BUDAPESTI CORVINUS EGYETEM

GAZDASÁGINFORMATIKA
DOKTORI ISKOLA

TÉZISGYŰJTEMÉNY

TARJÁN GÁBOR

AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN

című Ph.D. értekezéshez

TÉMAVEZETŐ:

Dr. Kő Andrea, Ph.D.

egyetemi tanár

és

Dr. Mitev Ariel Zoltán, Ph.D.

egyetemi docens

BUDAPEST, 2020

INFORMÁCIÓRENDSZEREK TANSZÉK

TÉZISGYŰJTEMÉNY

TARJÁN GÁBOR

AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN

című Ph.D. értekezéshez

TÉMAVEZETŐ:

Dr. Kő Andrea, Ph.D.

egyetemi tanár

és

Dr. Mitev Ariel Zoltán, Ph.D.

egyetemi docens

TARTALOMJEGYZÉK

1 KUTATÁSI ELŐZMÉNYEK ÉS A TÉMA INDOKLÁSA

Nyilvánvaló érdekünk fűződik ahhoz, hogy az információbiztonsági tudatosság szintjét megbízhatóan tudjuk mérni egy gazdálkodó szervezetben, hiszen a gazdálkodó szervezetek információ vagyona és annak védelme a profit és a non-profit széférában is egyre nagyobb jelentőséggel bír. Ez egyrészt versenyképességi kérdés, másrészt pedig olyan megfelelőségi kritérium, melyet számos nemzetközi standard és előírás vár el a gazdálkodó szervezetektől (lásd pl. a SOX (2002), HIPAA (1996), GLBA (1999), FISMA (2002), PCI DSS (2016), ISO 27001 (2013) és egyéb standardokat). Az információbiztonsági incidensek, káresemények döntő hányada emberi hibára, gondatlanságra, szándékosságra vezethető vissza, ami ellen leginkább az információbiztonsági tudatossággal tudunk védekezni. Emiatt a gazdálkodó szervezetek vezetői számára elemi érdek ennek a tudatosságnak a növelése az egyén és a szervezet szintjén.

Ha tudunk módszertani segítséget adni ennek a komplex mérési problémának a megoldásában, akkor a kidolgozott modell közvetlen támogatást jelenthet a szervezetek mindennapi gyakorlatában.

Több évtizedes auditori gyakorlattal a hátam mögött régóta foglalkoztat az a gondolat, hogy hogyan lehet a vizsgált szervezetek információbiztonsági tudatosságát fejleszteni annak tükrében, hogy nagyon egyértelműen látszik: a különböző információbiztonsági incidensek mögött döntő hányadban maga az ember (képességei és attitűdje) áll.

Az információbiztonság tudatosság nem a véletlenek mentén alakul ki a szervezetekben, hanem vannak bizonyos jó gyakorlatok (kontrollok), melyek léte, nemléte, bevezetettsége, minősége meghatározza a szervezet ezirányú érettségét.

Jelentős gyakorlati hasznot tulajdonítok annak, ha a szervezetekben ismertek és bevezetettek ezek a jó gyakorlatok, és ha a szervezetek felsővezetését ki tudjuk szolgálni olyan információkkal, hogy hol tartanak az általuk vezetett szervezetek a tudatosság szempontjából.

Ha mindezt még meg tudjuk támogatni olyan mérésekkel, melyek objektív képet rajzolnak az egyes szervezetek információbiztonsági tudatosságának érettségéről, és ezt a képet olyan módon tudjuk prezentálni a szervezet vezetése számára, hogy abból könnyen tudnak cselekvési programot alkotni és végrehajtani, akkor egy nagyon fontos küldetést tudunk eredményesen teljesíteni: A szervezet képes lesz célzottan a szervezeti tudatosságát növelni, melyből minden érdekelt fél remélhet hasznokat.

A disszertációban bemutatott többéves kutatási folyamatot ennek a célnak rendeltem alá, és reményeim szerint a küldetést sikeresen tudtam teljesíteni a bemutatásra kerülő módszerek és eredmények tükrében.

1.1 A kutatás célja

A kutatásom célja az volt, hogy egy konzisztens és koherens modellt alkossak az információbiztonsági tudatosság érettségi szintjének mérésére és ezt a modellt teszteljem és validáljam hazai és nemzetközi kutatások tükrében.

Nagy hangsúlyt fektettem a nemzetközi összehasonlításra, hogy láthatóvá tegyem, mennyiben igazolhatók vissza a nemzetközi trendek és tendenciák, hol van esetleg markáns különbség a hazai és a nemzetközi gyakorlat között.

A kutatás elvárt eredményei a következők:

- EO1: Egy konzisztens és a szakmai közönség számára elfogadható fogalomkészlet létrehozása és rendszerezése az információbiztonsági tudatosság és annak érettségi szintje vonatkozásában
- EO2: Egy részletező információbiztonsági tudatosság érettségi modell megalkotása
- EO3: A tudatosság érettségét támogató kontrollok azonosítása
- EO4: A tudatosság érettségi szintjét jelző audit bizonyítékok azonosítása
- EO5: Nemzetközi eredmények összevetése a hazai tapasztalatokkal az információbiztonsági tudatosság érettségi modell kontextusában
- EO6: Az összefüggések feltárása az egyes kontrollok és audit bizonyítékok, illetve a szervezet információbiztonsági tudatosságának érettségi szintje között

A kutatás alapcélja az volt, hogy kapcsolatokat mutassak ki a szervezetekben bevezetett és működő kontrollok és a szervezet információbiztonsági tudatosságának érettségi szintje között olyan módon, hogy ugyanakkor azonosítsam azokat az audit bizonyítékokat is, melyek jellemzők lehetnek az információbiztonsági tudatosság egyes érettségi szintjein.

A kutatás célkitűzései (részcéljai) a következők:

- RO1: Mely kontrollok jellemzik az információbiztonsági tudatosság magasabb szintjét képviselő szervezeteket?
- RO2: Milyen audit bizonyítékok támasztják alá az egyes szervezetek információbiztonsági tudatosságának érettségét?
- RO3: Milyen módon használhatók fel a nemzetközi kutatásokban bemutatott érettségi modellek a magyarországi szervezetek jellemzésére?
- RO4: Milyen tényezőktől függ egy szervezet információbiztonsági tudatosságának érettsége?

1.2 Kutatási kérdések

A felvázolt kutatás a következő kutatási kérdésekre keresi a választ:

- RQ1: Hogyan írható le, hogyan értékelhető a gazdálkodó szervezetekben az információbiztonsági tudatosság szintje, minősége a szervezet szintjén?
- RQ2: Mérhető-e a változás (javulás, romlás) egy szervezet életében a tudatosság érettségi szintje vonatkozásában?
- RQ3: Összehasonlíthatók-e a gazdálkodó szervezetek az információbiztonsági tudatosság érettsége szempontjából szervezeti szinten?
- RQ4: Támogatható-e a tudatosság értékelés hagyományos audit eszközökkel (pl. ellenőrző listák)?

1.3 Kutatási megközelítés és modell

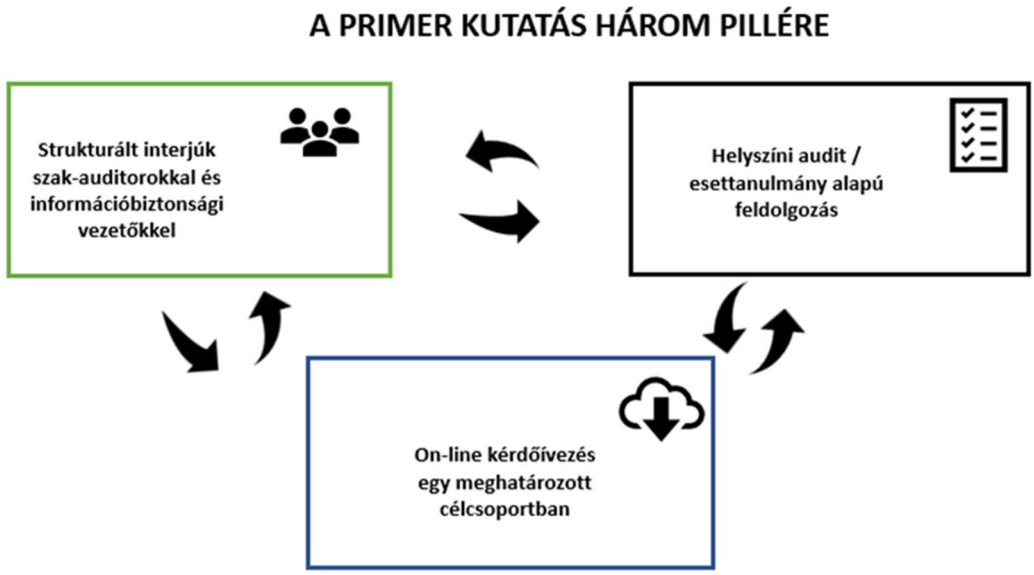
Kutatásom során egy kevert kutatásmódszertani megközelítést használtam: A kvantitatív kutatást támogatta egy alapvetően kérdőíves megkérdezés, melyet jól kiegészített néhány kvalitatív elem, pl. a szakauditorokkal folytatott interjúk és az esettanulmány (helyszíni audit) alapú feldolgozás.

A klasszikus szakirodalmi áttekintés (szekunder kutatás) és elemzés során tisztáztam a kutatási terület fogalomkészletét, alkottam egy a további elemzés szempontjából nélkülözhetetlen definíciót az információbiztonsági tudatosságra és megvizsgáltam a szóba jöhető statisztikai módszereket, melyek alkalmasak lehetnek a kutatási kérdésekben vélelmezett kapcsolatok létének és erősségének vizsgálatára.

A gyakorlati (primer) kutatás három pilléren nyugodott:

- on-line kérdőívezést hajtottam végre egy meghatározott célcsoportban
- strukturált interjúkat bonyolítottam le információbiztonsági szakauditorokkal és információbiztonsági vezetőkkel
- és egy esettanulmány alapú elemzést végeztem, hogy minta-szervezetek információbiztonsági tudatosságának érettségi szintjét megállapítsam helyszíni audit alapján.

Az 1. ábra mutatja az egyes pillérek kapcsolatát:



1. ábra: A primer kutatás három pillére (saját szerkesztés)

A három pillér kapcsolata:

- Az on-line kérdőív segítségével szert tettem egy olyan statisztikai értelemben feldolgozható adatmennyiségre, mely alkalmas volt a kidolgozott érettségi modell validálására, és segítette annak továbbfejlesztését.

- Interjúkon mértem fel, hogy a kérdőívezés során feltett kérdések mennyire voltak egyértelműek, kezelhetőek és ennek tükrében mennyire tekinthetők érvényesnek a válaszok, és a válaszok nyomán milyen kiegészítésekkel lehet élni a modellben.
- Az esettanulmány alapú feldolgozás pedig arra volt alkalmas, hogy megvizsgáljam az érettségi modell egyértelműségét, megismételhetőség jelző funkciójának működőképességét, azaz képes-e a változásokat (egyik szintről a másikra lépés) regisztrálni, kimutatni.

2 A FELHASZNÁLT MÓDSZEREK

A kutatás egyik fő célja az volt, hogy részleteiben kidolgozzak és validáljak egy érettségi modellt a szervezeti információbiztonsági tudatosság értékelésére. Ennek érdekében végeztem a szekunder és a primer kutatást.

A szekunder kutatás során egy átfogó elemzést végeztem a szakterület irodalmában. A szakirodalmi feldolgozás nyomán született meg egy saját „információbiztonsági tudatosság" definíció és egy továbbfejlesztett érettségi modell a tudatosság szervezeti érettségének értékelésére.

A primer kutatás három ágon vizsgálta a létrehozott érettségi modellt:

- Kérdőív segítségével elemeztem a modell gyakorlati használhatóságát és kerestem a kimutatható kapcsolatokat más nemzetközi modellekkel,
- Interjúkat folytattam szakauditorokkal, hogy szakmai szemüvegen keresztül is értékelhető legyen a létrejött érettségi modell és további információkat kapjak a gyakorlati használhatóságáról,
- Helyszíni próba-auditokon egy esettanulmány alapú megközelítést alkalmazva elemeztem az „élő és valós" szerveztek aspektusából az érettségi modell megfelelőségét.

A három irányú vizsgálat tapasztalatait egyesítettem az értekezés 4. fejezetében.

Mind a szekunder, mind pedig a primer kutatás során számos olyan módszertani kérdés merült fel, melyek megválaszolása döntő módon befolyásolta a kutatás menetét.

2.1 Módszertani választások a szekunder kutatás kapcsán

Mivel már az alapfogalmak tekintetében is jelentős átfedések, félreértések, félreértelmezések, illetve pongyola szóhasználat figyelhetők meg, ezért első lépésként a fellelhető szakirodalmak keresését néhány kulcsszó mentén végeztem el:

- Information security – információbiztonság
- Awareness – tudatosság
- Maturity – érettség

Jellemző a szakterület kutatottságára, hogy az „information security" fogalmára legalább 196.000.000 találatot jeleznek a különböző internetes keresők és az „információbiztonság" kifejezéshez is 20.800-at meghaladó találatot kaptunk. Ez így kezelhetetlen mennyiségű és minőségű szakmai anyagot jelent, ezért szükség volt egy erős szelekciós mechanizmus kialakítására.

A fogalmi kereteket bemutató szakirodalom feldolgozását egy szakirodalmi áttekintő cikk (review article) formájában dokumentáltam (Tarján (2018)). Számos olyan szakmai szervezet publikál anyagokat (pl. ISACA, SANS Institute) melyek nem minősülnek ugyan tudományos szakirodalomnak, de nem megkerülhetők ismertségük, gyakori használatuk és gyakorlatias megközelítésük miatt.

A legjobban használható információbiztonsági tudatosság érettségi modellt Spitzner (2012) 2012-ben publikálta egy blogbejegyzésben, amely ugyan nem minősíthető tudományos forrásnak, de azóta annyira elfogadottá vált modelljének alkalmazása, hogy évente többezren válaszolnak a SANS Institute on-line kérdőívére, és évente születnek tudományos értékű elemzések a SANS Institute gondozásában (2015) (2016) (2017) (2018) és (2019).

2.2 Módszertani választások a primer kutatás során

A szekunder kutatás során tisztáztam a szakterület fogalomkészletét és alkottam egy saját definíciót az információbiztonsági tudatosságra. Készítettem egy továbbfejlesztett modellt az információbiztonsági tudatosság érettségi szintjének mérésére. A gyakorlati kutatás volt hivatott a modell megfelelőségnek és használhatóságának vizsgálatára. Esetünkben három lehetséges módszertani eszköz és irány merült fel:

- Klasszikus kérdőíves felmérés,
- Terepkutatás mélyinterjúk alkalmazásával,
- Terepkutatás esettanulmány alapú megközelítésben.

A kutatás egyik deklarált célja az volt, hogy a nemzetközi szakirodalomban leírt modellek, az ennek alapján készült saját modell, és a modell alkalmazásából levonható következtetések hazai verifikálását végezzem el. Ez a cél két nemzetközi szakmai publikáció kapcsán valósult meg:

- Dzazali és Zolait (2012) már hivatkozott modelljét kívántam hazai környezetben részlegesen reprodukálni és tesztelni kérdőíves módszerrel. Az értekezés 3.3-as fejezetben szólok részletesebben ennek a modellnek az alkalmazásáról.
- Spitzner (2012) érettségi modelljéhez minden évben kapcsolódik egy világszintű kérdőíves felmérés, melynek eredményeit egy éves jelentésben foglalja össze a SANS Institute. A 2018-as és a 2019-es riport (SANS Institute (2018), SANS Institute (2019)) eredményei rendelkezésemre állnak és ez kínálta az összehasonlítás lehetőségét a hazai mintával. A disszertáció 3.3-as fejezetben bemutatom a kérdőívem kapcsolatát a hivatkozott érettségi modellel.

3 AZ ÉRTEKEZÉS EREDMÉNYEI

A kutatás mindkét fő fázisa szolgált kézzelfogható eredményekkel, melyeket ebben a fejezetben ismertetek.

3.1 A szakirodalmi kutatás eredményei

A tanulmányozott szakirodalmakból leszűrhetővé vált egy saját definíció az információbiztonsági tudatosságra és ennek felhasználásával összerakható volt egy érettségi modell, melyben felhasználtam más modellek tapasztalait is.

3.1.1 EGY DEFINÍCIÓ AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG FOGALMÁRA

Az irodalmi áttekintésem nyomán és az azonosított fogalmi rések alapján a következő információbiztonsági tudatosság fogalmat ajánlom használatra:

Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban.

(Information Security Awareness (ISA) is a knowledge and attitude of interested parties of an organization on the protection of information assets owned or managed by the organization.)

Ennek a definíciónak van néhány nagyon fontos rétege:

- Az információbiztonsági tudatosság nem csak a menedzserekről és alkalmazottakról szól, hanem az érdekelt felek széles rétegét érinti, akik mindannyian bizonyos hatással vannak a szervezet információbiztonsági tudatosságának állapotára (pl. egy pénzügyi szolgáltató esetében elvárunk némi információbiztonsági tudatosságot az ügyfelektől is, hiszen az általuk követett jó vagy rossz gyakorlat nagy hatással van az adott szervezet biztonsági állapotára – lásd a biztonságos PIN-kód használat a bankkártyatulajdonosok esetében)
- Tudás: A szabályok, eljárások és utasítások ismerete alapvető az információbiztonsági tudatosság szempontjából, de önmagában ez a fajta tudás még nem biztosít aktív védelmet az információs vagyonelemek felett.
- Attitűd: Ez egy pozitív hozzáállást tételez fel a biztonsággal kapcsolatos védelmi intézkedésekkel és kontrollokkal kapcsolatban. Azaz az emberek nem csak megértik, hogy mit kell csinálni és az miért helyes, hanem aktívan részt vesznek a megelőző és helyesbítő intézkedésekben. Jelentik az észlelt gyanús eseményeket, részt vesznek a mentési és helyreállítási műveletekben, követik a szabályokat és aktívan adnak egymásnak segítséget, ha váratlan biztonsági eseményekkel szembesülnek.
- Saját tulajdonú vagy kezelt információk: Az információ tulajdonlása fontos, de nem a szervezeti magatartást egyedüli módon befolyásoló tényező. Az adatfeldolgozás új korszaka számos esetben hoz létre olyan helyzeteket, amikor az adatfeldolgozó felelős az általa nem tulajdonolt adatokért (lásd pl. számítási felhő technológiai szolgáltató cégek). Ezeknek a speciális helyzeteknek komoly hatása van az információbiztonsági programokra és kampányokra, melyek az érintett szervezeteknél folynak.

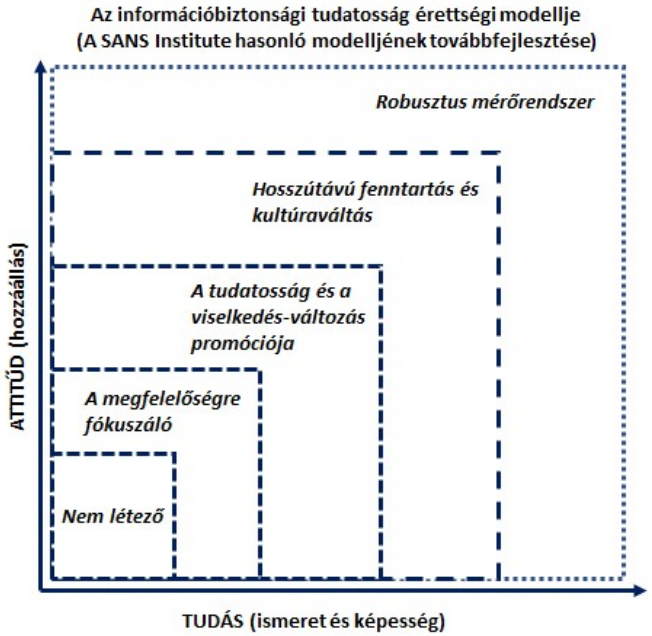
3.1.2 Egy saját érettségi modell az információbiztonsági tudatosság szintjének mérésére

Az értekezés szakirodalmi fejezeteiben is bemutattuk, hogy számos különböző érettségi modell létezik, mely alkalmas lehet az információbiztonsági tudatosság mérésére.

A 3.1.1 fejezetben hivatkozott információbiztonsági tudatosság definícióra alapozva *(Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban.)* már csak a következőket kellett megtennünk:

- El kellett fogadnunk a hivatkozott SANS Institute (2017) információbiztonsági tudatossági érettségi modelljének már meghatározott szintjeit.
- Két dimenziót (tudás és attitűd) kellett kapcsolnunk minden egyes érettségi szinthez.
- Meg kellett határoznunk az egyes érettségi szintekhez kapcsolható érdekelt feleket.
- El kellett készítenünk egy olyan kontroll leltárat, mely kontrolloknak a léte, összessége, együtt hatása és működése bizonyíték lehet az információbiztonsági tudatosság érettségi szintjére.
- Néhány értelmező megjegyzést kellett fűznünk és audit-bizonyítékokat kell meghatároznunk minden egyes érettségi szintekhez kötődően, hogy legyen egy közös értelmezésünk a szintekre vonatkozóan.

Mivel mindezeket a feladatokat elvégeztük, ezért a rendelkezésünkre állt egy olyan modell, mely alkalmas volt a validálásra. Nem feledve a fő célunkat, hogy egy auditálható, mérhető modellt kellett alkotnunk, szükségünk volt azoknak az objektív bizonyítékoknak az összegyűjtésére, melyek alkalmasak az információbiztonsági tudatosság érettségi szintjének mérésére egy szervezetben. Az alábbiakban leírt modellt alkalmasnak gondolom erre a célra. Az ajánlott modell vizualizált formában:



2. ábra: Az ajánlott modell az információbiztonsági tudatosság érettségének mérésére (saját ábra)

3.2 A primer kutatás eredményei

A három kutatási pillért kívántam a primer kutatással megtámogatni:

- Az on-line kérdőív volt hivatott olyan statisztikai értelemben feldolgozható adatmennyiség megszerzésére, mely alkalmas a kidolgozott érettségi modell validálására, illetve kellően reprezentatív minta esetében a sokaság egészére vonatkozó megállapítások rögzítésére (pl. a minta alapján a szervezetek jellemzően mely érettségi szintet képviselik).
- Az interjúkon kívántam felmérni, hogy a kérdőív alkalmazása során feltett kérdések mennyire voltak egyértelműek, kezelhetőek és ennek eredményeképpen mennyire tekinthetők érvényesnek a válaszok. Ugyancsak ettől a kutatási fázistól vártam, hogy olyan szempontok (pl. információbiztonsági tudatosságra utaló további speciális kontrollok) is előkerüljenek, melyek beépítése pontosíthatja az érettségi modellt és könnyítheti az egyértelmű kérdőív kitöltést
- Az esettanulmány alapú feldolgozás alkalmas volt arra, hogy megvizsgáljam az érettségi modell egyértelműségét, megismételhetőségét és jelző funkciójának működőképességét, azaz képes-e a változásokat (egyik szintről a másikra lépés) regisztrálni, kimutatni:
    - Egyértelműnek és megismételhetőnek akkor tekinthető az érettségi modell alapú besorolás, ha az on-line válaszadó kitöltése (eredménye) nagyjából megegyezik egy helyszíni auditon elvégzett próba eredményeivel.
    - Jelző funkció alatt a modell azon képességét értem, hogy alkalmas-e a változások mérésére, tehát két időperiódusban elvégzett értékelés képes-e változást kimutatni az érettségi szintben (és értelemszerűen a gazdálkodó szervezet által követett információbiztonsági tudatossági gyakorlatban).

3.2.1 On-line kérdőívezés egy meghatározott célcsoportban (kvantitatív kutatás)

A kérdőíves megkérdezéstől azt vártam, hogy legyen egy statisztikai értelemben elfogadható méretű magyarországi mintám, amely alkalmas lehet a nemzetközi összevetésre és a saját (továbbfejlesztett) modell igazolására.

A válaszok feldolgozása, elemzése kapcsán három nagyobb kutatási irányt vizsgáltam:

- Dzazali és Zolait (2012) modelljét – némileg korlátozott módon - összevetettem a magyar mintával. Itt csak azokat a tudatosság érettségi szintre ható tényezőket vizsgáltam, melyeket ők is jelentősnek ítéltek modelljükben,
- A SANS Institute 2018-as jelentése (SANS Institute (2018)) és a 2019-es jelentés (SANS Institute (2019)) Spitzner (2012) modelljét két egymást követő évben keletkezett nemzetközi mintán alkalmazta. Az ott bemutatott eredményeket vetettem össze a magyar adatokkal,

- A kérdőívem III. és IV. szekciójában leírt kontroll és auditbizonyíték halmazokat pedig összekapcsoltam az ötfokozatú érettségi modellel, hogy a kutatás által remélt egyik legfontosabb eredményt megkapjam: Legyenek „konyhakész" kontroll és audit bizonyíték listáim a saját modell egyes érettségi fokaihoz kapcsoltan.

Dzazali és Zolait (2012) modellje

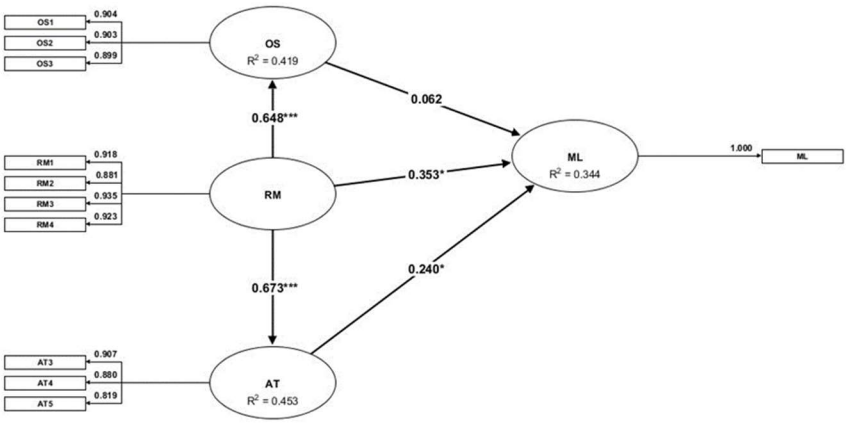
Dzazali és Zolait (2012) hat hipotéziséből hármat (DZ-H1, DZ-H2 és DZ-H4) vizsgáltam a kérdőívemmel. A vizsgált hipotézisek:

- DZ-H1: A kockázatelemzési mechanizmusnak (Risk Management Mechanism - RM) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (Maturity Level – ML).
- DZ-H2: A szervezeti struktúrának (Organisation Structure - OS) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (Maturity Level – ML).
- DZ-H4: A szervezeti tudatossági és képzési kultúrának (Awareness and training culture – AT) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (Maturity Level – ML).

Dzazali és Zolait (2012) modelljének tesztelésére a varianciaalapú strukturális egyenlőségek modelljét (PLS-SEM – Strukturális egyenletek modellje a parciális legkisebb négyzetek módszerével) használtam. Az elemzést az ADANCO Composite Modelling szoftverrel (v2.1.1) végeztem (Dijkstra - Henseler (2015)), és az első modellezési próbálkozás során a három konstrukcióhoz (és hipotézishez) tartozó összes állítást (RM1, RM2, RM3, RM4, RM5 és OS-1, OS-2, OS-3, OS-4, illetve AT-1, AT-2, AT-3, AT-4, AT-5) és a rájuk kapott válaszokat beemeltem a modellbe. Több iterációs lépés végrehajtásával kaptam egy olyan modellt, hogy az OS-4, az RM-5 és az AT-1, AT-2 állítások kihagyásával a modell minőségi kritériumai is megfelelővé váltak.

Az egyes iterációs lépések (szoftverfuttatások) megmutatták azt a sajátosságát a Dzazali-Zolait (2012) féle modellnek, hogy az egyes konstrukciókban olyan állítások keverednek, melyek egymással erős átfedésben vannak.

A végső strukturális modell és az eredmények az alábbi ábrában foglalhatók össze:



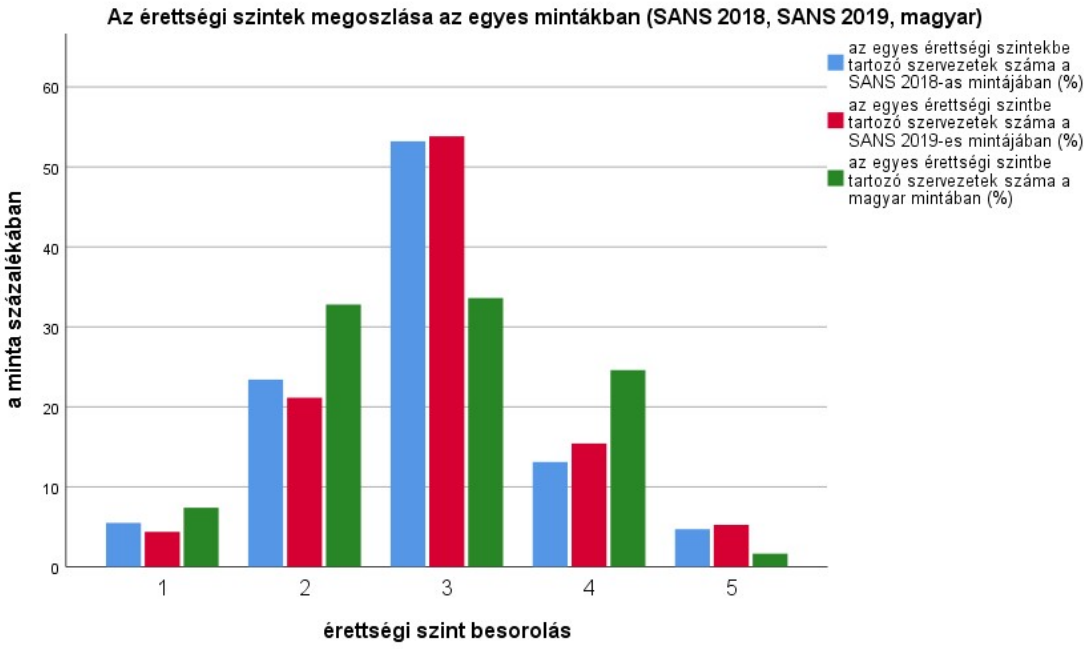
3. ábra: A végső strukturális modell és az eredmények (saját ábra az ADANCO modell alapján)

A végső strukturális modell és a kapcsolódó eredmények (jósági kritériumok) alapján az látható, hogy Dzazali és Zolait (2012) hipotézisei elfogadhatók voltak a magyar mintán is.

Spitzner (2012) modellje

A SANS Institute 2018-as és 2019-es jelentése (SANS Institute (2018) és (2019)) Spitzner (2012) modelljére alapozva mutat egy jellegzetes eloszlást az öt érettségi szint kapcsán a nagyjából 1700, illetve 1500 elemű nemzetközi mintában. A 122 elemű magyar minta és a két nemzetközi minta megoszlását az egyes érettségi szintek között összevetettem egy csoportosított oszlopdiagram formájában.

Szembeötlő, hogy míg a két nemzetközi minta erősen egybesimul minden érettségi szint esetében, addig a magyar minta ettől eltérő képet mutat: A fedőgörbe lényegesen laposabb, de a másik két mintához hasonló módon ez is a normális eloszlás jellegét mutatja.



4. ábra: Az érettségi szintek megoszlása a két nemzetközi és a magyar mintában (forrás: saját ábra)

Saját modell

A két nemzetközi és a magyar minta összevetése után a magyar mintán vizsgáltam néhány hipotézist, hogy a kidogozott modellt részleteiben tesztelhessem. A vizsgált hipotézisekkel kapcsolatos eredményeket a 3.3 fejezetben összegeztem. Az igazolt hipotézisek mentén létrehoztam egy gyorstesztet, mely alkalmas egy szervezet információbiztonsági tudatossága érettségi szintjének megállapítására. A disszertáció „E” melléklete tartalmazza ezt a modellt:

Érettségi szint	A szint általános jellemzői	Tudást (ismeretet és képességet) támogató kontrollok	Attitűdöt (hozzállást) támogató kontrollok	Audit bzonyítékok
1 - Nem létező	Információbiztonsági tudatosság gyakorlatilag nem létezik.	Nincsenek.	Nincsenek.	Nincsenek a tudatosság létezésére vonatkozóan.
2- A megfelelőségre fókuszáló	Információbiztonsági tudatosító program már létezik, de kifejezetten a megfelelőségre vagy külső audit követelmények teljesítésére készült.	Rendszeres (éves) és dokumentált tudatosító tréning események. Általános célú információbiztonsági tudatosító tananyagok (tartalmak) rendelkezésre állnak (pl. videók, hírlevél, prezentációs anyagok). Rendszeres (évenkénti) belső auditok. A beléptetési folyamat részeként a munkatársak bevezető képzést kapnak általános információbiztonsági tartalommal.	Dokumentált fegyelmi eljárás.	Képzési anyagok, képzési feljegyzések, dokumentált eljárás a vevői igények azonosítására, dokumentált eljárás a szállítók menedzselésére, dokumentált eljárás a bevezető és a rendszeres képzési eseményekre, aláírt titkossági megállapodások az alkalmazottakkal és a beszállítókkal, harmadik fél által készített audit jelentések, a vevők és/vagy harmadik fél által kibocsátott megfelelőség igazolások, kockázatértékelési jelentések
3 - A tudatosság és a viselkedés változás promóciója	Ez az információbiztonsági tudatossági szint egy olyan részletes kockázatértékelésen alapul, mely egyértelműen megmutatja, hogy mely biztonsági témaköröknek van a legnagyobb hatása a szervezeti célok megvalósítására, és az információbiztonsági erőfeszítések ezekre a kulcstémakörökre fókuszálnak.	A szervezet saját kockázatelemzésen alapuló információbiztonsági tudatosító szervezetspecifikus tananyagok (tartalmak) rendelkezésre állnak.	A hagyományos fegyelmi eljáráson túlmutató és szabályozott (dokumentált) ösztönző rendszer pl. jutalmak, díjak, kampány ajándékok stb. az információbiztonsági tudatosság területén.	A második szinthez képest olyan további elemek jelennek meg, mint pl. az információbiztonság tárgykörében releváns témakörök listája összekapcsolva egy részletes kockázatértékeléssel, vezetői átvizsgálások jegyzőkönyvei vagy emlékeztetői, információbiztonsági projektekhez kapcsolód dokumentáció (projekt alapító dokumentum – PAD, projekt terv, cselekvési terv, jelentések stb.), rendszeres vezetői kommunikációs tartalmak új kockázatokkal, védelmi intézkedésekkel és azok eredményeivel e-mail, blog, video stb. formájában.
4 -Hosszú távú fenntartás és kultúra váltás	Ezen a szinten van egy információbiztonsági tudatosító program, melynek vannak meghatározott folyamatai, erőforrásai és a vezetői támogatás is ott van mögötte hosszú távon, és minimálisan évente egyszer felülvizsgálják és aktualizálják a programot. Mind maga a program mind az információbiztonság megalapozott és folyamatosan aktualizált része a szervezeti kultúrának.	Dokumentált eljárásrend a kommunikált tartalmak rendszeres felülvizsgálatára és a tanulási célok meghatározására célcsoportonkénti bontásban. Rendszeres tudásfelmérés tesztek formájában.	Az egyes személyek személyes teljesítményértékelésének része az információbiztonsággal kapcsolatos célok teljesülésének értékelése.	A programhoz kapcsolódó dokumentáció (projektek definiált halmaza, projekt és program jelentések), az információbiztonsági tudatosításhoz rendelt részletes költségvetés hosszabb időtávra (pl. három évre).
5 -Robusztus mérőrendszer	Az információbiztonsági tudatosító programnak van egy erős mérőszám rendszere, mely alkalmas a fejlődés nyomon követésére és méri az egyes programelemek hatását. Ebből következően a program folyamatosan fejlődik és képes a beruházás megtérülését is bemutatni.	Dokumentált és bevezetett eljárás a szervezeti információbiztonsági tudatosság mérésére (mérőszámok, a mérés végrehajtása, és a mérési eredmények felhasználására).	Személyre, szervezeti egységre szabott "SMART" célok. (SMART - specific, measurable, attainable, realistic, timely - specifikus, mérhető, elérhető, realisztikus, jól időzített)	Dokumentált és nyomon követhető kulcs irányítási mutatók (KGI – Key Governance Indicator) és kulcs teljesítmény mutatók (KPI – Key Performance Indicator), biztonsági beruházás megtérülési mutatók (ROI – Return On Investment, ROSI – Return On Security Investment) kalkulációi.

3.2.2 Strukturált interjúk auditorokkal és információbiztonsági vezetőkkel (kvalitatív kutatás)

A kvalitatív kutatás során az volt a célom, hogy a kérdőíves megkérdezés (kvantitatív kutatás) eredményei alapján kiválasszak minden érettségi szintre (1-5 fokozat) legalább egy minta szervezetet, és a kérdőív kitöltőivel mélyinterjúkat szervezzek és hajtsak végre. Ezek az interjúk voltak hivatottak olyan további információk gyűjtésére, melyek alapján a modell működőképességének mélyebb értékelése és „finomhangolása” megtörténhetett.

A mélyinterjúkat célzottan olyan szakértőkkel folytattam le, akik napi szinten találkoznak az információbiztonsági tudatosság érettségi szintjével kapcsolatos problémákkal. A kiválasztott személyek között volt:

- Nemzetközi tanúsító testület sokéves gyakorlattal bíró szakauditora
- Nemzetközi hírű magyar start-up cég információbiztonsági vezetője
- Pénzügyi szektor felügyeleti szerve IT auditokat végző szervezeti egységének vezetője
- Multinacionális telekommunikációs szolgáltató cég magyarországi középvezetője
- Hivatásos „social engineer”
- Banki, pénzintézeti adatvédelmi felelős.

A főbb megállapításokat az értekezés 4.2 fejezete tárgyalja. Összességben megállapítható volt, hogy az interjúalanyok tudták értelmezni és használni az ötfokozatú modellt. Merőben új megközelítés vagy a kidolgozott érettségi modellnek ellentmondó információ nem került felszínre az interjúk során.

3.2.3 Esettanulmány alapú feldolgozás / Információbiztonsági tudatosság érettségi szintjének megállapítása helyszíni audit alapján

A kutatásnak ebben a szakaszában az előző alfejezetben leírt elvek és gyakorlat felhasználásával, de egy fordított szemléletű vizsgálattal ellenőriztem a modellem működőképességét: Random módon kiválasztott néhány gazdálkodó szervezetnél hagyományos audit módszertan alkalmazásával elvégeztem egy információbiztonsági tudatossági érettségi szint felmérést.

Szerencsémre a helyszíni auditokra olyan szervezeteknél találtam lehetőséget, ahol valamilyen különlegességet lehetett megtapasztalni, akár a szervezet profilja, akár az általa követett gyakorlat miatt. A helyszíni audittal vizsgált szervezetek:

- IT outsourcing szolgáltató
- IT szolgáltató (felhő titkosítás)
- Katasztrófavédelmi szakmai szervezet
- Nemzetközi Tanúsító Testület hazai fiókirodája
- Egyetemek (egyetemi belső informatikai szolgáltatók)
- Multinacionális egészségügyi diagnosztikai szolgáltató szervezet
- Sérült személyeket támogató szakmai egyesület.

Összességben megállapítható volt, hogy az ötfokozatú modell és annak elemei jól vizsgálhatók az auditok során. Az egyes érettségi szintekhez rendelt attribútumok összekapcsolhatók voltak az egyes vizsgált szervezetekkel és minden szervezet besorolható volt az ötfokozatú skálán. Az auditok tapasztalatai alapján kijelenthető, hogy egy előre elkészített kontroll lista és audit bizonyíték jegyzék támogatja a szervezetek értékelését és besorolását az ötfokozatú modell mentén. Ráadásul a lista és jegyzék léte biztosítja, hogy a szervezet számára ajánlásokat fogalmazhassunk meg egy következő érettségi szinte lépéshez szükséges tennivalók vonatkozásában.

3.3 A kutatási eredmények összegzése

Az 1. táblázat a kutatás célokat (RO1-RO4) és a témakörrel kapcsolatos eredményeket foglalja össze.

1. táblázat: A teljesült kutatási célok (saját szerkesztés)

Kutatási cél	A témakörrel kapcsolatos eredmények
RO1 Mely kontrollok jellemzik az információbiztonsági tudatosság magasabb szintjét képviselő szervezeteket?	A jellemző kontrollokat összegyűjtöttem abban a kérdőívben, melyet kitöltettem a kutatásban résztvevő személyekkel. Habár a kitöltőknek volt lehetőségük további kontrollokat is említeni és bevonni a modellbe, egyetlen válaszadótól sem jött ilyen jellegű kezdeményezés, amiből arra következtetek, hogy sikerült egy többé-kevésbé teljes kontroll leltárt készíteni. A kérdőívek feldolgozása, a helyszíni auditok és a szakértői interjúk alapján kijelenthető, hogy a kontrollok jól hozzárendelhetők az egyes érettségi szintekhez.
RO2 Milyen audit bizonyítékok támasztják alá az egyes szervezetek információbiztonsági tudatosságának érettségét?	A jellemző audit bizonyítékokat is összegyűjtöttem abban a kérdőívben, melyet kitöltettem a kutatásban résztvevő személyekkel. Habár a kitöltőknek volt lehetőségük további audit bizonyítékokat is említeni és bevonni a modellbe, egyetlen válaszadótól sem jött ilyen jellegű kezdeményezés, amiből arra következtetek, hogy sikerült egy többé-kevésbé teljes audit bizonyíték leltárt összerakni. A kérdőívek feldolgozása, a helyszíni auditok és a szakértői interjúk alapján kijelenthető, hogy a felsorolt audit bizonyítékok jól hozzárendelhetők az egyes érettségi szintekhez.
RO3 Milyen módon használhatók fel nemzetközi kutatásokban bemutatott érettségi modellek a magyarországi szervezetek jellemzésére?	Azt gondolom, hogy Spitzner (2012) modellje jól értelmezhető a magyar kérdőív kitöltők számára, mert az értelmezéssel kapcsolatos kérdést, észrevételt a kitöltőktől nem kaptam és a korlátos számú interjúm is azt igazolta, hogy a modell jól adaptálható a hazai környezetben. Erről az értekezés 4.1.3-as pontjában szólok bővebben.
RO4 Milyen tényezőktől függ egy szervezet információbiztonsági tudatosságának érettsége?	Az előzetesen azonosított tényezők (bevezetett kontrollok és feltárt audit bizonyítékok) jól reflektálnak az egyes érettségi szintek jellegére és erős kapcsolatot vélelmezek az érettségi szintek és kontrollok, illetve audit bizonyítékok között.

A kutatás eredményeinek összefoglalásaként a doktori értekezésben felvetett hipotéziseket és az egyes hipotézisekhez kapcsolódó döntéseket jeleníti meg a 2. táblázat.

2. táblázat: A hipotézisek és a kapcsolódó döntések (saját szerkesztés)

HIPOTÉZISEK: AZ ELSŐ HÁROM DZAZALI ÉS ZOLAIT (2012) MODELLJÉNEK HIPOTÉZISEI, A KÖVETKEZŐ HAT PEDIG A SAJÁT HIPOTÉZISEK.	A HIPOTÉZISHEZ KAPCSOLÓDÓ DÖNTÉSEK (ÉS AZ ÉRTEKEZÉS MEGFELELŐ FEJEZETE, MELY RÉSZLETEIBEN IS BEMUTATJA A DÖNTÉST.)
DZ-H1: A kockázatelemzési mechanizmusnak (**Risk Management Mechanism - RM**) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (**Maturity Level – ML**).	Elfogadva (lásd a 4.1.2 fejezetet!)
DZ-H2: A szervezeti struktúrának (**Organisation Structure - OS**) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (**Maturity Level – ML**).	Elfogadva (lásd a 4.1.2 fejezetet!)
DZ-H4: A szervezeti tudatossági és képzési kultúrának (**Awareness and training culture – AT**) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (**Maturity Level – ML**).	Elfogadva (lásd a 4.1.2 fejezetet!)
KH1: Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több kontroll azonosítható a működésében.	Elfogadva (lásd a 4.1.4.1 fejezetet!)
KH2: Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több audit bizonyítékot szolgáltat.	Elfogadva (lásd a 4.1.4.2 fejezetet!)
KH3: Minél több tudatosító kontrollt működtet egy szervezet, annál több audit bizonyíték keletkezik a szervezetben.	Elfogadva (lásd a 4.1.4.3 fejezetet!)
KH4: Az üzleti vállalkozások jellemzően magasabb információbiztonsági tudatosság érettségi szintet képviselnek, mint a non-profit szervezetek.	Elfogadva (lásd a 4.1.4.4 fejezetet!)
KH5: A nagyobb szervezetek jellemzően magasabb érettségi szintet képviselnek.	Elutasítva (lásd a 4.1.4.5 fejezetet!)
KH6: A menedzserek jellemzően magasabbra értékelik szervezetüket az érettség szempontjából, mint a szervezetben dolgozó szakértők.	Elutasítva (lásd a 4.1.4.6 fejezetet!)
KH7: Az egyes érettségi szintekhez tartozó jellemző kontrollok a vizsgált mintában azonosíthatók és ezáltal maga a kidolgozott érettségi modell megfelelősége is igazolható.	*Nem vizsgált a mintanagyság (kis számú rendelkezésre álló megfigyelés) miatt!*
KH8: Az egyes érettségi szintekhez tartozó jellemző audit bizonyítékok a vizsgált mintában azonosíthatók és ezáltal maga a kidolgozott érettségi modell megfelelősége is ezúton igazolható, megerősíthető.	*Nem vizsgált a mintanagyság (kis számú rendelkezésre álló megfigyelés) miatt!*

A 3. táblázatban összevetésre kerülnek a doktori értekezés bevezetésében megfogalmazott előzetesen elvárt kutatási eredmények (EO1-EO6) és a kutatás tényleges kimenetei. Az összerendelés célja annak bemutatása, hogy a kutatás eredményei hogyan válaszolják meg a kutatás elvárt eredményeit.

3. táblázat: Az előzetesen várt és tényleges eredmények

A KUTATÁS TÉNYLEGES KIMENETE	AZ ELŐZETESEN VÁRT KIMENET
A szakirodalom erősen informatikai orientációjú és nem szolgáltat kielégítő definíciót az információbiztonsági tudatosságra, emiatt egy a kutatás során következetesen használható meghatározást kellett alkotnom. Ezt tárgyalja a disszertáció 2.2.3 fejezete.	**EO1:** A tárgykörben hozzáférhető szakirodalom egyértelmű és következetes fogalomhasználat mellett pontosan leírja az információbiztonsági tudatosság fogalmát.
A Spitzner (2012) féle modell mögött sokéves tapasztalat húzódik, és egy jelentős nemzetközi adatbázis hozzáférhető a szervezetek önértékelési eredményeiről. Ezt taglalja az értekezés 2.4.3.3 alfejezete. Spitzner mellett még egy kutatás eredményei voltak beforgathatók a nemzetközi összevetésbe: Dzazali és Zolait (2012) modelljét is lehetett részben összevetni hazai megfigyelésekkel.	**EO2:** A kutatás során sikerül azonosítani olyan érettségi modellt, mely alkalmas a szervezetek információbiztonsági tudatosságának érettségét értékelni és mérni.
Spitzner (2012) modelljéhez kapcsolódó nemzetközi statisztikák (pl. a szervezetek megoszlása az egyes érettségi szintek között) jól összehasonlíthatók egy magyarországi mintával. Gondot csak a szükséges megfigyelésszám (és így a megfelelő mintanagyság) produkálása okoz: A vártnál lényegesen rosszabb válaszadói hajlandóság miatt a kérdőíves vizsgálat elhúzódott és jelentős erőfeszítéseket igényelt. Ennek részleteit a 4.1 fejezet tárgyalja.	**EO3:** A kutatás kapcsán lehetséges olyan hazai adatfelvételezést végezni, mely alapján a hazai és nemzetközi adatok összevethetők.
A kérdőíves minta mérete (122 válaszadó) és a válaszok minősége (volt olyan vizsgálat, mely esetében csak 72 válasz volt figyelembe vehető) miatt statisztikai módszerekkel nem lehetett az előzetesen elvárt eredményt (EO4) megvalósítani, de a személyes interjúk és auditok tudták annyira árnyalni a képet, hogy az egyes érettségi szintekhez tartozó kontrollok meghatározhatók legyenek.	**EO4:** A kutatás eredményeképpen lehetséges az egyes érettségi szintek és a hozzájuk kapcsolódó kontrollok azonosítása.

A kérdőíves minta mérete (122 válaszadó) és a válaszok minősége (volt olyan vizsgálat, mely esetében csak 72 válasz volt figyelembe vehető) miatt statisztikai módszerekkel nem lehetett az előzetesen elvárt eredményt (EO5) megvalósítani, de a személyes interjúk és auditok tudták annyira árnyalni a képet, hogy az egyes érettségi szintekhez kapcsolódó audit bizonyítékok meghatározhatók legyenek.	EO5: A kutatás eredményeképpen lehetséges az egyes érettségi szintek és a hozzájuk kapcsolódó audit bizonyítékok azonosítása.
Mivel a kutatás során megerősítést nyertek a kontrollokra és az audit bizonyítékokra vonatkozó előfeltételezések, emiatt azokat közvetlenül felhasználhatjuk egy ilyen audit ellenőrző lista készítésére.	EO6: Létrehozható egy olyan audit ellenőrző lista, mely lehetővé teszi a szervezeti tudatosság érettségének gyors és valós értékelését egy hagyományos audit környezetben.
NÉHÁNY KIEGÉSZÍTŐ MEGÁLLAPÍTÁS	NÉHÁNY TOVÁBBI ELŐZETES FELTÉTELEZÉS, MELYEK NEM VOLTAK UGYAN A KUTATÁS FÓKUSZÁBAN, DE FIGYELEMRE MÉLTÓ AZ ELMÉLET ÉS A GYAKORLAT ÜTKÖZÉSE
122 db értékelhető kitöltött kérdőív, ami lényegesen kevesebb, mint az előzetes várakozásom volt. Sajnos a szakmai közönség olyan sok kérdőívvel találkozik, hogy egyre kevésbé hajlamos adatforrásként hozzájárulni kutatásokhoz.	EO+ Nagyfokú válaszadói hajlandóságot (legalább 2-300 elemű minta) fog mutatni a kérdőívvel megcélzott szakmai közönség.
Bizonyos esetekben túlértékelt érettségi szintek az egyes szervezeteknél (számos inkonzisztencia = magas vélelmezett érettségi szint kontra alacsony számú azonosított kontroll a szervezetekben)	EO++ Azt vártuk, hogy a magyar mintában nagyjából a SANS Institute által felvázolt és nemzetközi mintán alapuló megoszlást fogunk találni.

3.4 A kutatás jelentősége

Kutatásom segítséget nyújt a

- gyakorló auditoroknak, hogy hatékonyabban tudják felmérni egy szervezetben az információbiztonsági tudatosság érettségi állapotát,
- vállalati szakembereknek, akik keresik azokat a kontrollokat, melyek bevezetése által hatékonyabban lehet növelni a szervezetben az információbiztonsági tudatosságot,
- cégvezetőknek, ha keresik azokat a vezetői eszközöket, melyekkel fokozhatják a szervezet információbiztonsági tudatosságát és ezáltal hatékonyabb ellenőrzést tudnak gyakorolni a szervezet információvagyona felett.

A disszertációban felvázolt kutatás mindhárom érdekelt fél (auditorok, vállalati szakemberek, cégvezetők) számára szolgáltat információkat és közvetlen segítséget nyújt a szervezeti információbiztonsági tudatosság területén. Mivel ez napjaink egyik fontos kihívása, ezért a kutatást hasznosnak vélem a gazdaság minden szereplője számára.

A kutatás során a két nemzetközi szakterületi modell és hozzájuk kapcsolódó nemzetközi és magyar minta összevetése révén lehetővé tette a létező információbiztonsági tudatossági érettségi modellek tovább gondolását, finomítását. Ennek a célnak a teljesülése jól kirajzolódik a kutatási eredményekben is.

Ez a kutatás minden ismert korlátjával együtt legalább három területen járult hozzá a szakterület vizsgálatához:

- A kutatás egyik dimenziója egy már létező nemzetközi modell (Spitzner (2012)) vizsgálata, kiegészítése és finomhangolása volt magyar szervezetek körében
- Egy második dimenzióként egy másik nemzetközi modell (Dzazali és Zolait (2012)) részleges vizsgálatát és elemzését végeztem el egy magyar mintán.
- A kutatás harmadik dimenziója pedig a szervezetekben azonosított kontrollok és audit bizonyítékok, illetve az adott szervezet információbiztonsági tudatosságának érettségi szintje között teremtett kapcsolatot olyan módon, hogy létrehoztam egy gyorstesztet, mely alkalmas egy szervezet információbiztonsági tudatossága érettségi szintjének megállapítására.

4 FŐBB HIVATKOZÁSOK

Babbie, E. (2008): A társadalomtudományi kutatás gyakorlata, Balassi Kiadó, ISBN 978-963-456-000-5

(A fordítás alapjául szolgáló eredeti kiadás: Babbie, E. (2001): The practice of Social Research, 9. kiadás, Wadsworth/Thomson Learning)

Dijkstra, T., K., Henseler, J. (2015): „Consistent Partial Least Squares Path Modeling", MIS Quarterly. Vol. 39. Issue 2. pp. 297-316

Dzazali, S., Zolait, A.H.; (2012): Assessment of information security maturity: An exploration study of Malaysian public service organizations, Journal of Systems and Information Technology, Vol. 14 Iss: 1 pp. 23-57

FISMA (2002): „The Federal Information Security Management Act of 2002"

Fornell, C., K., Larcker, D.,F.; (1981): „Evaluating Structural Equation Models with Unobservable Variables and Measurement Error", Journal of Marketing Research. 18. February. Pp. 39-50

Füstös, L., Tárnok, O. (2017): Strukturális egyenletek modellje – Másodgenerációs statisztikai módszerek. Módszertani füzetek 2017/1 HU ISSN 2062-2473, p 1, p 3, p 18,

GDPR (2016): – General data Protection Regulation - Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.)

GLBA (1999): - The Gramm–Leach–Bliley Act – „Financial Services Modernization Act of 1999"

HIPAA (1996): „The Health Insurance Portability and Accountability Act of 1996"

ISACA (2007): COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models, IT Governance Institute Rolling Meadows, IL 60008 USA, ISACA 2007

ISACA (2012): COBIT Five: A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows, IL 60008 USA, ISACA 2012

ISACA (2018): COBIT2019 Framework: Introduction and Methodology, Schaumburg, IL 60173 USA, ISACA 2018

ISACA (2015): Glossary of terms, Rolling Meadows, IL 60008 USA, ISACA 2015

ISO (2013): ISO 27001 - International Standard ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, 2013, p 5

ISO (2012): ISO 27032 – International Standard ISO/IEC 27032:2012, Information technology -- Security techniques -- Guidelines for cybersecurity, 2012, p 11

ITIL (2013): ITIL Maturity Model, Axelos Global Best Practice, Axelos Limited 2013

Lancaster, C., L., Stillman, D., (2010): The M-Factor: How the Millennial Generation Is Rocking the Workplace, HarperCollins

NIST (2013): NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology, 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930, USA, 2013

Országgyűlés Hivatala (2013): 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Pasquini, A., Galié, E. (2013): „COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process", Proceedings of FIKUSZ '13 Symposium for Young Researchers, pp. 67-76

PCI (2016): PCI DSS - Payment Card Industry Data Security Standard – Requirements and Security Assessment Procedures, Version 3.2 – April 2016

SANS (2015): SANS Securing The Human – SANS Security Awareness Report 2015

SANS (2016): SANS Securing The Human – Awareness is Hard: A Tale of Two Challenges - SANS Security Awareness Report 2016

SANS (2017): SANS Security Awareness – It's time to Communicate – SANS Security Awareness Report 2017

SANS (2018): SANS Building Successful Security Awareness Programs – SANS Security Awareness Report 2018

SANS (2019): SANS The Rising Era of Awareness Training – SANS Security Awareness Report 2019

SOX (2002): The Sarbanes–Oxley Act of 2002 - "Corporate and Auditing Accountability, Responsibility, and Transparency Act of 2002" (H.R. 3763) by Mike Oxley (R-OH) on February 14, 2002

Spitzner, L. (2012): „Security Awareness Maturity Model" SANS Institute, Security Awareness Blog, 22 May 2012 https://securingthehuman.sans.org/blog/2012/05/22/security-awareness-maturity-model (22.12.2017)

Webster, J., Watson, T., R. (2002): Analyzing the Past to prepare for the Future: Writing a Literature Review, MIS Quarterly Vpl. 26 No. 2 / June 2002, p xvi

Yau, H., K., (2014): "Information Security Controls", Advances in Robotics & Automation 2013, Volume 3, Issue 2, p 118

5 PUBLIKÁCIÓK JEGYZÉKE

2020. február

FOLYÓIRATCIKK

(1)

GÁBOR TARJÁN (2017): Some Conceptual Questions on Information Security Awareness
In *SEFBIS JOURNAL NO.11/2017 pp.* 10-17

(2)

GÁBOR TARJÁN (2018): Measuring Organizational Information Security Awareness Levels Supported by a Maturity Model
In *SEFBIS JOURNAL NO.12/2018 pp.* 48-59

KONFERENCIA KÖZLEMÉNY

(3)

TARJÁN GÁBOR (2019): Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben – egy érettségi modell alkalmazása
In OGIK 2018 Válogatott közlemények, pp. 89-92

KONFERENCIA ABSZTRAKT

(4)

TARJÁN GÁBOR (2018): Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben – egy érettségi modell alkalmazása
In OGIK 2018 Az előadások összefoglalói, pp. 62-63

(5)

TARJÁN GÁBOR [2019]: Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben – egy kérdőíves felmérés eredményei
In OGIK 2019 Az előadások összefoglalói, pp. 30-31

EGYÉB (KÖNYVRÉSZLETEK, KÖNYVFEJEZETEK)

(6)

TARJÁN, GÁBOR (2014): 24. ESET - ISO/IEC 27799:2008: INFORMÁCIÓBIZTONSÁGOT ÉLVE VAGY HALVA! IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II. : INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) pp. 130-134.

(7)

TARJÁN, GÁBOR (2014): 9. ESET – ISO/IEC TR 27008:2011: A DICSEKVÉS KOCKÁZATA IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II. : INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) PP. 54-59.

(8)

TARJÁN, GÁBOR (2014): 8. eset - ISO/IEC 27007:2011: A felkészületlen auditoroktól ments meg Uram minket! IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II.: INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) PP. 48-52.

(9)

TARJÁN, GÁBOR (2014): 7.eset - ISO/IEC 27006:2011: Egy jó tanúsító testület mindenhez ért, vagy legalábbis úgy tesz IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II.: INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) PP. 42-46.

(10)

TARJÁN, GÁBOR (2014): 4. eset - ISO/IEC27003:2010: Miért is van szükségünk IBIR-re? IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II.: INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) PP. 24-29.

(11)

TARJÁN, GÁBOR (2014): 3. eset - ISO/IEC27002:2013: Tanácsadót vegyenek! IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II.: INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) PP. 20-23.

(12)

TARJÁN, GÁBOR (2014): 2. eset - ISO/IEC27001:2013: IBIR-t akarok gyorsan és könnyen! IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK II.: INFORMÁCIÓBIZTONSÁG AZ ISO 27000 SZABVÁNYCSALÁD TÜKRÉBEN, BUDAPEST: Hétpecsét Információbiztonsági Egyesület, (2014) PP. 14-18.

(13)

Szabó, Imre; Freidler, Gábor; Dudás, Gábor; Sum, Szabolcs; Szentkuti, Dániel; Csuka, Dénes; Gasparezt, András; Tarján, Gábor; Dósa, Imre; Bujáki, József (2010, 2009); et al. Az informatikai jog nagy kézikönyve, Budapest, Magyarország: Complex Kiadó (2010, 2009) 969 p.

(14)

TARJÁN, GÁBOR (2008): 39. eset - Információs rendszerek auditálásának szempontjai: Belső felülvizsgálat a Super Security Szoftverháznál In: Ködmön, István (szerk.) Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében, Budapest, Magyarország: Hétpecsét Információbiztonsági Egyesület, (2008) pp. 84-85.

(15)

TARJÁN, GÁBOR (2008): 23. eset - Felhasználói felelősségek: Információszivárgás a Személyes Adatok Zrt.-nél In: Ködmön, István (szerk.) Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében, Budapest, Magyarország: Hétpecsét Információbiztonsági Egyesület, (2008) pp. 52-53.

(16)

TARJÁN, GÁBOR (2008): 21. eset - A hozzáférés-ellenőrzéshez fűződő működési követelmény: Hozzáférésellenőrzés-szabályzat az Érzékeny Adatok Zrt.-nél In: Ködmön, István (szerk.) Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében, Budapest, Magyarország: Hétpecsét Információbiztonsági Egyesület, (2008) pp. 48-49.

(17)

TARJÁN, GÁBOR (2008): 14. eset - Védelem a rosszindulatú és mobil kódok ellen: Komplex védekezés a Védett Iroda Kft.-nél In: Ködmön, István (szerk.) Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében, Budapest, Magyarország: Hétpecsét Információbiztonsági Egyesület, (2008) pp. 34-35.

(18)

TARJÁN, GÁBOR (2008): 11. eset - Üzemeltetési eljárások és felelősségi körök: A Krőzus Bankház információbiztonsági szabályzata In: Ködmön, István (szerk.) Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében, Budapest, Magyarország: Hétpecsét Információbiztonsági Egyesület, (2008) pp. 28-29.

(19)

TARJÁN, GÁBOR (2008): 10. ESET - BERENDEZÉSEK VÉDELME: SZERVERSZOBA AZ ÓPERENCIÁS TENGEREN TÚLI ÖNKORMÁNYZATNÁL IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK: INFORMÁCIÓBIZTONSÁG AZ ISO 27001 TÜKRÉBEN, BUDAPEST, MAGYARORSZÁG: HÉTPECSÉT INFORMÁCIÓBIZTONSÁGI EGYESÜLET, (2008) PP. 26-27.

(20)

TARJÁN, GÁBOR (2008): 1. ESET - INFORMÁCIÓBIZTONSÁGI POLITIKA: INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT A SZAKSZERVÍZ KFT.-NÉL IN: KÖDMÖN, ISTVÁN (SZERK.) HÉTPECSÉTES TÖRTÉNETEK: INFORMÁCIÓBIZTONSÁG AZ ISO 27001 TÜKRÉBEN, BUDAPEST, MAGYARORSZÁG: HÉTPECSÉT INFORMÁCIÓBIZTONSÁGI EGYESÜLET, (2008) PP. 8-9.

(21)

TARJÁN, GÁBOR (2008): AZ INFORMÁCIÓBIZTONSÁG IPARÁGI ÉS SZABVÁNY ALAPÚ NEMZETKÖZI KÖVETELMÉNYRENDSZEREI, MAGYAR MINŐSÉG 17: 2 PP. 41-49. (2008)

(221)

TARJÁN, GÁBOR (2001): AZ ÖNKORMÁNYZATI MŰKÖDÉS MINŐSÉGJAVÍTÁSÁNAK KORSZERŰ ESZKÖZEI
MAGYAR MINŐSÉG 10: 9 P. 8 (2001)

(23)

TARJÁN, GÁBOR; TUROPOLI, ESZTER (2001): AZ ISO 9001:2000-ES BEVEZETÉSE A TANÁCSADÓ SZEMSZÖGÉBŐL, MINŐSÉG ÉS MEGBÍZHATÓSÁG 35: 3 PP. 144-147. (2001)

(24)

TARJÁN, GÁBOR (1988): Z-ELMÉLET SZEREPE A JAPÁN VEZETÉSI, SZERVEZÉSI GYAKORLATBAN
VEZETÉSTUDOMÁNY 19 : 6 PP. 37-44. , 8 P. (1988)

(25)

TARJÁN, GÁBOR (1988): JAPÁN GAZDASÁGI SIKEREK A GAZDASÁGI ETIKA TÜKRÉBEN
KÖZGAZDASÁGI SZEMLE 35 : 7-8 PP. 936-946. , 11 P. (1988)