2010. *A szervezeti magatartás alapjai.* Budapest: Aula.
12. Bakacsi, G., 2012. A GLOBE-kutatás kultúraváltozóinak vizsgálata faktoranalízis segítségével. *Vezetéstudomány,* pp. 12-22.
13. Balogh, Á., 2011. *Kulturális intelligencia – a 21. század kulcskompetenciája?,* Veszprém: Pannon Egyetem.
14. Balogh, Á., Gaál , Z. & Szabó, L., 2011. Relationship Between Organizational Culture and Cultural Intelligence. *Management & Marketing Challenges for the Knowledge Society,* 6(1), pp. 95-110.
15. Barna, I. & Székelyi, M., 2008. *Túlélőkészlet az SPSS-hez.* Budapest: Typotex Elektronikus Kiadó Kft..
16. Barrett, M. P., 2018. *Framework for Improving Critical Infrastructure Cybersecurity,* Gaithersburg: National Institute of Standards and Technology.
17. Bauer, P., 2010. *Introducing a Capacity Management Maturity Model.* [Online] Available at: http://www.teamquest.com/pdfs/whitepaper/maturity-model.pdf
18. Beloglazov, A., 2013. *Computing, Energy-Efficient Management of Virtual Machines in Data Centers for Cloud,* Melbourne : Department of Computing and Information Systems The University of Melbourne .

19. Birmingham, P. & Wilkinson, D., 2003. *Using Research Instruments (Routledge Study Guides) (Volume 2).* London: Routledge.
20. Bogdány, E., 2014. *Átadni tudni kell! Vezetői szerep átadás a hazai kis- és középvállalkozásokban.,* Veszprém: Pannon Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola.
21. Bognár, F. & Gaál, Z., 2013. A beszállítói kapcsolatok megbízhatósági és karbantartási konzekvenciái. *Vezetéstudomány,* pp. 14-21.
22. Botta, A., 2016. Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems,* p. 684–700.
23. Boukalas, C., 2014. *Homeland Security, Its Law and Its State: A Design of Power for the 21st Century.* New York: Routledge.
24. Bowen, P. & Kissel, R., 2017. *Program Review for Information Security Management Assistance (PRISMA),* Gaithersburg: National Institute of Standards and Technology.
25. Bower, M., 1966. *The Will to Manage: Corporate Success Through Programmed Management.* hely nélk.:Mcgraw-Hill; First Edition edition .
26. Brostoff, S. & M.A., S., 2001. Safe and sound: a safety-critical approach to security. *ACM: Cloudcroft,* pp. 41-50.
27. Buecker, A., Arunkumar, S., Blackshaw, B. & Borrett, M., 2014. *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security.* hely nélk.:IBM.
28. Buyya, R., Broberg , J. & Goscinski, A., 2013. *Cloud Computing: Principles and Paradigms.* Hoboken: Wiley.
29. Cacciattolo, K., 2014. Understanding Organisational Cultures. *European Scientific Journal,* pp. 1-7.
30. Cameron & Quinn, 2000. Diagnosing and Changing Organization Culture. In: hely nélk.:Electronically reproduced by permission of Pearson Education, Inc. Upper Saddle River, New Jersey..
31. Cameron, K. S. & Quinn, R. E., 2006. *Diagnosing and changing organizational culture: based on the competing values framework.* San Francisco: Revised ed. John Wiley & Sons .
32. Cameron, K. S. & Quinn, R. E., 2011. *Diagnosing and changing organizational culture: based on the competing values framework.* San Francisco: Jossey-Bass.
33. Cameron, K. S., Quinn, R. E., DeGraff, J. & Thakor, A. V., 2007. *Competing values leadership: Creating value in organizations.* Northampton: Edward Elgar Publishing.
34. Caroll, G. & Harrison, R. J., 2005. Organizational demography and culture: Insights from a formal model and simulation. *Administrative Science Quarterly,* pp. 637-667.
35. Catteddu, D. & Hogben, G., 2009. *Benefits, risks and recommendations for information security,* Heraklion: ENISA - European Union Agency for Network and Information Security.
36. Cavelty, M. D., 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Zurich: The Swedish Institute Of International Affairs.

37. Chawla, V. & Sogani, P., 2011. *Cloud Computing – The Future.* India, Springer, pp. 113-118.
38. Chou, D. C., 2015. Cloud computing: A value creation model. *Computer Standards & Interfaces,* p. 72–77.
39. Consorcium, I., 2007. *ISM3 - Information Security Managment Maturity Model.* Spain: ismeretlen szerző
40. Conway, G. & Curry, E., 2012. *Managing Cloud Computing: A Life Cycle Approach.* Porto, Springer.
41. Conway, G., Doherty, D. E., Carcary, D. M. & Crowley, C., 2017. *Enterprise Cloud Adoption - Cloud Maturity Assessment Model.* Maynooth, Innovation Value Institute.
42. Covin, J. G. & Slevin, D. P., 1990. Juggling enterpreneurial and organizational structure. How to act together. *Sloan Management Review,* pp. 43-53.
43. Creswell, J. & Plano Clark, V., 2010. *Designing and Conducting Mixed Methods Research.* Thousand Oaks, California: SAGE Publications.
44. Csallner, A., 2015. *Bevezetés az SPSS statisztikai programcsomag használatába,* Szeged: Szegedi Tudományegyetem.
45. Deal, T. & Kennedy, A., 2000. *Corporate Culture: The Rites and Rituals of Corporate Life.* Cambridge: Perseus Books.
46. Dekker, M. & Liveri, D., 2015. *Cloud Security Guide for SMEs,* Heraklion: ENISA - European Union Agency for Network and Information Security.
47. Dekker, M., Liveri, D. & Matina, L., 2013. *Cloud Security Incident Reporting,* Heraklion: European Union Agency for Network and Information Security.
48. Denzin, N. K., 2016. *Triangulation 2.0.* Pennsylvania: SAGE Journal.
49. Dobák, M. & Antal, Z., 2016. *Vezetés és szervezés.* Budapest: Akadémia Kiadó Kft..
50. Dobi, L., Szűcs, E., Takács, T. & Matkó Andrea, 2013. Vezetési stílusok és a szervezeti kultúra kapcsolatának azonosítása egy magyarországi Zrt-nél. *Debreceni Műszaki Közlemények,* pp. 94-111.
51. Draft, R. L., 2012. *Management.* Mason: South-Western.
52. Drogseth, D., 2011. *The Road to the Responsible Cloud,* Boulder: EMA - IT & Data Management Research , Industry Analysis & Consulting.
53. Duarte, A.́. & Mira da Silva, M., 2013. *Cloud Maturity Model.* Santa Clara, IEEE Xplore.
54. Dykas, W., 2007. Cyber Security...A circular Maturity Model. *3rd Annual Cyber Security Summit.*
55. Educause, 2009. *7 things you should know about cloud computing.,* hely nélk.: Educause.
56. Fayol, H., 1981. *Administration industrielle et générale.* Paris: Dunod.
57. Fehér, P., Kő, A. & Szabó, Z., 2016. Kapacitásmodellezés és az IT-architektúratervezés kihívásainak vizsgálata statisztikai és prediktív analitikai eszközökkel. *Statisztikai szemle,* pp. 1149-1164.

58. Fekete - Berzsenyi, H., 2017. *erre tart a hajó?: A szervezeti stratégia, a struktúra és a kultúra hatásainak vizsgálata a vállalati teljesítményre II. kötet.* Riga: GlobeEdit.
59. Gaál, Z., 1999. Emberi tőke – szervezeti kultúra. *Harvard Business Manager ,* pp. 69-76.
60. Gaál, Z., Szabó, L. & Obermayer-Kovács, N., 2009. „Tudásmenedzsment-profil" érettségi modell. *Vezetéstudomány.*
61. Gao, X., Zhong, W. & Mei, S., 2013. nformation Security Investment When Hackers Disseminate Knowledge. *Decision Analysis,* pp. 352-368.
62. Geoffrey Karokola, Stewart Kowalski, Louise Yngström, 2011. Towards An Information Security Maturity Model for Secure e-Government Services: A Stackeholders View. *Department of Computer and System Sciences Stockholm Univerity/Royal Institute of Technology.*
63. Girma, S., 2016. The relationship between leadership style, job satisfaction and culture of the organization. *International Journal of Applied Research,* pp. 35-45.
64. Goleman, D., Boyatzis, R. & McKee, A., 2003. *Primal Leadership: Realizing the Power of Emotional Intelligence.* Boston: Harvard Business Review Press.
65. Goyal, S., 2014. Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *I.J. Computer Network and Information Security,* pp. 20-29.
66. Grace, L., 2010. *Basics About Cloud Computing,* Pittsburgh: Software Engineering Institute Carniege Mellon University.
67. Gregory, R., Prifling, M. & Beck, R., 2009. The role of cultural intelligence for the emergence of negotiated culture in IT offshore outsourcing projects. *Information Technology & People,* 22(3), pp. 224-241.
68. Grivas, S. G., Peter, M., Giovanoli, C. & Hubli, K., 2018. FHNW Maturity Models for Cloud and Enterprise IT. *Business Information Systems and Technology 4.0,* pp. 133-146.
69. Guangming , C., Yao , L., Zhiwei , G. & Xiaoyin , L., 2017. *Cloud data governance maturity model.* Beijing, IEEE Press.
70. Haig, Z., Hajnal, B., Kovács, L. & Muha, L., 2009. *A kritikus információs infrastruktúrák meghatározásának módszertana,* Budapest: ENO Advisory Kft.
71. Hampden-Turner , C. & Trompenaars, F., 2006. Cultural Intelligence: Is Such a Capacity Credible?. *Group & Organization Management,* pp. 56-63.
72. Handy, C. B., 1999. *Understanding Organisations.* Harmondsworth: Penguin.
73. Handy, C., 1995. *Gods of Management: The Changing Work of Organizations. 4 Sub edition.* US: Oxford University Press.
74. Hansen, R., 2016. *Cyber Security Capability Assessment,* Tallinn: Tallin University of Technology.
75. Harrison, R. L., 1992. Toward a Theory of Inter-Refuge Corridor Design. *Conservation Biology,* pp. 293-295.
76. Hax, A. C. & Majluf, N. S., 1984. *Strategic Management: An Integrative Perspective.* New Jersey: Prentice Hall; Facsimile edition.

77. Heidrich, B., 2001. *Szervezeti kultúra és interkulturális menedzsment.* hely nélk.:Human Telex Consulting.
78. Heidrich, B., 2001. *Szervezeti kultúra és interkultúrális menedzsment.* Budapest: Human Telex Consulting .
79. Hills, M. D., 2002. *Kluckhohn and Strodtbeck's Values Orientation Theory,* Melbourne: International Association for Cross-Cultural Psychology.
80. Hofstade, G., 2010. *Cultures and Organisations: Software for the Mind.* London: McGraw-Hill.
81. Hofstede, G., 1980. *Culture's Consequences: International Differences in Work - Related Values.* Beverli Hills: ismeretlen szerző
82. Hofstede, G., Hofstede, G. J. & Minkov, M., 2010. *Cultures and organizations; Software of the mind.* New York: McGraw-Hill.
83. Horváth, V., 2018. *A projektmenedzsment kompetencia és a projektsiker összefüggései az olajipar projekt-intenzív upstream üzletágában.* Veszprém: Budapesti Corvinus Egyetem.
84. Hosking, D. M., 1988. Organising, leadership and skilful process. *Journal of Management Studies,* pp. 147-166.
85. House, R. J., Hanges, P. J., Javida, M. & Dorfman, P. W., 2004. *ulture, Leadership, and Organizations: The GLOBE Study of 62 Societies.* California: Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies.
86. IBM, 2008. *Information Security Maturity Model - How can we grow from ISO17799/27001 certification?.* hely nélk.:ismeretlen szerző
87. ISACA, 2010. *Cloud Computing Management Audit/Assurance Program.* [Online] Available at: https://www.isaca.org/Pages/default.aspx
88. Jahdwanl, P., 2012. *GTSI Cloud Computing Building a Framework for Succesful Transition,* hely nélk.: ismeretlen szerző
89. Jaiswar, S., 2011.. *Private cloud setup in six easy steps.* [Online] Available at: http://searchdatacenter.techtarget.in/tip/Private-cloud-setup-in-six-easy-steps
90. Jensen , E. & Laurie , C., 2016. *Doing Real Research: A Practical Guide to Social Research.* SAGE Publications Ltd: Thousand Oaks.
91. Jermier, J. & Forbes, R., 2016. Metaphors, organizations and water: Generating new images for environmental sustainability. *Human Relations,* p. 1001–1027.
92. Karcsics, É., 2011. *Menedzseri kompetencia-elvárások a munkaerőpiacon. Doktori értekezés..* Budapest: Budapesti Műszaki- és Gazdaságtudományi Egyetem, Gazdálkodás- és Szervezéstudományi Doktori Iskola.
93. Karcsics, É., 2012. Vezetőkkel szemben támasztott munkaerő-piaci kompetencialvárások a heti világgazdaság és a the economist álláshirdetéseinek elemzése alapján. *Vezetéstudomány,* pp. 31-44.

94. Kargas, A. & Varoutas, D., 2015. On the relation between organizational culture and leadership: An empirical analysis. *Cogent Business & Management ,* pp. 1-18.
95. Karokola, G., Kowalski, S. & Yngström, L., 2011. *Towards An Information Security Maturity Model for Secure e-Government Services: A Stackeholders View.* London, University of Plymouth.
96. Karoliny, M. & Poór, J., 1994. *Személyzeti/emberierőforrásmenedzsment kézikönyv.* Budapest: Közgazdasági és Jogi Könyvkiadó.
97. Kavis, M. J., 2014. *Architecting the Cloud.* New Jersey: John Wiley & Sons Inc.
98. Kemp, L., 2016. 'Trapped' by metaphors for organizations: Thinking and seeing women's equality and inequality. *Human Relations,* p. 975–1000.
99. Kiss, C. & Csillag, S., 2014. *Szervezeti kultúra,* Budapest: NKE.
100. Kluckhohn, C., 1951. Values and value-orientations in the theory of action: An exploration in definition and classification.
101. Kluckhohn, F. & Strodtbeck, F. L., 1973. *Variations in Value Orientations.* London: Greenwood Press.
102. Kollman Tobias, Stöckmann, C., Linstaedt, J. & Kensbock, J., 2015. *European Startup Monitor,* hely nélk.: KPMG.
103. Kosztyán, Z., 2014. *Projektek és üzleti folyamatok tervezése, nyomon követése.* Veszprém: ismeretlen szerző
104. Kotter, J. P., 2012. *Leading change.* Boston: Harvard Business School Press.
105. Kovács, L. & Krasznay, C., 2017. Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* pp. 3-16.
106. Kovács, L., 2018. *A kibertér védelme.* Budapest: Dialóg Campus Kiadó.
107. Központi Statisztikai Hivatal, 2019. *Az infokommunikációs szektor helyzete,* Budapest: Központi Statisztikai Hivatal.
108. Kroeber, A. L. & Kluckhohn, C., 1978. *Culture: A Critical Review of Concepts and Definitions.* hely nélk.:Kraus Reprint Company.
109. Kvale, S., 2014. *InterViews: An Introduction to Qualitative Research Interviewing.* Thousand Oaks: SAGE Publications.
110. Lee, C. H., Geng, X. & Raghunathan, S., 2016. Mandatory Standards and Organizational Information Security. *Information Systems Research,* pp. 70-86.
111. Lessing, M., 2008. Best Practices show the way to Information Security Maturity. *Council for Scientific and Industrial Research, South Africa.*
112. Levitt, T., 2003. The Globalization of Markets. *Harvard NOM Working Paper ,* pp. 92-102.
113. Lippert, R., Gaál, Z. & Kovács, T., 2015. A vezetői szerepek és a szervezeti kultúra hatása a klasztersiker érettségi modelljére. *Vezetéstudomány,* pp. 2-13.
114. Liveri, D. & Skouloudi, C., 2016. *Exploring Cloud Incidents,* Heraklion: ENISA - European Union Agency for Network and Information Security.

115. Marchese, K., Crane, J. & Haley, C., 2015. 3D opportunity for the supply chain: Additive manufacturing delivers. *Deloitte University Press.*
116. Mathur, N. & Purohit, R., 2017. Issues and Challenges in Convergence of Big Data, Cloud and Data Science. *International Journal of Computer Applications (,* February, 160(9), pp. 7-12.
117. Matkó, A., 2016. Versenyképesség és szervezeti kultúra vizsgálata az észak-alföldi régió önkormányzatainál. *Gazdálkodási - és Szervezéstudományi Folyóirat: A Virutális Iintézet Közép - Európai kutatására közleményei,* pp. 87-97.
118. Mattoon, S., Hensle, B. & Baty, J., 2011. *Cloud Computing Maturity Model Guiding Success with Cloud Capabilities,* California: Oracle.
119. Mattoon, S., Hensle, B. & Baty, J., 2011. *Oracle: Cloud Computing Maturity Model,* hely nélk.: ismeretlen szerző
120. Mazutis, D. & Slawinski, N., 2008. Leading Organizational Learning Through Authentic. *Dialogue Management Learning,* 39. kötet, pp. 437-456.
121. Mead, R., 1998. *International management. Cross cultural dimensions.* Massachussets: Blackwell Publisher Inc..
122. Metzler, A., 2009. *The Mandate to Implement Unified Performance management.* [Online].
123. Mintzberg, H., 2010. *A menedzsment művészete.* Budapest: Alinea Kiadó.
124. Mitra, S. & Ransbotham, S., 2015. Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research,* pp. 565-584.
125. Mohelska, H. & Sokolova, M., 2015. Organisational Culture and Leadership – Joint Vessels?. *Procedia - Social and Behavioral Sciences,* pp. 1011-1016 .
126. Morgan, G., 2007. *Images of Organization.* London: SAGE Publications, Inc.
127. Munk, S., 2018. A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* pp. 113-131.
128. Nagaraj, C. & Sathish kumar, N. M., 2015. Cloud Computing With a Model Futuristic Maturity. *International Journal of Advance Research In Science And Engineering.*
129. Naranjo-Valencia, J. C., Jimenez-Jimenez, D. & Sanz Valle, R., 2011. Innovation or imitation? The role of organizational culture. *Management Decision.*
130. Narasimhalu, A. D., Dayasindhu, N. & Subramanian, R., 2004. *INFOSeMM: Infosys IT Security Maturity Model: A Report,* Singapore: Singapore Management University.
131. Ohmae, K., 1999. *The Borderless World, rev ed.* New York: HarperBusiness.
132. Oju, O., 2009. Impact Assessment of Corporate Culture on Employee Job Performance. *Business Intelligence Journal,* 2. kötet, pp. 388-397.
133. Oju, O., 2010. Organisational Culture and Corporate Performance: Empirical Evidence from Nigeria. *Journal of Business Systems, Governance and Ethics,* 5(2), pp. 88-100.
134. OnX Enterprise Solutions, 2011. *The Federated Cloud Maturity Model©: Charting the Path to Cloud Computing,* hely nélk.: ismeretlen szerző

135. Örtenblad, A., Putnam, L. L. & Trehan, K., 2016. Beyond Morgan's eight metaphors: Adding to and developing organization theory. *Human relations,* p. 875–889.
136. Pató, G., 2006. *ompetenciák, feladatok logisztikai rendszerekben. Doktori értekezés..* Veszprém: Pannon Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola.
137. Pekgünk, P., M. Griffin, P. & Keskinocak, P., 2016. Centralized vs. Decentralized competition for Price and Lead-Time Sensiive Demand. *Decision Science.*
138. Peters, T. & Waterman, R., 1990. *A siker nyomában.* Budapest: Közgazdasági és Jogi Kiadó.
139. Pettigrew, A. M., 1979. *Administrative Science Quarterly ,* December, 24(4), pp. 570-581.
140. Phelps, T., 2008. SUNY Information Security Initiative - A model to Map Our Information Security.
141. Pinto, J., 2016. 'Wow! That's so cool!': The Icehotel as organizational trope. *Human Relations,* p. 891–914.
142. Pisoni, A. & Onetti, A., 2018. When startups exit: comparing strategies in Europe and the USA. *Journal of Business Strategy,* pp. 26-33.
143. Plutchik, R., 1983. *Foundations of Experimental Research.* New York: Harper & Row.
144. Plutchik, R., 1991. *The Emotions.* Lanham: University Press of America.
145. Puthal, D., Sahoo, B. P. S., Mishra, S. & Swain, S., 2015. *Cloud Computing Features, Issues and Challenges: A Big Picture.* India, IEEE.
146. Quinn, R. E., 1988. Beyond Rational Management, Jossey. In: San Francisco: Bass Publishers.
147. Quinn, R. E., Bright , D., Faerman, S. R. & Thompson , M. P., 2015. *Becoming a Master Manager: A Competing Values Approach.* New Jersey: WILEY.
148. Quinn, R., 1996. *Deep Change: Discovering the Leader Within.* hely nélk.:Jossey-Bass.
149. Ransbotham, S., Mitra, S. & Ramsey, J., 2012. Are markets for vulnerabilities effective?. *MIS Quarterly,* pp. 43-64.
150. Rittinghouse, J. W. & Ransome, J. F., 2009. *Cloud Computing - Implementation, Management and Security.* Boca RAton: CRC Press.
151. Roberts, N. & Varun , G., 2014. Leveraging Information Technology Infrastructure to Facilitate a Firm's Customer Agility and Competitive Activity: An Empirical Investigation. *Journal of Management Information Systems,* pp. 231-270.
152. Sajtos, L. & Mitev, A., 2007. *SPSS kutatási és adatelemzési kézikönyv,* Budapest: Alinea Kiadó.
153. Saleh, D. M. F., 2011. Information Security Model. *International Journal of Computer Science and Security (IJCSS).*
154. Saleh, M. F., 2011. Information Security Maturity Model. *International Journal of Computer Science and Security (IJCSS).*
155. Sántha, K., 2015. *Trianguláció a pedagógiai kutatásban.* Budapest: Eötvös József Könyvkiadó.
156. Sántha, K., 2017. *A trianguláció-tipológiák és a MAXQDA kapcsolata a kvalitatív vizsgálatban.* Budapest: Vezetéstudomány.

157. Schabracq, M., 2007. *Changing organizational culture: the change agent's guidebook.* Hoboken: Wiley.
158. Schein, E. H., 1992. *Organizational culture and leadership.* San Francisco: Jossey-Bass Publishers.
159. Scholtz , T., Byrnes , F. C. & Wheatman, J., 2016. *ITScore for Information Security,* Stamford: Gartner.
160. Shan, T., 2010. *Cloud Computing Maturity Model (CM)2.* [Online] Available at: http://tonyshan.sys-con.com/node/1469466
161. Shaul , O., Vakola, M. & Armenakis, A., 2011. Change Recipients' Reactions to Organisational Change: A 60-Year Review of Quantitative Studies. *The Journal of Applied Behavioral Science,* pp. 461-524.
162. Sjelin, N. & White, G., 2016. The Community Cyber Security Maturity Model. *Cyber-Physical Security,* pp. 161-183.
163. Spencer, L. M. & Spencer, S. M., 1993. *Competence at work: Models for superior performance.* New York: John Wiley & Sons.
164. Spilák, V. & Kosztyán, Z. T., 2010. *Információbiztonság, mint a versenyképesség záloga.* Veszprém, ismeretlen szerző
165. Spilák, V. & Kosztyán, Z. T., 2013. *A szervezeti kultúra és vezetési stílusok hatása az információbiztonsági kiválóságra.* Győr, Neumann János Számítógép-tudományi Társaság.
166. Spilák, V., 2008. *Az információbiztonság, mint a modern társadalom kihívása.* Győr, GIKOF.
167. Subramanian, J., 2011. *Cloud Computing Maturity Model.* [Online] Available at: http://blog.netmagicsolutions.com/cloud-computing-maturity-model-ccmm-2/
168. Sultan, N., 2010. Cloud computing for education: A new dawn. *International Journal of Information Management,* 30(2), pp. 109-116.
169. Sürücü, L. & Yesilada, T., 2017. The Impact of Leadership Styles on Organizational Culture. *International Journal of Business and Management Invention,* pp. 31-39.
170. Szabó, L. & Dancsecz, G., 2009. A nemzetközi sportrendezvény-szervezési projektek sikerténye zői és a siker megítélésenk kritériumai. *Vezetéstudomány,* pp. 30-31.
171. Szádecky, T., 2016. Risk management of new technologies. *Academic and Applied Research in Military and Public Management Science,* pp. 279-290.
172. Szintay, I., 2003. *Vezetéstudomány.* Miskolc: Bíbor Kiadó.
173. Szokolszky, Á., 2004. *Kutatómunka a pszichológiában.* Budapest: Osiris Kiadó.
174. Tashakkori, A. M. & Teddlie , C. B., 2002. *Handbook of Mixed Methods in Social & Behavioral Research.* Thousand Oaks: SAGE Publications.
175. Taylor, F. W., 1983. *A tudományos vezetés alapjai.* Budapest: Közgazdasági és Jogi Könyvkiadó.
176. The Open Group, 2011. *Open Information Security Management Maturity Model (O-ISM3).* Zaltbommel: Van Haren Publishing.

177. Tolbert, P. S. & Hall, R. H., 2008. *Organizations: Structures, Processes and Outcomes.* London: Routledge.
178. Török, G., 2012. *Vezetői funkciók és szerepek hagyományos és virtuális környezetben.* Gödöllő: Szent István Egyetem.
179. Török, J., 2017. Kultúra összehasonlító (cross-cultural) és interkulturális (intercultural) kutatási modellek: összehasonlító elemzés. *Szakmai Füzetek Budapesti Gazdasági Főiskola,* pp. 11-16.
180. Trompenaars, F. & Hampden-Turner, C., 1998. *Riding the Waves of Culture.* London: Nicholas Brealey .
181. Turulja, L. & Bajgoric, N., 2016. Innovation and inforamtion technology capability as antecedents of firms' success. *Interdisciplinary Description of Complex Systems,* Issue 14, pp. 148-156.
182. Urquhart, J., 2008. *A maturity model for cloud computing.* [Online] Available at: http://news.cnet.com/8301-19413_3-10122295-240.html?part=rss&tag=feed&subj=TheWisdomofClouds
183. Vasvári, G., 2008. *AZ IT VIRTUALIZÁCIÓ,* hely nélk.: ismeretlen szerző
184. Vidyaraman, S., Chandrasekaran, M. & Upadhyay, S., 2008. Position: the user is the enemy. *ACM: New Hampshire.,* pp. 75-80.
185. Weber, M., 1947. The theory of social and economic reform. *Free Press.*
186. Weinman , J., 2016. Hybrid Cloud Economics. *IEEE Cloud Computing ,* pp. 18-22.
187. Weinman, J., 2015. The Strategic Value of the Cloud. *IEEE Cloud Computing,* pp. 66-70.
188. Weiss, D., Repschlaeger, J., Zarnekow, R. & Schroedl, H., 2013. *Towards a Consumer Cloud Computing Maturity Model - Proposition of Development Guidelines, Maturity Domains and Maturity Levels.* Jeju Island, PACIS.
189. Wienman, J., 2012. *Cloudonomics.* Hoboken: Wiley.
190. Yang , C., Yi, W., Saggi, N. & Jose, B.-A., 2015. IT capabilities and product innovation performance: The roles of corporate entrepreneurship and competitive intensity. *Information & Management,* pp. 643-657.
191. Zaleznik, A., 1992. Managers and Leaders: Are They Different?. *Harvard Business Review.*
192. Zhao, H., Liu, X. & Li, X., 2014. Towards efficient and fair resource trading in community-based cloud computing. *Journal of Parallel and Distributed Computing,* pp. 3087-3097.

9 Mellékletek jegyzéke

1. melléklet: Kvantitatív kutatás során használt kérdőív

„SZVIF" KÉRDŐÍV

A kutatás a szervezeti kultúra, vezetői szerepek, az információbiztonsági kiválóság, valamint a felhő alapú megoldások alkalmazásának kapcsolati térkép feltárását tűzte ki célul

A szervezetünk mindennapi működésére jellemző, hogy…

A jellemzők meghatározásához minden csoportban osszon fel 100 pontot a négy állítás között aszerint, hogy melyik írja le legpontosabban az Ön elképzelését. Adhatja mind a 100 pontot egy jellemzőnek, de fel is oszthatja (pl. A 60 pont; B 25 pont; C 5 pont; D 10 pont).

A szervezetet jellemző domináns karakterisztikák	**Jelenlegi**	**Kívánatos**
A…olyan, mint egy kiterjedt család, az emberek jól ismerik egymást.		
B…dinamikus, vállalkozó szellemű hely, az emberek hajlandók kockáztatni.		
C…eredményorientált, az emberek teljesítmény orientáltak és versenyző szelleműek.		
D…szabályozott és strukturált, az emberek cselekedeteit formális előírások szabályozzák.		
Összesen	**100**	**100**

A szervezeti irányítás jellemzői	**Jelenlegi**	**Kívánatos**
A…az irányítás támogatja a dolgozók fejlődését és gondoskodik róluk.		
B…az irányítás támogatja a dolgozók vállalkozó kedvét, innovációs tevékenységét és kockázatvállalását.		
C…az irányítás értékeli a rámenős, eredményorientált hozzáállást.		
D…az irányítás támogatja az egyenletes, szabályozott működést.		
Összesen	**100**	**100**

A vezetési stílus jellemzői	**Jelenlegi**	**Kívánatos**
A…a vezetési stílust az aktív részvétel, a csapatmunka és az egyetértésre törekvés jellemzi		
B…a vezetési stílust a szabadságra és az egyéni felelősségvállalásra törekvés jellemzi.		
C…a vezetési stílust a versenyszellem ösztönzése, a magas elvárások jellemzik.		
D…a vezetési stílust a kiszámíthatóság, a kapcsolatok stabilitása jellemzi.		
Összesen	**100**	**100**

A szervezetet összetartó erő	Jelenlegi	Kívánatos
A…a szervezet összetartó erejét a kölcsönös bizalom, a szervezet iránti fokozott elkötelezettség jelenti		
B…a szervezet összetartó ereje a fejlődés iránti elkötelezettség, az előremutatás és az élen járás.		
C…a szervezet összetartó ereje az eredményesség és a célok elérésének hangsúlyozása.		
D…a szervezet összetartói a formális szabályok, irányelvek és az egyenletes működés biztosítása.		
Összesen	**100**	**100**

A stratégiai hangsúlyok	Jelenlegi	Kívánatos
A…fontos a személyes fejlődés, a nyitottság és a nagyfokú bizalom.		
B…a szervezet új erőforrások megszerzését és új kihívások, célok hajszolását hangsúlyozza.		
C…a szervezet a versengést, a kihívó célok megvalósítását és a piacvezető pozíció elérését hangsúlyozza.		
D…fontos az állandóság, a stabilitás és a hatékony működés.		
Összesen	**100**	**100**

Siker kritériumok	Jelenlegi	Kívánatos
A…a siker alapja az emberi erőforrás fejlesztése, a csapatmunka, az elkötelezettség, az emberekkel való törődés.		
B…siker alapja a legegyedibb és legújabb termékek kifejlesztése, a termékvezető, innovátor szervezet.		
C…a siker alapja a piacvezető pozíció elérése, alapvető fontosságú a piaci versenyelőny.		
D…a siker a hatékonyságon alapul, melyhez megbízható teljesítés és költséghatékonyság társul.		
Összesen	**100**	**100**

Kérjük adja meg, hogy milyen gyakorisággal végzi vezetője a következő tevékenységeket (egyet karikázzon be). (1. Majdnem soha, 2. Nagyon ritkán, 3. Ritkán, 4. Időnként, 5. Gyakran, 6. Nagyon gyakran, 7. Majdnem mindig)

	Jelenlegi	Kívánatos
1. Találékony ötletei vannak	1 2 3 4 5 6 7	1 2 3 4 5 6 7
2. Biztosítja a napi tevékenységek állandóságát	1 2 3 4 5 6 7	1 2 3 4 5 6 7
3. Támogatja a szervezet fejlődését	1 2 3 4 5 6 7	1 2 3 4 5 6 7
4. Gondosan átnézi a részletes jelentéseket	1 2 3 4 5 6 7	1 2 3 4 5 6 7
5. Fenntartja a céltudatosságot a szervezetben	1 2 3 4 5 6 7	1 2 3 4 5 6 7
6. Segíti az egyetértést a szervezeten belül	1 2 3 4 5 6 7	1 2 3 4 5 6 7
7. Meghatározza a beosztottak felelősségi körét	1 2 3 4 5 6 7	1 2 3 4 5 6 7
8. Odafigyel a beosztottak személyes problémáira	1 2 3 4 5 6 7	1 2 3 4 5 6 7
9. Minimalizálja a munkafolyamatok fennakadását	1 2 3 4 5 6 7	1 2 3 4 5 6 7
10. Új koncepciókat és eljárásokat dolgoz ki	1 2 3 4 5 6 7	1 2 3 4 5 6 7
11. Ösztönzi a csoportos döntéshozatalt	1 2 3 4 5 6 7	1 2 3 4 5 6 7
12. Gondoskodik róla, hogy mindenki tudja, merre tart a szervezetet	1 2 3 4 5 6 7	1 2 3 4 5 6 7
13. Befolyásolja a magasabb szinten hozott döntéseket	1 2 3 4 5 6 7	1 2 3 4 5 6 7
14. Összehasonlítja a jelentéseket, hogy felfedezze az eltéréseket	1 2 3 4 5 6 7	1 2 3 4 5 6 7
15. Figyeli, ha az egység teljesíti a kitűzött célokat	1 2 3 4 5 6 7	1 2 3 4 5 6 7
16. Empatikus és segítő a beosztottak problémáiban	1 2 3 4 5 6 7	1 2 3 4 5 6 7
17. Technikai információk segítségével dolgozik	1 2 3 4 5 6 7	1 2 3 4 5 6 7
18. Vannak felsőbb szintű kapcsolatai	1 2 3 4 5 6 7	1 2 3 4 5 6 7
19. Egyértelmű célokat tűz ki	1 2 3 4 5 6 7	1 2 3 4 5 6 7
20. Érzékenyen és gondoskodó módon törődik az egyénekkel	1 2 3 4 5 6 7	1 2 3 4 5 6 7
21. Nyomon követi, hogy mi zajlik a szervezetben	1 2 3 4 5 6 7	1 2 3 4 5 6 7
22. A problémákat kreatívan, ügyesen kezeli	1 2 3 4 5 6 7	1 2 3 4 5 6 7
23. Segíti a szervezetet, hogy az elérje a céljait	1 2 3 4 5 6 7	1 2 3 4 5 6 7
24. Ösztönzi a dolgozókat, hogy ötleteiket megosszák a csoporttal	1 2 3 4 5 6 7	1 2 3 4 5 6 7
25. Keresi az innováció és a fejlesztések lehetőségeit	1 2 3 4 5 6 7	1 2 3 4 5 6 7
26. Tisztázza a prioritásokat és irányokat	1 2 3 4 5 6 7	1 2 3 4 5 6 7
27. Meggyőzően adja elő az új ötleteket a felsőbb vezetésnek	1 2 3 4 5 6 7	1 2 3 4 5 6 7
28. A rend érzetét teremti meg a szervezetben	1 2 3 4 5 6 7	1 2 3 4 5 6 7
29. Törődik a beosztottak igényeivel	1 2 3 4 5 6 7	1 2 3 4 5 6 7
30. Fontosnak tartja, hogy a szervezet elérje céljait	1 2 3 4 5 6 7	1 2 3 4 5 6 7

Szervezetünk IT működésére jellemző, hogy…

Kérjük jelölje meg, hogy a következő állítások közül melyik jellemzi leginkább a szervezet IT működését (1. Egyáltalán nem jellemző– 7. Leginkább jellemző).

	Jelenlegi	Kívánatos
1. Fizikai biztonság fejlettsége	1 2 3 4 5 6 7	1 2 3 4 5 6 7
2. Logikai biztonság fejlettsége	1 2 3 4 5 6 7	1 2 3 4 5 6 7
3. Humán biztonság fejlettsége	1 2 3 4 5 6 7	1 2 3 4 5 6 7
4. Külső fenyegetettségek felismerése	1 2 3 4 5 6 7	1 2 3 4 5 6 7
5. Belső fenyegetettsége felismerése	1 2 3 4 5 6 7	1 2 3 4 5 6 7
6. Tudatos kockázatelemzés	1 2 3 4 5 6 7	1 2 3 4 5 6 7
7. Belső felelőségek tisztázottak	1 2 3 4 5 6 7	1 2 3 4 5 6 7
8. Külső szolgáltatás/üzemeltetés esetén a felelőségek tisztázottak	1 2 3 4 5 6 7	1 2 3 4 5 6 7
9. Biztonsággal kapcsolatos területeket kontrolálják	1 2 3 4 5 6 7	1 2 3 4 5 6 7
10. Felismert fenyegetettségeket kezelik	1 2 3 4 5 6 7	1 2 3 4 5 6 7
11. Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	1 2 3 4 5 6 7	1 2 3 4 5 6 7

A szervezet virtualizációs technológiák alkalmazásával kapcsolatosan elmondható, hogy…

Kérjük jelölje meg, hogy a következő állítások közül melyik jellemzi leginkább a szervezet felhő alapú megoldások alkalmazását (1. Egyáltalán nem jellemző– 7. Leginkább jellemző).

	Jelenlegi	Kívánatos
1. Privát felhő szolgáltatásokat használ	1 2 3 4 5 6 7	1 2 3 4 5 6 7
2. Publikus felhő szolgáltatásokat használ	1 2 3 4 5 6 7	1 2 3 4 5 6 7
3. Külső üzemeltetés felel a felhő alapú megoldásokért	1 2 3 4 5 6 7	1 2 3 4 5 6 7
4. Belső üzemeltetés felel a felhő alapú megoldásokért	1 2 3 4 5 6 7	1 2 3 4 5 6 7
5. Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)	1 2 3 4 5 6 7	1 2 3 4 5 6 7
6. Platform szolgáltatást vesz igénybe/biztosít (PaaS)	1 2 3 4 5 6 7	1 2 3 4 5 6 7
7. Szofvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	1 2 3 4 5 6 7	1 2 3 4 5 6 7
8. Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak	1 2 3 4 5 6 7	1 2 3 4 5 6 7
9. Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak	1 2 3 4 5 6 7	1 2 3 4 5 6 7
10. Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem)	1 2 3 4 5 6 7	1 2 3 4 5 6 7

2. melléklet: Az esettanulmány során vizsgált minta

Nem	Kor	Munkaköri pozíció	Legmagasabb iskolai végzettség	Munkaköri kategória
Férfi	40	Application Operation Manager	Egyetem	Menedzser
Férfi	34	Infrastructure Operation and Development Manager	Egyetem	Menedzser
Férfi	38	Application Development Manager	Főiskola	Menedzser
Férfi	37	Service desk and Inventory Manager	Főiskola	Menedzser
Férfi	46	IT Strategy and Governance Manager	Egyetem	Menedzser
Férfi	38	IT Security Manager	Főiskola	Menedzser
Nő	39	Assistant	Egyetem	Aszisztens
Férfi	39	Team Leader Architect	Főiskola	Csoportvezető
Férfi	44	Program Manager Sales & Marketing	Főiskola	Csoportvezető
Nü	33	Program Manager B2B & CNO	Egyetem	Csoportvezető
Nő	34	Program Manager Mob/Fin/HR/IT	Egyetem	Csoportvezető
Férfi	41	Test Coordinator	Főiskola	Szakértő
Nő	28	Test Coordinator	Főiskola	Szakértő
Férfi	32	IT Business Analyst	Főiskola	Szakértő
Férfi	37	IT Solution Integrator	Főiskola	Szakértő
Férfi	29	IT Project Manager	Egyetem	Szakértő
Férfi	39	IT Business Analyst	Főiskola	Szakértő
Férfi	42	IT Business Analyst	Főiskola	Szakértő
Férfi	29	IT Business Analyst	Középiskola	Szakértő
Férfi	57	IT Solution Integrator	Középiskola	Szakértő
Férfi	31	IT Project Manager	Főiskola	Projektmenedzser
Férfi	35	IT Project Manager	Egyetem	Projektmenedzser
Férfi	32	IT Business Analyst	Egyetem	Szakértő
Nő	30	IT Business Analyst	Főiskola	Szakértő
Férfi	50	IT Business Analyst	Főiskola	Szakértő
Férfi	29	IT Solution Integrator	Egyetem	Szakértő
Férfi	36	IT Solution Architect	Középiskola	Szakértő
Férfi	39	IT Solution Architect	Főiskola	Szakértő
Férfi	30	IT Solution Architect	Főiskola	Szakértő
Férfi	39	Technical Leader Product	Középiskola	Csoportvezető
Nő	44	Team Leader Workflow	Főiskola	Csoportvezető
Férfi	47	Technical Leader In-house Development	Főiskola	Csoportvezető
Férfi	40	Team Leader Exernal Development	Főiskola	Csoportvezető
Férfi	39	Team Leader DWH	Egyetem	Csoportvezető
Férfi	38	Technical Leader Reporting	Főiskola	Csoportvezető
Férfi	37	IT Technical Delivery Project Manager	Főiskola	Projektmenedzser
Férfi	52	IT Application Expert	Középiskola	Szakértő
Férfi	40	IT Application Expert	Főiskola	Szakértő
Férfi	39	IT Application Expert	Középiskola	Szakértő

Nem	Kor	Munkaköri pozíció	Legmagasabb iskolai végzettség	Munkaköri kategória
Férfi	42	IT Application Expert	Középiskola	Szakértő
Nő	34	IT Application Expert	Főiskola	Szakértő
Férfi	38	IT Application Expert	Főiskola	Szakértő
Nő	44	IT Application Expert	Középiskola	Szakértő
Férfi	36	IT Application Expert	Középiskola	Szakértő
Férfi	33	IT Application Expert	Főiskola	Szakértő
Férfi	38	IT Application Expert	Főiskola	Szakértő
Férfi	35	Report Developer	Főiskola	Szakértő
Férfi	39	Report Developer	Főiskola	Szakértő
Férfi	34	Report Developer	Középiskola	Szakértő
Férfi	29	DWH Expert	Főiskola	Szakértő
Férfi	46	DWH Expert	Főiskola	Szakértő
Férfi	40	DWH Expert	Főiskola	Szakértő
Férfi	38	DWH Expert	Főiskola	Szakértő
Férfi	39	Technical Expert	Középiskola	Szakértő
Férfi	48	Technical Expert	Középiskola	Szakértő
Nő	35	Technical Expert	Egyetem	Szakértő
Nő	39	Product Expert	Főiskola	Szakértő
Férfi	30	Product Expert	Főiskola	Szakértő
Nő	42	Workflow Expert	Középiskola	Szakértő
Nő	46	Workflow Expert	Középiskola	Szakértő
Férfi	41	Workflow Expert	Főiskola	Szakértő
Férfi	48	Workflow Expert	Főiskola	Szakértő
Férfi	39	Service Desk & Inventory Team Leader	Főiskola	Csoportvezető
Férfi	46	IT Infrastructure Architect	Főiskola	Szakértő
Férfi	37	IT Infrastructure Portfolio Expert	Egyetem	Projektmenedzser
Nő	39	IT Infrastructure Project Manager	Egyetem	Projektmenedzser
Nő	24	Junior PM & Task Manager	Egyetem	Szakértő
Férfi	42	IT Infrastructure Expert	Középiskola	Szakértő
Férfi	32	IT Infrastructure Expert	Egyetem	Szakértő
Férfi	49	IT Infrastructure Expert	Középiskola	Szakértő
Férfi	43	IT Infrastructure Expert	Főiskola	Szakértő
Férfi	41	IT Infrastructure Expert	Főiskola	Szakértő
Férfi	35	IT Infrastructure Expert	Főiskola	Szakértő
Férfi	53	IT Infrastructure Expert	Középiskola	Szakértő
Férfi	38	IT Infrastructure Expert	Középiskola	Szakértő
Férfi	58	IT Infrastructure Expert	Főiskola	Szakértő
Férfi	39	IT Infrastructure Expert	Főiskola	Szakértő
Férfi	30	IT Service Desk Expert	Középiskola	Szakértő
Férfi	31	IT Service Desk Expert	Főiskola	Szakértő

Nem	Kor	Munkaköri pozíció	Legmagasabb iskolai végzettség	Munkaköri kategória
Nő	44	IT Service Desk Expert	Középiskola	Szakértő
Nő	27	IT Service Desk Expert	Főiskola	Szakértő
Nő	41	Process, SLA, OLA, QA Expert	Főiskola	Szakértő
Nő	43	Resource Analyst	Egyetem	Szakértő
Férfi	34	Procurement & Financial Expert	Egyetem	Szakértő
Férfi	38	IT Operations	Főiskola	Szakértő
Férfi	39	IT Operations	Középiskola	Szakértő
Férfi	42	IT Operations	Egyetem	Szakértő
Férfi	40	IT Operations	Főiskola	Szakértő
Férfi	45	IT Operations	Középiskola	Szakértő
Férfi	44	IT Operations	Főiskola	Szakértő
Férfi	42	IT Operations	Főiskola	Szakértő
Nő	39	IT Operations	Főiskola	Szakértő

3. melléklet: Információbiztonsági érettség Pearson-féle lineáris korreláció

		Fizikai biztonság fejlettsége	Logikai biztonság fejlettsége	Humán biztonság fejlettsége	Külső fenyegetettségek felismerése	Belső fenyegetettsége felismerése	Tudatos kockázatelemzés	Belső felelősségek tisztázottak	Külső szolgáltatás/üzemeltetés esetén a felelősségek	Felismert fenyegetettségeket	Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés
Fizikai biztonság fejlettsége	Pearson Korreláció	1	.631**	.668**	.194**	.185**	.417**	.154*	-.158*	.369**	.349**
Sig. (2-tailed)		.000	.000	.004	.006	.000	.023	.019	.000	.000	
N	219	219	219	219	219	219	219	219	219	219	
Logikai biztonság fejlettsége	Pearson Korreláció	.631**	1	.868**	.102	.137*	.317**	.189**	-.060	.256**	.296**
Sig. (2-tailed)	.000		.000	.132	.042	.000	.005	.375	.000	.000	
N	219	219	219	219	219	219	219	219	219	219	
Humán biztonság fejlettsége	Pearson Korreláció	.668**	.868**	1	.131	.138*	.466**	.227**	-.067	.315**	.318**
Sig. (2-tailed)	.000	.000		.052	.042	.000	.001	.321	.000	.000	
N	219	219	219	219	219	219	219	219	219	219	
Külső fenyegetettségek felismerése	Pearson Korreláció	.194**	.102	.131	1	.042	.151*	-.067	-.140*	.091	.013
Sig. (2-tailed)	.004	.132	.052		.538	.026	.325	.038	.178	.849	
N	219	219	219	219	219	219	219	219	219	219	
Belső fenyegetettsége felismerése	Pearson Korreláció	.185**	.137*	.138*	.042	1	.158*	-.069	-.024	.105	.092
Sig. (2-tailed)	.006	.042	.042	.538		.019	.308	.725	.122	.174	
N	219	219	219	219	219	219	219	219	219	219	

	Fizikai biztonság fejlettsége	Logikai biztonság fejlettsége	Humán biztonság fejlettsége	Külső fenyegetettségek felismerése	Belső fenyegetettsége felismerése	Tudatos kockázatelemzés	Belső felelősségek tisztázottak	Külső szolgáltatás/üzemeltetés esetén a felelősségek	Felismert fenyegetettségeket	Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	
Tudatos kockázatelemzés	Pearson Korreláció	.417**	.317**	.466**	.151*	.158*	1	.078	-.124	.475**	.333**
Sig. (2-tailed)	.000	.000	.000	.026	.019		.249	.067	.000	.000	
N	219	219	219	219	219	219	219	219	219	219	
Belső felelősségek tisztázottak	Pearson Korreláció	.154*	.189**	.227**	-.067	-.069	.078	1	.025	.156*	.126
Sig. (2-tailed)	.023	.005	.001	.325	.308	.249		.708	.021	.064	
N	219	219	219	219	219	219	219	219	219	219	
Külső szolgáltatás/üzemeltetés esetén a felelősségek tisztázottak	Pearson Korreláció	-.158*	-.060	-.067	-.140*	-.024	-.124	.025	1	-.089	-.144*
Sig. (2-tailed)	.019	.375	.321	.038	.725	.067	.708		.192	.033	
N	219	219	219	219	219	219	219	219	219	219	
Felismert fenyegetettségeket kezelik	Pearson Korreláció	.369**	.256**	.315**	.091	.105	.475**	.156*	-.089	1	.299**
Sig. (2-tailed)	.000	.000	.000	.178	.122	.000	.021	.192		.000	
N	219	219	219	219	219	219	219	219	219	219	
Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	Pearson Korreláció	.349**	.296**	.318**	.013	.092	.333**	.126	-.144*	.299**	1
Sig. (2-tailed)	.000	.000	.000	.849	.174	.000	.064	.033	.000		
N	219	219	219	219	219	219	219	219	219	219	

4. melléklet: Információbiztonsági kiválóság Anti-image mátrix

Anti-image korreláció	Fizikai biztonság fejlettsége	Logikai biztonság fejlettsége	Humán biztonság fejlettsége	Külső fenyegetettségek felismerése	Belső fenyegetettsége felismerése	Tudatos kockázatelemzés	Belső felelősségek tisztázottak	Külső szolgáltatás/üzemeltetés esetén a felelősségek tisztázottak	Biztonsággal kapcsolatos területeket kontrolálják	Felismert fenyegetettségeket kezelik	Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés
Fizikai biztonság fejlettsége	.915[a]	-.163	-.198	-.111	-.101	-.020	.007	.090	-.149	-.128	-.118
Logikai biztonság fejlettsége	-.163	.701[a]	-.780	.021	-.035	.199	.023	.001	.048	-.016	-.061
Humán biztonság fejlettsége	-.198	-.780	.717[a]	-.016	.020	-.283	-.111	-.051	-.108	.042	.010
Külső fenyegetettségek felismerése	-.111	.021	-.016	.754[a]	.006	-.037	.103	.101	-.094	9.267E-5	.083
Belső fenyegetettsége felismerése	-.101	-.035	.020	.006	.818[a]	-.080	.101	-.015	.018	-.017	-.015
Tudatos kockázatelemzés	-.020	.199	-.283	-.037	-.080	.783[a]	.103	.018	-.293	-.288	-.136
Belső felelősségek tisztázottak	.007	.023	-.111	.103	.101	.103	.733[a]	-.050	-.138	-.090	-.047
Külső szolgáltatás/üzemeltetés esetén a felelősségek tisztázottak	.090	.001	-.051	.101	-.015	.018	-.050	.750[a]	.093	-.010	.097
Biztonsággal kapcsolatos területeket kontrolálják	-.149	.048	-.108	-.094	.018	-.293	-.138	.093	.872[a]	-.117	-.027
Felismert fenyegetettségeket kezelik	-.128	-.016	.042	9.267 E-5	-.017	-.288	-.090	-.010	-.117	.858[a]	-.112
Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	-.118	-.061	.010	.083	-.015	-.136	-.047	.097	-.027	-.112	.903[a]

5. melléklet: Információbiztonsági kiválóság faktorelemzés eredményei

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.793
Bartlett's Test of Sphericity	Approx. Chi-Square	766.250
	df	55
	Sig.	.000

Communalities

	Initial	Extraction
Fizikai biztonság fejlettsége	1.000	.696
Logikai biztonság fejlettsége	1.000	.870
Humán biztonság fejlettsége	1.000	.887
Külső fenyegetettségek felismerése	1.000	.632
Belső fenyegetettsége felismerése	1.000	.735
Tudatos kockázatelemzés	1.000	.631
Belső felelőségek tisztázottak	1.000	.592

Külső szolgáltatás/üzemeltetés esetén a felelőségek tisztázottak	1.000	.482
Biztonsággal kapcsolatos területeket kontrolálják	1.000	.571
Felismert fenyegetettségeket kezelik	1.000	.597
Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	1.000	.400

Extraction Method: Principal Component Analysis.

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.775	34.320	34.320	3.775	34.320	34.320	2.520	22.910	22.910
2	1.223	11.115	45.435	1.223	11.115	45.435	2.274	20.669	43.579
3	1.085	9.864	55.299	1.085	9.864	55.299	1.213	11.026	54.605
4	1.010	9.184	64.483	1.010	9.184	64.483	1.087	9.878	64.483
5	.904	8.214	72.697						
6	.795	7.225	79.922						

7	.697	6.333	86.255						
8	.584	5.307	91.563						
9	.448	4.077	95.640						
10	.366	3.324	98.964						
11	.114	1.036	100.000						

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component			
	1	2	3	4
Fizikai biztonság fejlettsége	.803	.034	.205	-.091
Logikai biztonság fejlettsége	.770	.319	.383	-.172
Humán biztonság fejlettsége	.844	.268	.287	-.144
Külső fenyegetettségek felismerése	.238	-.549	.210	-.480
Belső fenyegetettsége felismerése	.234	-.237	.465	.638
Tudatos kockázatelemzés	.691	-.231	-.223	.224
Belső felelőségek tisztázottak	.281	.548	-.423	-.182

	Component			
	1	2	3	4
Külső szolgáltatás/üzemeltetés esetén a felelőségek tisztázottak	-.214	.545	.193	.319
Biztonsággal kapcsolatos területeket kontrolálják	.698	-.140	-.250	-.038
Felismert fenyegetettségeket kezelik	.587	-.138	-.396	.277
Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	.529	-.022	-.262	.226

Extraction Method: Principal Component Analysis.

a. 4 components extracted.

Rotated Component Matrix[a]

	Component			
	1	2	3	4
Fizikai biztonság fejlettsége	.726	.372	.168	.061
Logikai biztonság fejlettsége	.920	.153	-.004	-.013
Humán biztonság fejlettsége	.898	.280	.028	-.031
Külső fenyegetettségek felismerése	.198	-.050	.763	.091
Belső fenyegetettsége felismerése	.165	.201	-.156	.802
Tudatos kockázatelemzés	.244	.732	.150	.115
Belső felelőségek tisztázottak	.232	.243	-.277	-.634
Külső szolgáltatás/üzemeltetés esetén a felelőségek tisztázottak	.068	-.235	-.647	.061
Biztonsággal kapcsolatos területeket kontrolálják	.335	.624	.240	-.109

	Component			
	1	2	3	4
Felismert fenyegetettségeket kezelik	.099	.766	.024	-.006
Biztonsági eseményekkel kapcsolatban megtörténik a számonkérés	.184	.604	-.041	-.008

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

6. melléklet: Információbiztonsági kiválóság érettségi szint meghatározása

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
1,02805	4	-0,57644	2	-0,37965	2	0,10509	3	3
1,22656	4	-0,77154	1	-0,3321	2	-0,45699	2	2
-0,73659	2	-0,19795	2	0,59089	3	-2,28316	1	2
-1,30599	1	-1,13614	1	1,05435	4	-0,80131	1	1
-2,08154	1	0,3419	3	-0,19146	2	1,00306	4	2
-0,40161	2	-1,79997	1	-0,41415	2	-0,46252	2	2
-0,45812	2	0,00723	3	0,95243	4	-2,17955	1	2
-0,78807	1	1,16535	4	-0,18488	2	0,16207	3	2
-0,41487	2	-0,72439	1	-0,29973	2	1,81068	4	2
-0,51607	2	0,63845	3	0,04682	3	1,92516	4	3
-0,27842	2	0,16666	3	-0,96132	1	0,83996	4	2
-0,65927	2	-0,3228	2	-0,0651	2	0,75108	4	2
-0,99959	1	-1,21616	1	-0,82219	1	1,31235	4	1
-0,5502	2	-1,3353	1	-0,77307	1	0,47217	3	2
-1,10026	1	1,05552	4	-0,76819	1	-0,67427	1	1
-0,97389	1	0,28274	3	-2,29001	1	0,34292	3	2
0,16424	3	-1,61254	1	0,8308	4	0,74776	4	3
-0,63808	2	-0,31073	2	-0,50478	2	0,07765	3	2
-0,68898	2	-0,06877	3	-0,48932	2	-1,83143	1	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
-1,3436	1	-1,42451	1	-0,05165	2	-0,46566	2	1
-0,5893	2	-0,49265	2	-0,574	2	-1,70255	1	2
0,70349	3	-1,77994	1	-1,22358	1	-1,49748	1	1
-0,5398	2	-0,38378	2	-2,5752	1	-0,81841	1	1
-0,72813	2	0,24324	3	-1,3512	1	-1,87267	1	2
-1,18438	1	0,22314	3	-0,96676	1	-1,01455	1	1
-0,54434	2	-0,44277	2	-1,38106	1	-0,52523	2	2
2,58656	4	-2,16952	1	-1,73794	1	0,41374	3	2
1,19489	4	-0,56194	2	-2,29686	1	1,23006	4	2
-0,85944	1	0,42507	3	-1,1387	1	0,41156	3	2
-0,96023	1	0,13588	3	-1,3514	1	0,01614	2	2
-0,63486	2	-0,92717	1	0,16361	3	-0,45671	2	2
-0,23816	2	-0,36286	2	0,62033	3	-0,13614	2	2
-0,41229	2	-0,00964	3	-1,66871	1	-1,17698	1	2
0,37274	3	-1,52881	1	0,57676	3	-1,839	1	2
-1,91702	1	1,42247	4	-0,08796	2	-0,8671	1	2
-0,56541	2	0,38821	3	-0,192	2	-1,11822	1	2
-1,07427	1	-1,23004	1	0,81987	4	-2,07064	1	1
-1,40096	1	0,16739	3	-1,30828	1	-0,89997	1	1
-0,99589	1	0,21194	3	0,21284	3	-0,49176	2	2
-1,66199	1	-0,54225	2	0,00295	3	-0,49861	2	2
-0,54743	2	-0,13839	2	0,7896	4	0,8529	4	3
-0,4062	2	-0,4397	2	0,47993	3	1,1342	4	3
-0,8636	1	-0,79381	1	0,73914	4	0,39817	3	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
-1,25496	1	0,13721	3	1,34864	4	0,37806	3	2
1,20559	4	-1,69977	1	0,15712	3	0,03309	2	2
0,03821	3	-0,83546	1	-0,02307	2	0,3383	3	2
0,85256	4	-1,26524	1	0,85303	4	0,11237	3	3
-1,08275	1	-0,02215	3	1,92312	4	0,00117	2	2
-1,46238	1	-0,13456	2	-0,03648	2	0,38426	3	2
-0,43577	2	-0,33871	2	-1,00669	1	0,12247	3	2
-0,74167	2	-0,68706	2	-0,86663	1	-1,62297	1	1
-0,3986	2	-0,18689	2	0,23268	3	1,53185	4	3
1,05945	4	-1,77246	1	-0,29616	2	0,98352	4	2
-0,76532	1	-0,42736	2	0,00267	3	-0,45889	2	2
-0,80587	1	-0,40097	2	-0,6441	2	0,78432	4	2
-1,72997	1	0,87234	4	1,14848	4	0,12659	3	3
-0,88806	1	-0,41021	2	1,39619	4	1,10758	4	2
0,65542	3	-0,59832	2	0,21113	3	-0,19647	2	2
0,87694	4	-0,91855	1	-2,35425	1	2,1612	4	2
0,39074	3	0,52437	3	0,5422	3	-0,29653	2	3
-0,00107	3	-0,30538	2	0,66084	3	-0,92429	1	2
-1,51926	1	-0,72002	1	1,35342	4	-0,07778	2	2
-0,31732	2	-0,66562	2	-0,75703	1	0,05151	2	2
0,12899	3	1,50856	4	1,2018	4	-1,04175	1	3
1,4682	4	0,1272	3	-0,38798	2	-1,17078	1	2
-0,71907	2	1,56193	4	0,50676	3	-1,24652	1	2
-0,10961	2	1,78985	4	-0,15707	2	-1,66383	1	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
0,25802	3	0,74063	4	0,57284	3	-0,29501	2	3
-0,92195	1	-1,21283	1	-0,17977	2	-0,52537	2	1
1,07885	4	0,38643	3	2,11069	4	0,18526	3	3
-1,79944	1	-0,68002	2	0,49011	3	-0,50735	2	2
1,27373	4	1,01587	4	1,44755	4	-1,32267	1	3
0,36592	3	1,11603	4	1,04721	4	0,21238	3	3
-0,6783	2	1,98511	4	0,56412	3	0,49292	3	3
-0,29819	2	0,55893	3	-0,33314	2	-0,37679	2	2
0,32305	3	1,05295	4	1,0185	4	-0,10153	2	3
1,55379	4	0,97926	4	0,81805	4	-1,21412	1	3
1,85838	4	1,39338	4	0,22374	3	-0,03243	2	3
2,10459	4	2,20075	4	-1,26145	1	0,75982	4	3
1,4666	4	1,97263	4	-0,27903	2	0,25331	3	3
1,32246	4	0,79255	4	-0,52603	2	-0,79241	1	2
0,02049	3	1,43294	4	-1,20414	1	-0,60087	2	2
0,75023	3	1,641	4	-0,5594	2	-1,33139	1	2
0,19964	3	0,84394	4	0,35143	3	0,11785	3	3
0,89071	4	1,53813	4	-0,76158	1	0,62869	3	3
-1,1115	1	-1,2265	1	0,67464	3	-1,13449	1	1
-1,56982	1	-0,90843	1	0,77449	4	-0,51269	2	2
1,26133	4	1,41298	4	1,92951	4	-0,88309	1	3
0,46061	3	2,44462	4	0,92241	4	-0,60782	1	3
0,76582	3	1,01765	4	2,48477	4	1,15891	4	4
-0,84594	1	-1,10151	1	1,33931	4	-0,58103	2	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
2,04529	4	0,27298	3	1,06418	4	0,88189	4	4
0,86015	4	1,38657	4	0,50931	3	0,74607	4	4
0,90496	4	1,26813	4	-1,11929	1	-0,19989	2	2
1,30349	4	0,99435	4	-0,0044	3	-0,40598	2	3
0,75422	3	0,98285	4	1,15386	4	-0,49546	2	3
0,06879	3	2,58018	4	1,13638	4	-0,34345	2	3
1,73212	4	0,891	4	0,81591	4	-0,97128	1	3
1,85811	4	0,04463	3	-0,81927	1	-0,01443	2	2
1,76225	4	0,47878	3	-0,00535	2	-0,63344	1	2
1,40506	4	1,38228	4	-1,51707	1	-0,94989	1	2
2,01877	4	-0,2915	2	-0,16129	2	-1,03336	1	2
1,26917	4	2,30918	4	-0,38005	2	-0,95305	1	2
1,0508	4	-0,03642	3	2,00955	4	-1,21528	1	3
1,13784	4	0,99493	4	-0,85387	1	-1,20171	1	2
1,29456	4	0,98233	4	-0,19465	2	0,0594	3	3
-1,19377	1	-1,01158	1	0,33637	3	-0,63388	1	1
1,79844	4	-0,30274	2	0,72675	3	-0,74333	1	2
0,9912	4	0,32314	3	-1,37576	1	-0,11606	2	2
2,39842	4	0,82497	4	-0,5711	2	-1,69439	1	2
0,80528	4	-0,11345	3	1,20969	4	-0,30981	2	3
-0,45358	2	2,52644	4	-1,70317	1	-0,73941	1	2
-0,14842	2	1,11557	4	0,26552	3	0,11384	3	3
1,37482	4	-0,36953	2	-0,01593	2	-0,04301	2	2
1,72005	4	-0,20869	2	0,23724	3	-0,00496	2	3

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
-1,49262	1	-1,00385	1	0,50942	3	-0,11974	2	2
-1,68874	1	0,90938	4	0,14986	3	0,84041	4	3
0,22349	3	-0,24235	2	0,87245	4	0,90995	4	3
0,03314	3	-0,45658	2	0,59334	3	1,21157	4	3
-0,64393	2	-0,80225	1	0,79585	4	0,43685	3	2
-0,81562	1	0,12034	3	1,46204	4	0,45543	3	2
1,97651	4	-1,80373	1	0,23997	3	0,09013	3	2
1,02881	4	-0,94786	1	0,11648	3	0,43403	3	2
1,07223	4	-1,27368	1	0,90973	4	0,15105	3	3
-0,64341	2	-0,03903	3	2,03653	4	0,07854	3	3
1,26011	4	-0,9435	1	-0,16361	2	0,38139	3	2
0,00357	3	-0,35558	2	-0,89329	1	0,19984	3	2
1,00504	4	-1,1435	1	-0,88877	1	-1,59589	1	1
0,9141	4	-0,43199	2	0,33502	3	1,62276	4	3
1,27912	4	-1,7809	1	-0,23946	2	1,0222	4	2
1,08382	4	-1,00807	1	-0,11338	2	-0,47531	2	2
0,5015	3	-0,84053	1	-0,77964	1	0,73404	3	2
0,77285	3	0,07185	3	0,96465	4	0,08502	3	3
0,08772	3	-0,7627	1	1,2912	4	1,07762	4	3
1,52878	4	-0,82654	1	0,20006	3	-0,18293	2	2
2,29207	4	-1,28791	1	-2,34583	1	2,20861	4	2
2,11849	4	-0,02332	3	0,50674	3	-0,23843	2	3
1,19438	4	-0,66631	2	0,61256	3	-0,91556	1	2
0,88113	4	-1,39625	1	1,26351	4	-0,07584	2	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
0,7757	3	-0,90228	1	-0,7114	2	0,10374	3	2
-1,25473	1	0,69804	3	0,02539	3	0,77658	4	2
0,00382	3	-0,23391	2	0,81575	4	0,87126	4	3
-0,73778	2	-0,35262	2	0,51049	3	1,15453	4	3
-0,8636	1	-0,79381	1	0,73914	4	0,39817	3	2
-0,81562	1	0,12034	3	1,46204	4	0,45543	3	2
0,22981	3	-1,34728	1	0,2621	3	0,06305	3	2
0,47755	3	-0,85233	1	0,09033	3	0,41567	3	2
0,09645	3	-0,9212	1	1,01472	4	0,18101	3	2
-1,08275	1	-0,02215	3	1,92312	4	0,00117	2	2
-1,90172	1	-0,11769	3	-0,14989	2	0,30689	3	2
-0,43577	2	-0,33871	2	-1,00669	1	0,12247	3	2
0,13169	3	-0,91528	1	-0,8777	1	-1,60943	1	1
-1,05228	1	0,0329	3	0,30045	3	1,55699	4	2
0,30333	3	-1,42841	1	-0,13447	2	1,05217	4	2
-0,76532	1	-0,42736	2	0,00267	3	-0,45889	2	2
-1,02554	1	-0,39253	2	-0,7008	2	0,74564	3	2
-1,29596	1	0,661	3	1,02401	4	0,06275	3	2
-1,10774	1	-0,40178	2	1,33949	4	1,06889	4	2
-0,65194	2	-0,15875	2	0,34667	3	-0,14618	2	2
-0,10832	2	-0,61168	2	-2,25592	1	2,20667	4	2
-0,70643	2	0,90988	4	0,72778	3	-0,19205	2	3
-0,00107	3	-0,30538	2	0,66084	3	-0,92429	1	2
-0,6459	2	-0,94825	1	1,34236	4	-0,06424	2	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
-0,09765	3	-0,67405	2	-0,70033	2	0,0902	3	2
-0,92352	1	0,12853	3	-0,16968	2	0,16501	3	2
-0,08081	3	-0,33197	2	-0,19656	2	-0,4067	2	2
-0,95626	1	-0,18951	2	0,53419	3	-2,32185	1	2
-1,44582	1	0,56136	3	-0,57554	2	0,05694	3	2
-1,10576	1	-0,01058	3	-0,29645	2	0,9731	4	2
-0,40161	2	-1,79997	1	-0,41415	2	-0,46252	2	2
-0,7897	1	0,09432	3	0,98299	4	-2,15922	1	2
-1,00774	1	1,17379	4	-0,24158	2	0,12338	3	2
-0,1952	2	-0,73283	1	-0,24303	2	1,84936	4	2
-0,84765	1	0,72553	4	0,07738	3	1,94549	4	3
-0,05875	3	0,15822	3	-0,90462	1	0,87865	4	2
-0,87894	1	-0,31436	2	-0,1218	2	0,71239	3	2
-0,35538	2	-1,48156	1	-0,89662	1	1,30271	4	2
-0,5502	2	-1,3353	1	-0,77307	1	0,47217	3	2
-1,31993	1	1,06396	4	-0,82489	1	-0,71295	1	1
-0,6423	2	0,19566	3	-2,32057	1	0,3226	3	2
0,16424	3	-1,61254	1	0,8308	4	0,74776	4	3
-0,19874	2	-0,32761	2	-0,39138	2	0,15502	3	2
-0,46931	2	-0,07721	3	-0,43262	2	-1,79274	1	2
-0,62738	2	-0,69953	2	-1,00909	1	-0,27279	2	2
-0,5893	2	-0,49265	2	-0,574	2	-1,70255	1	2
0,38139	3	-1,64724	1	-1,18636	1	-1,49266	1	1
-0,5398	2	-0,38378	2	-2,5752	1	-0,81841	1	1

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
-0,9478	1	0,25167	3	-1,40791	1	-1,91136	1	1
-0,10083	3	-0,05914	3	-0,92779	1	-0,94681	1	2
-0,21276	2	-0,52986	2	-1,41162	1	-0,54555	2	2
-0,90856	1	1,9449	4	-1,41604	1	-0,40115	2	2
-0,08257	3	0,9912	4	1,30231	4	-1,37093	1	3
-0,09848	3	1,67944	4	-0,43736	2	-0,51911	2	3
-0,04048	3	1,94147	4	-1,1475	1	2,62939	4	3
0,58002	3	0,71609	3	-1,07313	1	1,36597	4	2
0,31281	3	1,62879	4	-0,66145	2	0,33255	3	3
0,50117	3	1,86057	4	-0,95484	1	1,26274	4	3
-0,24695	2	1,65382	4	-0,08401	2	0,98968	4	3
-0,65881	2	1,43169	4	-1,17045	1	2,03508	4	2
0,26865	3	0,51101	3	0,24806	3	0,27193	3	3
0,12681	3	0,18288	3	0,11578	3	-0,05076	2	3
-0,1915	2	1,03574	4	-0,1108	2	1,27787	4	3
-0,62756	2	1,93257	4	0,40221	3	1,89304	4	3
-0,70297	2	1,44263	4	-0,71534	1	0,35455	3	2
-1,03994	1	1,26171	4	-0,51766	2	1,27444	4	2
0,32438	3	0,2295	3	-0,98301	1	1,38638	4	2
-0,50754	2	0,33566	3	0,20704	3	0,87146	4	3
0,53426	3	-0,30347	2	-1,02268	1	-0,58604	2	2
0,80968	4	-0,31167	2	0,02387	3	-0,17818	2	3
0,67385	3	-0,12617	3	0,03025	3	-1,1271	1	2
1,41791	4	-0,60307	2	-0,68768	2	-0,4279	2	2

Inf. bizt. területek érettség factor	Inf. bizt. területek érettség	Inf. bizt. menedzsment érettség factor	Inf.bizt. menedzsment érettség érettség	Külső információbiztonságot befolyásoló tényezők factor	Külső inf. bizt.befolyásoló tényezők érettség	Belsői inf. bizt. befolyásoló tényezők factor	Belső inf. bizt. befolyásoló tényezők érettség	Geometriai átlag
-0,03348	3	0,27466	3	1,44793	4	0,86132	4	3
1,5141	4	-0,9364	1	1,8411	4	-0,5662	2	2
0,19766	3	0,5867	3	1,63177	4	2,20089	4	3
0,96042	4	-0,30567	2	1,74618	4	0,78994	4	3
1,05619	4	-1,02047	1	1,6665	4	1,81693	4	3
0,58625	3	0,68632	3	0,34428	3	1,46515	4	3
0,63991	3	-0,39006	2	1,80369	4	0,20658	3	3
0,74465	3	0,87213	4	1,23842	4	1,83761	4	4

7. melléklet: A felhő alapú megoldások alkalmazása Pearson-féle lineáris korreláció

		Privát felhő szolgáltatásokat használ	Publikus felhő szolgáltatásokat használ	Külső üzemeltetés felel a felhő alapú megoldásokért	Belső üzemeltetés felel a felhő alapú megoldásokért	Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)	Platform szolgáltatást vesz igénybe/biztosít (PaaS)	Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak	Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak	Adatok kihelyezhetősége meghatározott, azaz mely adatok helyezhetőek ki és melyek nem)
Privát felhő szolgáltatásokat használ	Pearson Korreláció	1	.223**	.118	.690**	.690**	.370**	-.028	-.119	.386**	-.077
	Sig. (2-tailed)		.001	.082	.000	.000	.000	.685	.080	.000	.255
	N	219	219	219	219	219	219	219	219	219	219
Publikus felhő szolgáltatásokat használ	Pearson Korreláció	.223**	1	.636**	.160*	.428**	.567**	.346**	.177**	-.128	.377**
	Sig. (2-tailed)	.001		.000	.018	.000	.000	.000	.009	.058	.000
	N	219	219	219	219	219	219	219	219	219	219
Külső üzemeltetés felel a felhő alapú megoldásokért	Pearson Korreláció	.118	.636**	1	-.052	.264**	.448**	.420**	.196**	-.130	.281**
	Sig. (2-tailed)	.082	.000		.447	.000	.000	.000	.004	.054	.000
	N	219	219	219	219	219	219	219	219	219	219
Belső üzemeltetés felel a felhő alapú megoldásokért	Pearson Korreláció	.690**	.160*	-.052	1	.529**	.306**	.004	-.101	.389**	-.098
	Sig. (2-tailed)	.000	.018	.447		.000	.000	.959	.137	.000	.149
	N	219	219	219	219	219	219	219	219	219	219
Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)	Pearson Korreláció	.690**	.428**	.264**	.529**	1	.438**	.055	-.107	.302**	.061
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.417	.116	.000	.367
	N	219	219	219	219	219	219	219	219	219	219

		Privát felhő szolgáltatásokat használ	Publikus felhő szolgáltatásokat használ	Külső üzemeltetés felel a felhő alapú megoldásokért	Belső üzemeltetés felel a felhő alapú megoldásokért	Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)	Platform szolgáltatást vesz igénybe/biztosít (PaaS)	Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak	Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak	Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem)
Platform szolgáltatást vesz igénybe/biztosít (PaaS)	Pearson Korreláció	.370**	.567**	.448**	.306**	.438**	1	.420**	.082	-.024	.210**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.228	.722	.002
	N	219	219	219	219	219	219	219	219	219	219
Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	Pearson Korreláció	-.028	.346**	.420**	.004	.055	.420**	1	.204**	-.093	.251**
	Sig. (2-tailed)	.685	.000	.000	.959	.417	.000		.002	.169	.000
	N	219	219	219	219	219	219	219	219	219	219
Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak	Pearson Korreláció	-.119	.177**	.196**	-.101	-.107	.082	.204**	1	-.080	.309**
	Sig. (2-tailed)	.080	.009	.004	.137	.116	.228	.002		.237	.000
	N	219	219	219	219	219	219	219	219	219	219
Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak	Pearson Korreláció	.386**	-.128	-.130	.389**	.302**	-.024	-.093	-.080	1	-.173*
	Sig. (2-tailed)	.000	.058	.054	.000	.000	.722	.169	.237		.010
	N	219	219	219	219	219	219	219	219	219	219
Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem)	Pearson Korreláció	-.077	.377**	.281**	-.098	.061	.210**	.251**	.309**	-.173*	1
	Sig. (2-tailed)	.255	.000	.000	.149	.367	.002	.000	.000	.010	
	N	219	219	219	219	219	219	219	219	219	219

8. melléklet: Felhő alapú megoldások alkalmazása Anti-image mátrix

Anti-image korreláció	Privát felhő szolgáltatásokat használ	Publikus felhő szolgáltatásokat használ	Külső üzemeltetés felel a felhő alapú megoldásokért	Belső üzemeltetés felel a felhő alapú megoldásokért	Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)	Platform szolgáltatást vesz igénybe/biztosít (PaaS)	Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak	Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak	Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem
Privát felhő szolgáltatásokat használ	.724a	.096	-.115	-.476	-.444	-.145	.129	.012	-.128	.059
Publikus felhő szolgáltatásokat használ	.096	.745a	-.453	-.115	-.262	-.261	.004	-.063	.159	-.225
Külső üzemeltetés felel a felhő alapú megoldásokért	-.115	-.453	.733a	.268	-.059	-.086	-.241	-.077	.009	.020
Belső üzemeltetés felel a felhő alapú megoldásokért	-.476	-.115	.268	.739a	-.080	-.110	-.074	-.010	-.173	.065
Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS)	-.444	-.262	-.059	-.080	.793a	-.105	.082	.137	-.164	-.053
Platform szolgáltatást vesz igénybe/biztosít (PaaS)	-.145	-.261	-.086	-.110	-.105	.836a	-.311	.010	.117	-.013
Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS)	.129	.004	-.241	-.074	.082	-.311	.748a	-.081	-.040	-.087
Szolgáltatókkal szemben támasztott biztonsági elvárások definiáltak	.012	-.063	-.077	-.010	.137	.010	-.081	.731a	-.053	-.236
Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak	-.128	.159	.009	-.173	-.164	.117	-.040	-.053	.796a	.065
Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem)	.059	-.225	.020	.065	-.053	-.013	-.087	-.236	.065	.785a

9. melléklet: Felhő alapú megoldások alkalmazásának érettségi szint meghatározása

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
0,75136	4	2,22713	4	4
1,18718	4	0,76717	4	4
3,60515	4	-0,53369	2	3
2,51471	4	-0,50243	2	3
1,80103	4	2,07717	4	4
3,07999	4	0,19594	3	3
0,32041	3	1,69962	4	3
0,75578	4	1,12656	4	4
1,40129	4	1,54532	4	4
-0,16905	2	0,36444	3	2
3,60515	4	-0,53369	2	3
0,14033	3	0,67371	3	3
-0,55936	2	0,35709	3	2
0,12282	3	1,58082	4	3
0,44331	3	0,49167	3	3
0,9809	4	0,908	4	4
0,52205	3	0,43755	3	3
1,46868	4	-0,15962	2	3
0,97998	4	1,57574	4	4
-0,03597	3	1,63965	4	3

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
0,64263	3	0,31468	3	3
2,05061	4	0,55979	3	3
-1,15272	1	0,34345	3	2
1,79375	4	0,58386	3	3
-0,71753	2	0,66705	3	2
0,45953	3	0,8413	4	3
-0,21871	2	0,97504	4	3
-1,14151	1	0,13049	3	2
-0,53766	2	1,45451	4	3
1,38731	4	0,16545	3	3
1,51788	4	0,79416	4	4
1,41508	4	0,16717	3	3
2,13919	4	-0,92115	1	2
1,79106	4	-0,67832	1	2
-0,73561	2	2,06879	4	3
0,2738	3	1,34269	4	3
0,06551	3	1,08095	4	3
0,83867	4	0,6806	3	3
-0,61259	2	0,86379	4	3
0,16549	3	1,35271	4	3
1,65982	4	0,06171	3	3

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
0,48509	3	1,30057	4	3
-0,92281	1	1,84249	4	2
-0,89481	1	1,53828	4	2
0,5186	3	-0,06057	3	3
1,03723	4	1,49131	4	4
-0,19823	2	1,62951	4	3
0,75058	4	1,79326	4	4
0,29019	3	2,05739	4	3
0,34868	3	1,43929	4	3
2,37348	4	-0,50603	2	3
0,75136	4	2,22713	4	4
1,31608	4	1,36126	4	4
2,29529	4	-0,31253	2	3
1,0847	4	1,17608	4	4
1,62885	4	0,66025	3	3
1,46908	4	1,5732	4	4
0,95346	4	0,61984	3	3
-1,22183	1	0,88463	4	2
0,38402	3	1,81326	4	3
0,11081	3	1,88686	4	3
0,6534	4	1,9498	4	4

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
-0,85449	1	-0,33239	2	1
-0,40085	2	-0,46436	2	2
1,63896	4	-1,10283	1	2
-0,56771	2	-1,11014	1	1
-0,49518	2	-0,05595	3	2
0,3179	3	-0,26428	2	2
-0,723	2	1,21301	4	3
-0,96765	1	-0,45602	2	1
-0,51425	2	-0,25046	2	2
0,94046	4	-1,48482	1	2
-0,95931	1	-0,49281	2	1
-0,64525	2	-0,43737	2	2
0,02411	3	-0,54128	2	2
-0,90332	1	0,90071	4	2
-1,14539	1	0,12791	3	2
-0,60623	2	0,42935	3	2
-0,65247	2	0,49726	3	2
-0,53994	2	0,04011	3	2
-0,84677	1	0,89121	4	2
-0,50516	2	0,35453	3	2
-1,03757	1	0,17824	3	2

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
0,00419	3	-0,8511	1	2
-0,77995	2	1,02795	4	3
-1,38593	1	0,12657	3	2
-1,21135	1	0,10587	3	2
-1,21135	1	0,10587	3	2
-0,32259	2	-1,13541	1	1
-0,40965	2	-0,30788	2	2
0,02747	3	0,38312	3	3
-1,13907	1	-0,99854	1	1
0,00311	3	1,77149	4	3
-0,78061	2	-0,27272	2	2
-1,03379	1	-1,18218	1	1
-1,34963	1	-0,63127	2	1
-1,46611	1	-0,23467	2	1
-0,24826	2	-1,17438	1	1
0,9574	4	-1,38582	1	2
-0,29128	2	-0,53296	2	2
0,09876	3	-1,19005	1	2
0,10091	3	-1,21579	1	2
-1,35279	1	-0,06804	3	2
-1,41908	1	0,32119	3	2

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
-0,32601	2	0,47599	3	2
0,10276	3	-0,16913	2	2
-0,35882	2	-0,52797	2	2
-0,63487	2	-0,15027	2	2
-0,93737	1	-0,47447	2	1
-0,11567	3	-1,25766	1	2
-1,35279	1	-0,06804	3	2
0,69402	4	-0,58627	2	3
-1,00147	1	-0,13518	3	2
-0,99137	1	0,13199	3	2
-0,59959	2	-1,10724	1	1
-0,28356	2	-0,95403	1	1
-0,92613	1	1,453	4	2
-0,78368	2	-0,05911	3	2
-0,37583	2	-0,62871	2	2
0,06605	3	-0,48539	2	2
1,19925	4	-1,62573	1	2
-0,11486	3	-1,35073	1	2
-0,23861	2	-1,55012	1	1
-1,03379	1	-1,18218	1	1
0,52024	3	-0,65865	1	2

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
-0,10465	3	-0,33101	2	2
0,80246	4	-1,33314	1	2
-0,50316	2	-0,39953	2	2
-1,03379	1	-1,18218	1	1
0,08313	3	-1,34964	1	2
-0,85706	1	-1,22862	1	1
-0,50358	2	-1,32149	1	1
-0,59668	2	-0,49118	2	2
-1,11492	1	-0,33496	2	1
0,28192	3	-1,44163	1	2
0,10814	3	-1,514	1	2
-0,02531	3	-0,60278	2	2
-0,50316	2	-0,39953	2	2
-0,07276	3	0,37471	3	3
-0,801	1	0,83589	4	2
-0,14269	2	1,00898	4	3
-1,27941	1	1,10146	4	2
-0,10687	3	-0,2656	2	2
1,03139	4	-0,40306	2	3
-1,34963	1	-0,63127	2	1
-1,17538	1	-0,2407	2	1

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
1,36395	4	-0,31463	2	3
-0,8648	1	0,78811	4	2
0,25712	3	0,08911	3	3
-0,97821	1	1,002	4	2
-0,0231	3	0,04246	3	3
-0,20101	2	1,0466	4	3
0,64976	4	0,44336	3	3
2,63952	4	-1,57717	1	2
-0,89948	1	0,21127	3	2
0,15963	3	1,8023	4	3
-1,31696	1	0,70078	3	2
0,8177	4	0,01402	3	3
-1,325	1	0,35052	3	2
0,78981	4	-0,48228	2	3
-1,2385	1	-0,41469	2	1
0,06585	3	0,70058	3	3
1,49026	4	-1,30817	1	2
-0,04052	3	-0,26221	2	2
-0,09368	3	-0,08409	3	3
-0,86394	1	-0,03983	3	2
0,85224	4	0,25899	3	3

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
0,81074	4	-0,91342	1	2
0,32041	3	1,69962	4	3
0,45905	3	0,2967	3	3
0,37947	3	0,18976	3	3
-1,06885	1	0,73419	4	2
-1,03379	1	-1,18218	1	1
-0,54269	2	-1,2745	1	1
1,9143	4	-1,22812	1	2
0,44751	3	-0,11988	3	3
0,78497	4	-1,39085	1	2
0,08385	3	-0,32064	2	2
-1,13907	1	-0,99854	1	1
1,58794	4	-0,59047	2	3
-0,25516	2	0,82526	4	3
-1,15535	1	1,4994	4	2
-1,3138	1	0,13756	3	2
-0,28945	2	-1,33003	1	1
-0,67775	2	-0,37883	2	2
-0,96765	1	-0,45602	2	1
0,75942	4	-1,38691	1	2
0,74511	4	-1,06724	1	2

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
-0,59959	2	-1,10724	1	1
-0,28356	2	-0,95403	1	1
-0,92613	1	1,453	4	2
-0,78368	2	-0,05911	3	2
-0,37583	2	-0,62871	2	2
0,06605	3	-0,48539	2	2
1,19925	4	-1,62573	1	2
-0,11486	3	-1,35073	1	2
-0,23861	2	-1,55012	1	1
-1,03379	1	-1,18218	1	1
0,52024	3	-0,65865	1	2
-0,10465	3	-0,33101	2	2
0,80246	4	-1,33314	1	2
-1,03379	1	-1,18218	1	1
-0,23861	2	-1,55012	1	1
-1,03379	1	-1,18218	1	1
0,52024	3	-0,65865	1	2
-0,10465	3	-0,33101	2	2
0,80246	4	-1,33314	1	2
-0,50316	2	-0,39953	2	2
-1,03379	1	-1,18218	1	1

Publikus felhő szolgáltatások	Publikus felhő szolgáltatások érettség	Privát felhő szolgáltatások	Privát felhő szolgáltatások érettség	Geometriai átlag
0,08313	3	-1,34964	1	2
-0,85706	1	-1,22862	1	1
-0,50358	2	-1,32149	1	1
-0,59668	2	-0,49118	2	2
-0,28356	2	-0,95403	1	1
-0,92613	1	1,453	4	2
-0,78368	2	-0,05911	3	2
-0,37583	2	-0,62871	2	2

10. melléklet: Felhő alapú megoldások alkalmazásának faktorelemzés eredményei

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.760
Bartlett's Test of Sphericity	Approx. Chi-Square	743.096
	df	36
	Sig.	.000

Communalities

	Initial	Extraction
Privát felhő szolgáltatásokat használ jelenlegi	1.000	.798
Publikus felhő szolgáltatásokat használ jelenlegi	1.000	.724
Külső üzemeltetés felel a felhő alapú megoldásokért jelenlegi	1.000	.635

	Initial	Extraction
Belső üzemeltetés felel a felhő alapú megoldásokért jelenlegi	1.000	.703
Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS) jelenlegi	1.000	.719
Platform szolgáltatást vesz igénybe/biztosít (PaaS) jelenlegi	1.000	.636
Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS) jelenlegi	1.000	.426
Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak jelenlegi	1.000	.463
Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem) jelenlegi	1.000	.357

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.184	35.374	35.374	3.184	35.374	35.374	2.744	30.488	30.488
2	2.277	25.296	60.670	2.277	25.296	60.670	2.716	30.183	60.670
3	.808	8.974	69.644						
4	.755	8.391	78.035						
5	.652	7.239	85.274						
6	.410	4.555	89.829						
7	.370	4.116	93.946						
8	.328	3.643	97.589						
9	.217	2.411	100.000						

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component 1	Component 2
Privát felhő szolgáltatásokat használ jelenlegi	.685	-.573
Publikus felhő szolgáltatásokat használ jelenlegi	.739	.421
Külső üzemeltetés felel a felhő alapú megoldásokért jelenlegi	.594	.531
Belső üzemeltetés felel a felhő alapú megoldásokért jelenlegi	.576	-.609
Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS) jelenlegi	.774	-.347
Platform szolgáltatást vesz igénybe/biztosít (PaaS) jelenlegi	.770	.207

	Component	
	1	2
Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS) jelenlegi	.415	.504
Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak jelenlegi	.203	-.650
Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem) jelenlegi	.281	.527

Extraction Method: Principal Component Analysis.

a. 2 components extracted.

Rotated Component Matrix[a]

	Component	
	1	2
Privát felhő szolgáltatásokat használ jelenlegi	.092	.889
Publikus felhő szolgáltatásokat használ jelenlegi	.824	.212
Külső üzemeltetés felel a felhő alapú megoldásokért jelenlegi	.796	.033
Belső üzemeltetés felel a felhő alapú megoldásokért jelenlegi	-.011	.838
Infrastruktúra szolgáltatást vesz igénybe/biztosít (IaaS) jelenlegi	.314	.787
Platform szolgáltatást vesz igénybe/biztosít (PaaS) jelenlegi	.697	.388

	Component	
	1	2
Szoftvert, mint szolgáltatás vesz igénybe/biztosít (SaaS) jelenlegi	.649	-.073
Belső felhő megoldásokkal szemben támasztott biztonsági elvárások definiáltak jelenlegi	-.307	.608
Adatok kihelyezhetősége meghatározott, azaz mely adatok helyzhetőek ki és melyek nem) jelenlegi	.569	-.183

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

11. melléklet: Esettanulmány során alkalmazott kérdések

- Milyen területekért felelt az átalakítás előtt és milyen területekért fog felelni az új struktúrában?
- Negatívan vagy pozitívan értinti önt az átalaktás?
- Hogyan látja, változott a szakértők hozzáállása az átalakítás során? Ön szerint milyen hatások érték őket?
- Milyen volt a kommunikáció és információ átadás a változást koordináló személyek részéről?
- Hogyan érintette az átalakítás a korábbi vezetői, beosztotti kapcsolatokat? Hogy hatott ez a mindennapi munkára?
- Milyen volt a vállalati környezet az átalakítási folyamat során? Jellemző volt esetleg bizyontalanság, tömeges elvándorlás?
- Mit gondol az átalakítási folyamatról? Hogyan ítéli meg az átalakítás előkészítettségét, az átalakításról szóló kommunikácók folyamatosságát? Milyen hiányosságok voltak ön szerint és hogy lehetett volna kiküszöbölni őket?
- Milyen új lehetőségeket, kihívásokat jelent az új szervezeti struktúra?
- Hogyan fognak változni a vezetői szerepek, a korábbi, csak lokális feladatkörök a Pan-Europai-vá történő átalakulás után? Milyen hatással lehet ez a Magyarországi működésre és ügyfelekre?
- Hogyan változott az átalakítás során a lokális IT működése és szervezeti kultúrája?
- Ön szerint melyek azok a tényezők, amelyeket figyelembe kell venni, ha egy szervezet információbiztonságát kívánjuk vizsgálni?
- Ezen területek közül melyek azok, amelyekbe erős szervezetük és melyek amelyekben gyengék?
- Ön mit tenne azért, hogy a rendszereiket megvédjék a fenyegetettségek ellen?
- Vizsgálják-e rendeszeresen a külső és belső fenyegetettségeket? A feltárt hiányosságok kiküszöbölésével foglalkoznak-e és ha igen, akkor azt, milyen módon teszik (határidők, felelősök, stb.)?
- Szervezeténél milyen fizikai, logikai, humán biztonságot szavatoló megoldásokat alkalmaznak?
- Definiálva vannak-e szervezeténél a felelősségek? Megtörténik-e a folyamatos számonkérés, esetleges felelősségre vonás?
- A számonkérések eredményeit visszacsatolják-e? Amennyiben igen, akkor milyen módon építik bele a mindennapi működésük folyamataiba?
- Az átalakulás és az új tudáscentrumok milyen hatással vannak az információbiztonságra?
- Melyek ön szerint azok az előnyök, amely a felhő alapú megoldások mellett szólnak?

- Az önök szervezete alkalmaz-e felhő alapú megoldásokat? Mi alapján döntöttek úgy, hogy ezeken a területeken bevezetik a felhő megoldásokat?
- Az alkalmazott felhő alapú szolgáltatásokat szervezeten belülről vagy kívülről veszik-e igénybe?
- Az új szervezeti működés milyen hatással lesz ön szerint a felhő alapú megoldások alkalmazására? Előremozdítja vagy háttérbe szorítja?
- El tudná mondani, hogy az ön meglátása szerint, az új működésnek melyek azok a tényezői, amelyek pozitív és melyek azok, amelyek negatív hatással vannak ezen technológiák bevezetésére?

12. melléklet: Vezetői szerepekkel kapcsolatos statisztikai eredmények

Domináns vezető szerep azonosítása (részlet)

Bróker	Innovátor	Mentor	Facilitátor	Koordinátor	Direktor	Producer	Monitor
-0,117230	1,414710	-0,142610	0,033020	-0,121290	-0,422480	-0,164670	0,043570
-0,075470	0,872230	0,024870	0,038700	-0,341910	-0,835750	-1,453660	0,268120
-0,075470	1,803580	0,807650	-0,186650	-0,685780	-0,595020	-0,671550	-0,876890
1,817230	0,780130	0,361920	0,901340	0,810330	-0,193970	0,608950	0,479390
0,583270	-0,770520	2,353520	-0,441240	0,465520	0,083330	-0,673650	-1,148010
-0,075470	1,018750	-0,434530	-0,641110	-0,186690	-1,169010	-0,424760	0,268120
1,158490	-0,110770	0,300460	-0,411290	-0,436240	1,765840	0,095420	0,281780
0,499750	1,612880	0,845210	-0,666580	0,234680	0,172770	0,396370	0,031720
1,158490	1,070020	0,616280	1,216530	0,626180	-0,460300	-0,414660	0,745360

A vezetői szerepek felmérés statisztikai eredményei

Domináns szervezeti kultúra	Terjedelem	Minimum	Maximum	Átlag	Szórás	Gyakoriság a teljes mintában
Bróker	5,00	1	6	2,58	1,07	12
Innovátor	6,00	1	7	3,99	1,77	56
Mentor	6,00	1	7	4,00	1,58	21
Facilitátor	6,00	1	7	2,81	1,41	30
Koordinátor	4,00	3	7	5,40	1,05	13
Direktor	6,00	1	7	3,59	1,90	46
Producer	6,00	1	7	2,89	1,42	25
Monitor	3,00	4	7	5,88	0,92	16

13. melléklet: Információbiztonsági kiválóság kvartilisek

Főkomponensek	*ELSŐ KVARTILIS (1)*	*MÁSODIK KVARTILIS (0,5)*	*HARMADIK KVARTILIS (0,75)*
Biztonsági területek	-0,753495	-0,10832	0,79049
Információbiztonság menedzsment érettség	-0,709775	-0,13456	0,72081
Külső információbiztonságot befolyásoló tényezők	-0,71337	-0,00535	0,73346
Belsőinformációbiztonságot befolyásoló tényezők	-0,604345	0,05151	0,745855

14. melléklet: Felhő alapú megoldások alkalmazásának kvartilisei

Főkomponensek	*ELSŐ KVARTILIS (1)*	*MÁSODIK KVARTILIS (0,5)*	*HARMADIK KVARTILIS (0,75)*
Publikus felhő szolgáltatások	-0,79234	-0,14269	0,646195
Privát felhő szolgáltatások	-0,65865	-0,14269	0,717485

15. melléklet: Szervezeti kultúra és információbiztonsági kiválósággsal kapcsolatos statisztikai eredmények

ANOVA eredmények szervezeti kultúra és információbiztonsági kiválóság esetében

ANOVA	*Négyzetösszeg*	*Átlag négyzet*	*F*	*Szignifikancia*
Csoportok között	16,403	5,468	16,726	0,000
Csoporton belül	70,282	0,327		
Összesen	86,685			

A domináns szervezeti kultúra és az információbiztonsági kiválóság kapcsolatának Post-Hoc elemzése (Tamhane)

(I) Domináns szervezeti kultúra	(J) Domináns szervezeti kultúra	*Átlag eltérés (I-J)*	*Szignifikancia*
Klán	Piac	-0,455	0,000
	Hierarchia	-0,690	0,000
Adhokrácia	Piac	-0,470	0,000
	Hierarchia	-0,706	0,000
Piac	Klán	0,6455	0,000
	Adhokrácia	0,470	0,000
Hierarchia	Klán	0,690	0,000
	Adhokrácia	0,706	0,000

16. melléklet: Vezetői szerepek és információbiztonsági kiválósággsal kapcsolatos statisztikai eredmények

ANOVA eredmények vezetői szerepek és információbiztonsági kiválóság esetében

ANOVA	*Négyzetösszeg*	*Átlag négyzet*	*F*	*Szignifikancia*
Csoportok között	24,410	3,487	11,815	0,000
Csoporton belül	62,275	0,295		
Összesen	86,685			

A vezetői szerepek és az információbiztonsági kiválóság kapcsolatának Post-Hoc elemzése (Tamhane)

(I) Domináns vezetői szerep	(J) Domináns vezetői szerep	*Átlag eltérés (I-J)*	*Szignifikancia*
Bróker	Koordinátor	-1,103	0,003
	Direktor	-0,986	0,006
	Monitor	-0,958	0,018
Innovátor	Koordinátor	-0,769	0,001
	Direktor	-0,652	0,000
	Monitor	-0,625	0,000
Mentor	Koordinátor	-0,674	0,005
	Direktor	-0,557	0,002
Facilitátor	Koordinátor	-0,836	0,000
	Direktor	-0,719	0,000
	Monitor	-0,692	0,017
Koordinátor	Bróker	1,103	0,003
	Innovátor	0,769	0,001
	Mentor	0,674	0,005
	Facilitátor	0,836	0,000
Direktor	Bróker	0,986	0,006
	Innovátor	0,652	0,000
	Mentor	0,557	0,002
	Facilitátor	0,719	0,000
Monitor	Bróker	0,958	0,018
	Innovátor	0,625	0,038
	Facilitátor	0,692	0,017

17. melléklet: Szervezeti kultúra és felhő alapú megoldások alkalmazásával kapcsolatos statisztikai eredmények

ANOVA eredmények szervezeti kultúra és a felhő alapú megoldások alkalmazása esetében

ANOVA	*Négyzetösszeg*	*Átlag négyzet*	*F*	*Szignifikancia*
Csoportok között	69,182	23,061	23,061	0,000
Csoporton belül	78,005	23,061		
Összesen	147,187			

A szervezeti kultúra és a felhő alapú megoldások kapcsolatának Post-Hoc elemzése (Tamhane)

(I) Domináns szervezeti kultúra	(J) Domináns szervezeti kultúra	*Átlag eltérés (I-J)*	*Szignifikancia*
Klán	Adhokrácia	-0,839	0,000
	Piac	0,422	0,004
	Hierarchia	0,619	0,000
Adhokrácia	Klán	0,839	0,000
	Piac	1,261	0,000
	Hierarchia	1,459	0,000
Piac	Klán	-0,422	0,004
	Adhokrácia	-1,261	0,000
Hierarchia	Klán	-0,619	0,000
	Adhokrácia	-1,459	0,000

18. melléklet: Vezetői szerepek és felhő alapú megoldások alkalmazásával kapcsolatos statisztikai eredmények

ANOVA eredmények vezetői szerepek és a felhő alapú megoldások alkalmazása esetében

ANOVA	*Négyzetösszeg*	*Átlag négyzet*	*F*	*Szignifikancia*
Csoportok között	120,261	17,180	24,262	0,000
Csoporton belül	149,411	0,708		
Összesen	269,671			

A vezetői szerepek és a felhő alapú megoldások kapcsolatának Post-Hoc elemzése (LSD)

(I) Domináns vezetői szerep	(J) Domináns vezetői szerep	*Átlag eltérés (I-J)*	*Szignifikancia*
Bróker	Innovátor	-0,839	0,000
	Koordinátor	0,558	0,027
	Producer	0,490	0,027
	Monitor	0,688	0.005
Innovátor	Bróker	0,839	0,000
	Mentor	0,708	0,000
	Facilitátor	0,889	0,000
	Koordinátor	1,397	0,000
	Direktor	1,220	0,000
	Producer	1,329	0,000
	Monitor	1,527	0,000
Mentor	Innovátor	-0,708	0,000
	Koordinátor	0,689	0,002
	Direktor	0,511	0,002
	Producer	0,621	0,001
	Monitor	0,818	0,000
Facilitátor	Innovátor	-0,889	0,000
	Koordinátor	0,508	0,016
	Direktor	0,330	0,026
	Producer	0,440	0,010
	Monitor	0,638	0,001
Koordinátor	Bróker	-0,558	0,027
	Innovátor	-1,397	0,000
	Mentor	-0,689	0,002
	Facilitátor	-0,508	0,016
Direktor	Innovátor	-1,220	0,000
	Mentor	-0,511	0,00
	Facilitátor	-0,330	0,026

Producer	Bróker	-0,490	0,027
	Innovátor	-1,329	0,000
	Mentor	-0,620	0,001
	Facilitátor	-0,440	0,010
Monitor	Bróker	-0,688	0,005
	Innovátor	-1,527	0,000
	Mentor	-0,818	0,000
	Facilitátor	-0,638	0,001

19. melléklet: ANOVA eredmények az információbiztonsági kiválóság és a felhő alapú megoldások alkalmazásának esetében

ANOVA	*Négyzetösszeg*	*Átlag négyzet*	*F*	*Szignifikancia*
Csoportok között	7,670	2,557	3,994	0.009
Csoporton belül	139,518	0,649		
Összesen	147,189			