BUDAPESTI CORVINUS EGYETEM

AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN

DOKTORI ÉRTEKEZÉS

Témavezető: Dr. Kő Andrea és Dr. Mitev Ariel Zoltán

TARJÁN GÁBOR

BUDAPEST

2020

TARJÁN GÁBOR

INFORMÁCIÓRENDSZEREK TANSZÉK

TÉMAVEZETŐ: DR. KŐ ANDREA ÉS DR. MITEV ARIEL ZOLTÁN

BUDAPESTI CORVINUS EGYETEM

GAZDASÁGINFORMATIKA DOKTORI ISKOLA

AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN

DOKTORI ÉRTEKEZÉS

TARJÁN GÁBOR

BUDAPEST

2020

KIVONAT

Az információbiztonsági tudatosság minősége, érettsége egy szervezetben létfontosságú, hiszen ez határozza meg azt, hogy a szervezet mennyire hatékonyan tudja védeni információs vagyonát.

Az értekezés áttekinti az információbiztonsági tudatosság fogalmát a szakirodalom tükrében és ajánl egy olyan fogalmi meghatározást, mely alapul szolgálhat egy mérési modell kidolgozáshoz. Az értekezésben megvizsgálom azt a mérési problémát, mellyel akkor szembesülünk, amikor ennek a tudatosságnak a minőségét (érettségét) szeretnénk szervezeti szinten mérni.

A szervezeti szintű mérést leginkább az érettségi modellek támogatják, ezért átfogóan bemutatom ezek világát, és végül felvázolok egy az információbiztonsági tudatosság mérésére alkalmas érettségi modellt, mely szervezeti szinten képes jellemezni az adott szervezet információbiztonsági tudatosságának érettségét.

A létrehozott modell használhatóságát tesztelendő, elvégeztem egy három pilléren nyugvó primer kutatást:

- Klasszikus kérdőíves megkérdezéssel vizsgáltam magyarországi szervezetek információbiztonsági tudatosságának érettségi szintjét úgy, hogy közben két nemzetközi szakirodalomban fellehető modell (Dzazali-Zolait, illetve Spitzner) által szolgáltatott eredményekkel is összevetettem az általam kapott eredményeket,
- Strukturált interjúkat folytattam információbiztonsági szak-auditorokkal és információbiztonsági vezetőkkel,
- Helyszíni auditokon értékeltem szervezetek információbiztonsági gyakorlatát, tudatosságát és érettségi szintjét.

A tapasztalatok összegzése nyomán javaslatokat fogalmaztam meg az érettségi modell alkalmazására és létrehoztam egy olyan kontroll készletet és audit-bizonyíték listát, melyek használatával fejleszthető egy szervezet információbiztonsági tudatosságának érettségi szintje, illetve könnyebben értékelhetővé válik egy szervezet ezirányú tevékenysége, erőfeszítései.

TARTALOMJEGYZÉK

Ábrajegyzék

TÁBLÁZATOK JEGYZÉKE

1 BEVEZETÉS

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. 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 információbiztonsági 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 Problémafelvetés

A kutatás a szervezeti információbiztonsági tudatosság érettségi szintjének meghatározására, mérésére és fejlesztésre irányult.

A kutatás viszonylag korai szakaszában kiderült, hogy bár bőséges az információbiztonsági tudatosság irodalma, de

- nincs szakmai konszenzus az információbiztonsági tudatosság fogalma kapcsán,

- hiányzik a részleteiben kidolgozott mérési, értékelési modell, mely alkalmas lenne a szervezetek besorolására érettségük szempontjából,
- nem, vagy csak részleteiben ismert a kapcsolat az egyes bevezetett szervezeti kontrollok és az információbiztonsági tudatosság állapota, érettsége között.

Ha birtokában lennénk egy konzisztens értékelő modellnek és megbízhatóan tudnánk nyilatkozni az egyes szervezetek információbiztonsági tudatosságának szintjéről, akkor lehetséges lenne megbízható információkkal kiszolgálni a szervezetek menedzsmentjét.

Ha mindezt meg tudnánk támogatni a tennivalók listájával is (a szervezetek számára rendelkezésre álló védelmi intézkedések, melyek növelik a tudatosságot), akkor igazán sokat tehetünk a szervezetek információbiztonsági állapotának javításért.

Mindez még megfejelhető olyan audit bizonyítékok listájával is, mely a klasszikus audit szituációt támogatná: viszonylag gyorsan, egyszerűen és egyértelműen megmondhatóvá tehető általa, hogy egy vizsgált szervezet milyen helyzetet foglal el egy képzeletbeli skálán, és mit kell azért tennie, hogy egy következő audit eseményen fejlődést tudjon prezentálni.

1.2 A kutatás célja

A kutatás 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.

Különös hangsúlyt fektettem a nemzetközi összevetésre, hogy lássam, mennyiben igazolhatók vissza a nemzetközi trendek és tendenciák, hol van esetleg markáns különbség a hazai és a nemzetközi gyakorlat között.

A kutatástól várt eredmények:

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
EO6:	AZ ÖSSZEFÜGGÉSEK FELTÁRÁSA AZ EGYES KONTROLLOK ÉS AUDIT BIZONYÍTÉKOK, ILLETVE A SZERVEZET INFORMÁCIÓBIZTONSÁGI TUDATOSSÁGÁNAK ÉRETTSÉGI SZINTJE KÖZÖTT

1.3 A kutatás alapjai

A kutatás céljai, a kutatási kérdések, a kutatási modellünk, egy kutatásmódszertani összefoglaló és a kutatási eredmények rövid összefoglalója került ebbe a fejezetbe, mely a kutatás egészét hivatott „madártávlatból" áttekinteni.

1.3.1 Kutatási irányok, célok és részcélok

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

A fő kutatási cél szorosan kapcsolódik ahhoz a problémakörhöz, amit az előző alfejezetben fogalmaztam meg.

Az alábbi kutatási részcélok pedig az alapcélt bontják le kisebb és logikailag jól összekapcsolható és könnyebben vizsgálható gondolati egységekre:

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

A kutatási célok tükrében megfogalmazhatók a konkrét kutatási kérdések.

1.3.2 A kutatási kérdések

A várt kutatási eredmények és a kapcsolódó kutatási célok tükrében a következő kutatási kérdésekre fókuszálok:

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)?

1.3.3 A KUTATÁSI MEGKÖZELÍTÉS

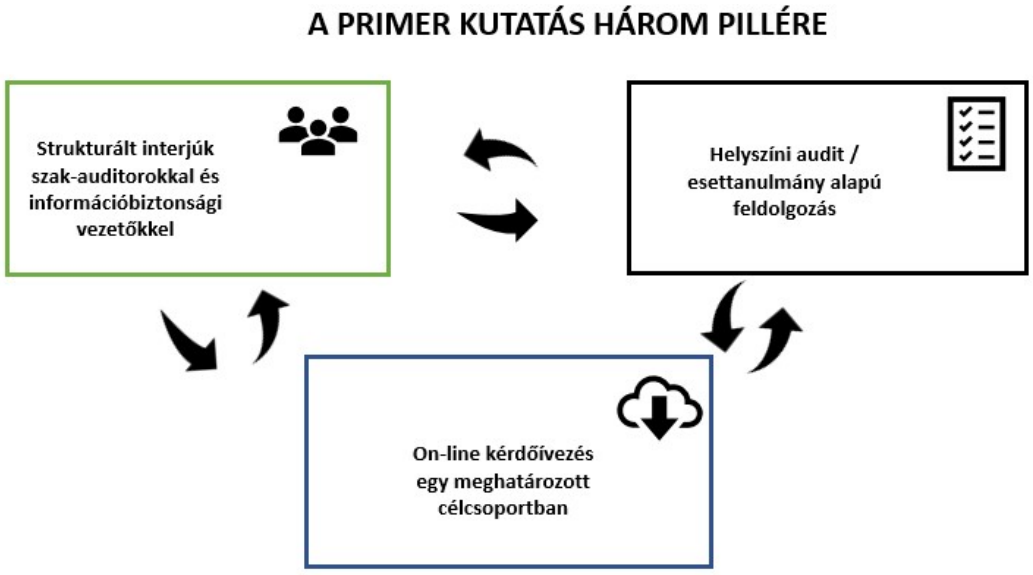
Kutatásom során egy kevert kutatásmódszertani megközelítést használtam: A kvantitatív kutatást támogatta egy alapvetően kérdőíves megkérdezés, melyet jól kiegészített néhány kvalitatív elem, pl. a szakauditorokkal folytatott interjúk és az esettanulmány (helyszíni audit) alapú feldolgozás.

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.

1.3.4 Kutatásmódszertani összefoglaló

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. Az egyes általam használt fogalmakat egymásra épülésük logikája mentén vizsgáltam az alábbi sorrendben:

- Információbiztonság
- Tudatosság
- Információbiztonsági tudatosság
- Az információbiztonsági tudatosságra ható kontrollok
- A tudatosság és az érettség mérési problémája
- Az érettségi modellek, mint „mérő" eszközök
- Strukturális egyenletek modelljei (SEM), mint a vizsgálat egyik kiemelt eszköze

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.

1.3.5 A kutatási eredmények összefoglalója

Mivel a kutatás alapcélja az volt, hogy kapcsolatokat mutassak ki a szervezetekben bevezetett és működő bizonyos kontrollok és a szervezet információbiztonsági tudatosságának érettségi szintje között, ezért a kutatás egyik alcélja (RO1) az lett, hogy első lépésben ezeket a kontrollokat próbáljam meg azonosítani, majd a következő kutatási lépésben kapcsoljam össze ezeket a kontrollokat az egyes érettségi szintekkel.

Hasonló logika mentén egy másik kutatási cél (RO2) lett az, hogy azonosítsam azokat az audit bizonyítékokat is, melyek jellemzők lehetnek az információbiztonsági tudatosságra a szervezetekben, majd a következő lépésben ezeket próbáljam meg összekötni az egyes érettségi szintekkel.

A nemzetközi kitekintés és a modell erősítése érdekében egy újabb kutatási alcél (RO3) az lett, hogy megtaláljam azokat a nemzetközi érettségi modelleket és a kapcsolódó kutatásokat, melyek alkalmasak lehetnek modellem igazolására.

Ebből a három kutatási alcélból pedig levezethető a negyedik alcél (RO4), mely arra irányul, hogy azonosítsam egyértelműen azokat a tényezőket, melyek képesek erősíteni a szervezeti tudatosságot, tehát egy menedzsment számára a napi gyakorlat nyelvére lefordítható intézkedéseket határozhat meg.

Az egyes kutatási célokhoz kötődően a disszertáció az alábbi eredményeket tartalmazza:

RO1: MELY KONTROLLOK JELLEMZIK AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG MAGASABB EGYES SZINTJEIT KÉPVISELŐ SZERVEZETEKET?

>> A témakört tárgyaló fejezet:

Mind a kérdőívek mind a szakértői interjúk megmutatták, hogy mely kontrollok jellemzik az egyes érettségi szinteket. Ezeket a tapasztalatokat a 4.1 és 4.2 fejezetek tárgyalják.

RO2: MILYEN AUDIT BIZONYÍTÉKOK TÁMASZTJÁK ALÁ AZ EGYES SZERVEZETEK INFORMÁCIÓBIZTONSÁGI TUDATOSSÁGÁNAK ÉRETTSÉGÉT?

>> A témakört tárgyaló fejezet:

Az audit bizonyítékok esetében hasonló képet tártunk fel, mint a kontrollok vizsgálatánál. A válaszadók egyértelműen összekapcsolták az audit bizonyítékokat a kontrollokkal és ilyen módon is igazolták a felállított modell használhatóságát. A 4.1.4.3 fejezet mutatja be a vizsgálati eredményeket.

RO3: MILYEN MÓDON HASZNÁLHATÓK FEL NEMZETKÖZI KUTATÁSOKBAN BEMUTATOTT ÉRETTSÉGI MODELLEK A MAGYARORSZÁGI SZERVEZETEK JELLEMZÉSÉRE?

>> A témakört tárgyaló fejezet:

Mindkét vizsgált nemzetközi modell használhatónak, értelmezhetőnek bizonyult a magyarországi szervezetek vonatkozásában és a kapott eredmények - néhány attribútum kivételével - igazodnak a nemzetközi vizsgálat eredményeihez. Az értekezés 4.1.2 és 4.1.3 fejezetei tárgyalják a témakört.

RO4: MILYEN TÉNYEZŐKTŐL FÜGG EGY SZERVEZET INFORMÁCIÓBIZTONSÁGI TUDATOSSÁGÁNAK ÉRETTSÉGE?

>> A témakört tárgyaló fejezet:

A vizsgálatból egyértelműen kiderült, hogy mely kontrollok léte vagy nemléte van befolyással egy szervezet tudatosságának érettségére. A 4. fejezet tárgyalja azokat az azonosított kulcselemeket, melyek tényleges hatással vannak erre.

A kutatási célokat elemezhető kutatási kérdésekre bontottuk le a fejezet korábbi részében. A már korábban említett kutatási kérdésekre született válaszokat a disszertáció következő fejezeteiben tárgyalom:

RQ1: HOGYAN ÍRHATÓ LE, HOGYAN ÉRTÉKELHETŐ A SZERVEZETEKBEN AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG SZINTJE, MINŐSÉGE A SZERVEZET SZINTJÉN?

>> A megoldás:

Egy saját érettségi modell kidolgozása egy lehetséges válasz a mérési problémára. Ezt mutatja be részleteiben a 2.5 fejezet.

RQ2: HOGYAN ÍRHATÓ LE, HOGYAN ÉRTÉKELHETŐ A GAZDÁLKODÓ SZERVEZETEKBEN AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG SZINTJE, MINŐSÉGE A SZERVEZET SZINTJÉN?

>> A megoldás:

A bemutatott saját érettségi modell alkalmas arra, hogy egy ötfokozatú skálán viszonylag nagy megbízhatósággal bemutassa, értékelhetővé tegye az adott szervezett érettségi szintjét. Ezt az értekezés 4. fejezete tárgyalja.

RQ3: MÉRHETŐ-E A VÁLTOZÁS (JAVULÁS, ROMLÁS) EGY SZERVEZET ÉLETÉBEN A TUDATOSSÁG ÉRETTSÉGI SZINTJE VONATKOZÁSÁBAN?

>> A megoldás:

Erre nézve sajnos a kutatás nem szolgáltatott elegendő bizonyítékot a vizsgálat időhorizontja miatt: A változásokhoz (pl. szintlépéshez az érettségi modellben) több év is szükséges lehet, ugyanakkor a primer kutatás legfontosabb eleme, a kérdőívezés, egy nagyjából tizenkéthónapos időszakot ölelt fel, amely nem alkalmas ilyen változások érzékelésére. A kutatás egyik jövőbeli iránya lehet a kérdőíves vizsgálat megismétlése egy-másfél év elteltével, bár az anonim kitöltés miatt ekkor sem feltétlenül lennének beazonosíthatók a fejlődést vagy romlást mutató szervezetek. Ezt a problémát és a lehetséges utakat tárgyalja az 5.7 fejezet.

RQ4: ÖSSZEHASONLÍTHATÓK-E A GAZDÁLKODÓ SZERVEZETEK AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGE SZEMPONTJÁBÓL SZERVEZETI SZINTEN?

>> A megoldás:

Az összehasonlíthatóságnak statisztikai bizonyítékai is keletkeztek (lásd. 4.1 fejezet), mert a mintanagyság elérte azt a szükséges méretet, amely mellett minden érettségi fokozathoz kellő számú megfigyelés kapcsolódott és a megfigyelések igazolták azt a feltételezést, hogy az egyes érettségi szintekhez meghatározhatók azok a jellemző kontrollok és audit bizonyítékok, melyek az összehasonlíthatóságot támogatják.

RQ5: TÁMOGATHATÓ-E A TUDATOSSÁG ÉRTÉKELÉS HAGYOMÁNYOS AUDIT ESZKÖZÖKKEL (PL. ELLENŐRZŐ LISTÁK)?

>> A megoldás:

Mivel a részleteiben kidolgozott érettségi modellben igyekeztem felsorolás-szerűen összeszedni az adott érettségi szintre jellemző kontrollokat és audit bizonyítékokat, majd aztán a kérdőív kitöltőitől, illetve az interjú alanyoktól azt kértem, hogy jelezzék, számukra mely kontrollok és audit bizonyítékok mely érettségi szintekhez köthetők. A tőlük nyert válaszok viszonylag erős megbízhatósággal igazolták előfeltételezéseimet.

A kutatás korai szakaszában meghatároztam, hogy milyen eredményeket várok a kutatási program következetes végrehajtásától. Figyelembe vettem a szakterület sajátosságait, jómagam beágyazottságát az auditori szakmában, és a sokéves gyakorlati tapasztalatot. Az ezek tükrében megfogalmazott és előzetesen várt kutatási eredmények:

EO1: A TÁRGYKÖRBEN HOZZÁFÉRHETŐ SZAKIRODALOM EGYÉRTELMŰ ÉS KÖVETKEZETES FOGALOMHASZNÁLAT MELLETT PONTOSAN LEÍRJA AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG FOGALMÁT.

> A kutatás eredménye:

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.

EO2: A KUTATÁS SORÁN SIKERÜL AZONOSÍTANI OLYAN ÉRETTSÉGI MODELLT, MELY ALKALMAS A SZERVEZETEK INFORMÁCIÓBIZTONSÁGI TUDATOSSÁGÁNAK ÉRETTSÉGÉT ÉRTÉKELNI ÉS MÉRNI.

> A kutatás eredménye:

A Spitzner (2012) féle modell mögött sokéves tapasztalat húzódik, és egy jelentős nemzetközi adatbázis hozzáférhető a szervezetek önértékelési eredményeiről. Ezt taglalja az értekezés 2.4.3.5 alfejezete. Spitzner mellett még egy kutatás eredményei voltak beforgathatók a nemzetközi összevetésbe: Dzazali és Zolait (2012) modelljét is lehetett részben összevetni hazai megfigyelésekkel. (Lásd 2.6.1 fejezet!)

EO3: A KUTATÁS KAPCSÁN LEHETSÉGES OLYAN HAZAI ADATFELVÉTELEZÉST VÉGEZNI, MELY ALAPJÁN A HAZAI ÉS NEMZETKÖZI ADATOK ÖSSZEVETHETŐK.

> A kutatás eredménye:

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 okozott: A vártnál lényegesen rosszabb válaszadói hajlandóság miatt a kérdőíves vizsgálat

elhúzódott és jelentős erőfeszítéseket igényelt. Ennek részleteit a 4.1 fejezet tárgyalja.

EO4: A KUTATÁS EREDMÉNYEKÉPPEN LEHETSÉGES AZ EGYES ÉRETTSÉGI SZINTEK ÉS A HOZZÁJUK KAPCSOLÓDÓ KONTROLLOK AZONOSÍTÁSA.

> A kutatás eredménye:

Mind a kérdőíves mind a személyes interjús adatgyűjtés során jól meghatározhatóvá váltak azok a kontrollok, melyek az egyes érettségi szinteket jellemzik.

EO5: A KUTATÁS EREDMÉNYEKÉPPEN LEHETSÉGES AZ EGYES ÉRETTSÉGI SZINTEK ÉS A HOZZÁJUK KAPCSOLÓDÓ AUDIT BIZONYÍTÉKOK AZONOSÍTÁSA.

> A kutatás eredménye:

A kérdőíves és a személyes interjús adatgyűjtés is azt mutatta, hogy az audit bizonyítékok jól hozzárendelhetők az egyes érettségi szintekhez.

EO6: LÉTREHOZHATÓ EGY OLYAN AUDIT ELLENŐRZŐ LISTA, MELY LEHETŐVÉ TESZI A SZERVEZETI TUDATOSSÁG ÉRETTSÉGÉNEK GYORS ÉS VALÓS ÉRTÉKELÉSÉT EGY HAGYOMÁNYOS AUDIT KÖRNYEZETBEN.

> A kutatás eredménye:

Mivel a kutatás során megerősítést nyertek a kontrollokra és az audit bizonyítékokra vonatkozó előfeltételezések, emiatt azokat közvetlenül felhasználhatjuk egy ilyen audit ellenőrző lista készítésére.

A kutatás általános természetéből következően nem minden elvárásom és előfeltételezésem teljesült. Ennek részleteit az 5.6 fejezet tárgyalja.

1.3.6 AZ ÉRTEKEZÉS KORLÁTAI

A tanulmány koncepciója és módszertani megközelítése is egyértelmű korlátok mentén alakult ki:

- Ugyan nem végeztem primer kutatást nemzetközi szinten, de két nemzetközi kutatás eredményeit összevetettük a magyarországi helyzettel:
  - Dzazali és Zolait (2012) modelljét részlegesen teszteltem a kérdőíves megkérdezés során,
  - Spitzner (2012) modelljét a maga teljességében vizsgáltam a magyar mintán.
- Dzazali és Zolait (2012) modelljének azon komponenseit nem vettem figyelembe, melyeket az általuk bemutatott kutatás is jelentéktelennek vagy alacsony hatásúnak mért.
- Spitzner (2012) modelljét sem változtatás nélkül használtam: Két dimenzióval (tudás és attitűd) kiegészítettem a saját modellemben (lásd 2.5 fejezet).

Az értekezésben leírt kutatás korlátos volta több szempontból is ismert és tudatosan vállalt:

- A szakterület önmagában annyira rétegzett (lásd pl. alapfogalmak szintjén az informatikai biztonság, információbiztonság, adatbiztonság, adatvédelem, kiberbiztonság, kibervédelem fogalmi keveredését!), hogy a teljeskörűségnek még csak a kisélete sem merülhet fel.

- Az alkalmazhatónak vélt érettségi modellek méréselméleti (skálaelméleti) korlátokat hordoznak: Jellemzően egy sorrendi skálán kell olyan műveleteket végzeni (pl. átlagszámítás), melyek az adott skálához nem, vagy csak erős korlátozó feltételekkel illeszkednek.
- A kidolgozott modell validálására első lépésben csak magyar vagy Magyarországon működő szervezetek körben került sor. Ha a modell beváltja a hozzáfűzött reményeket, akkor sor kerülhet nemzetközi kipróbálására is.
- A kutatás során nem végzünk ún. „action research" jellegű tevékenységet, azaz nem állapítottuk meg egy vagy több konkrét szervezet induló érettségi szintjét és majd pl. tanácsadási projekten keresztül nem javítottuk információbiztonsági tudatossági teljesítményét, és aztán értelemszerűen nem végzünk visszamérést egy hosszabb időtávon.

Mindezeket a korlátokat felismerve és vállalva, igyekeztem a kutatás megközelítési módját és módszertani elemeit úgy összehangolni, hogy az eredmények hitelessége és bemutathatósága ne szenvedjen csorbát.

1.4 Köszönetnyilvánítás

Mindenekelőtt szeretnék köszönetet mondani Dr. Kő Andreának, és Dr. Mitev Ariel Zoltán témavezetőimnek, akik nagy türelemmel és bölcsességgel irányították kutatásomat és a nehéznek tűnő pillanatokban egy-egy ötlettel rendszeresen átlendítettek a módszertani és szervezési problémákon.

Végezetül, de nem utoljára köszönöm a családomnak, hogy támogató magatartásukkal segítették a doktori tanulmányok és a kutatás előrehaladását.

1.5 Az értekezés szerkezete

Az értekezés további részeinek áttekintő szerkezete:

- A *2. fejezet* tartalmaz egy bővebb szakirodalmi áttekintést a kutatás tárgyában, illetve a szakirodalomból leszűrt tapasztalatok alapján bemutatom azt a továbbfejlesztett érettségi modellt, melynek a gyakorlati validálásával kapcsolatos eredményeket a 3. fejezetben ismertetem.
- A *3. fejezetben* beszélek a módszertani választásaimról is, illetve bemutatom az egyes kutatási pillérek mentén gyűjtött tapasztalatokat.
- A *4. fejezet* tárgyalja az elvégzett gyakorlati (primer) kutatás eredményeit.
- Az *5. fejezet* olyan következtetéseket és összefoglaló gondolatokat tárgyal, melyek a 3. és 4. fejezet eredményeiből következnek. Ebben a fejezetben fogalmaztam meg azokat a további kutatási kérdéseket és irányokat, melyek a kutatás továbbvitelét segítik, segíthetik.
- Az értekezés végén a mellékleteket és a hivatkozásokat listáztam.

2 SZAKIRODALMI ÁTTEKINTÉS – A SZEKUNDER KUTATÁS EREDMÉNYEI

Az értekezés elméleti megalapozása érdekében egy átfogó elemzést végeztem a szakterületen. Az egyes általam használt fogalmakat egymásra építve tárgyalom a szakirodalom tükrében:

- Információbiztonság: A szakirodalom tükrében milyen társfogalmakkal (pl. adatbiztonság, kiberbiztonság, adatvédelem, IT biztonság stb.) együtt értelmezhető ez a fogalom?
- Tudatosság: Mit gondolunk erről a fogalomról általában?
- Információbiztonsági tudatosság: A két fogalom összekapcsolásával milyen tartalom hozható létre és ebből létrehozhatunk-e a gyakorlati kutatás során használható saját definíciót?
- Az információbiztonsági tudatosságra ható kontrollok: Az információbiztonsági tudatosság milyen kontrollok bevezetésével, működtetésével fokozható?
- A mérési probléma: Az objektív mérést támogató és ellehetetlenítő tényezők hogyan foglalhatók össze?
- Az érettségi modellek: Alkalmasak-e az ún. érettségi modellek a mérési probléma kezelésére, és alkotható-e olyan részletes modell, mely a gyakorlati kutatás alapját képezheti?
- Strukturális egyenletek modelljei: Milyen matematikai apparátussal vizsgálható egy érettségi modellben megjelenő tényező (pl. egy kontroll vagy audit bizonyíték és annak hatása) az érettségi szintre?

2.1 A szakirodalmi kutatás módszertana

Ebben az alfejezetben a szakirodalmi kutatás logikáját és végrehajtási módját mutatom be.

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.

Megfogadva Webster és Watson (2002) tanácsát, egy háromlépéses megközelítésben tártam fel a további jelentősebb szakirodalmi forrásokat:

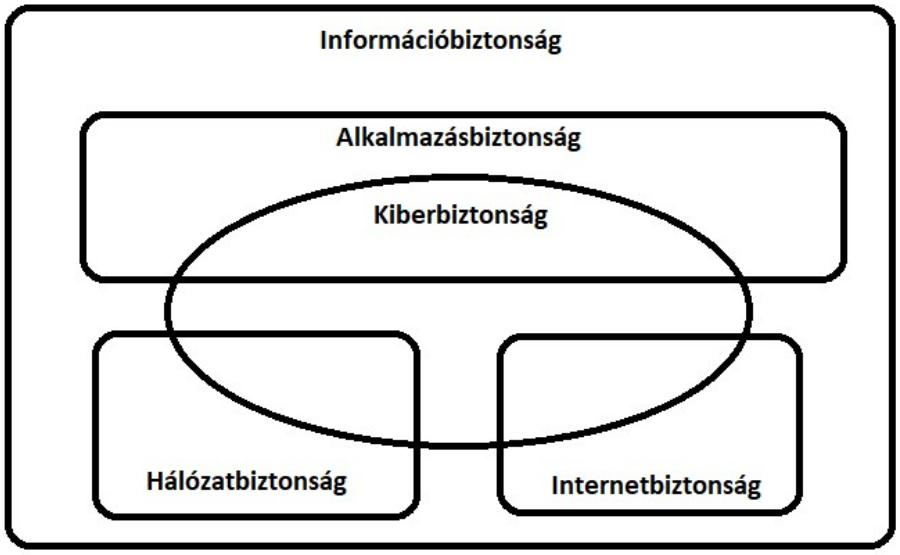
1. Azonosítottam a szakterület jelentősebb folyóiratait és bennük a jelentősebb szerzőket, illetve intézményeiket. A hazai szakértőket, véleményvezéreket személyesen is ismerve, a magyar nyelvű irodalmak azonosítása viszonylag könnyen ment, és a nemzetközileg jelentős szerzőkhöz és intézményekhez (pl. SANS Institute és Spitzner) is rajtuk keresztül vezetett az út.
2. Az így megtalált kulcs-szakirodalmak hivatkozásjegyzékét *időben visszafelé* követve számos értékes és klasszikusnak minősített irodalmi forrást találtam.
3. A korábban azonosított kulcs-szakirodalmak esetében alkalmaztam az *időben előrefelé* ható keresést is, azaz azt néztem meg, hogy ezekre a kulcs-szakirodalmakra milyen gyakorisággal hivatkoznak a viszonylag friss szakcikkek, hogy értékelni tudjam a korábbi azonosítási tevékenységem hatásosságát.

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 Az információbiztonsági tudatosság fogalmi keretei

Az információbiztonsági tudatosság fogalma meglehetősen összetett és komplex kérdéskör a szakirodalom tükrében. A következőkben kísérletet teszünk a fogalom pontosabb meghatározására, hogy a modellalkotási tevékenységünk szilárdabb alapokra kerüljön.

A köznapi és a szaknyelvben is nagyon keverednek az információbiztonsággal kapcsolatos fogalmak. Jogi megközelítésben hallhatunk adatbiztonságról, adatvédelemről, az internet világában jártas szerzők internetbiztonságról, kiberbiztonságról beszélnek, az informatikusok előszeretettel használják az informatikai biztonság vagy IT biztonság szavakat. Ha pedig valaki hálózati mérnökként dolgozik, akkor előszeretettel beszél hálózatbiztonságról, illetve a szoftverfejlesztők szívesen emlegetnek alkalmazásbiztonsági kihívásokat. Szükséges ebben a fogalmi dzsungelben némi rendet raknunk, és ezt a célt szolgálja a következő ábra.



2. *ábra: A fogalmak egymásra épülésének rendszere (saját ábra, készült az ISO/IEC 27032:2012 szabvány 11. oldalán található hasonló tartalmú ábra nyomán)*

Az ábra üzenete egyértelmű: Az értekezés az információbiztonság fogalmát a lehető legszélesebb értelmezésben használja és a szervezet egészére ható tulajdonságként és tevékenységhalmazként határozza meg.

2.2.1 Az információbiztonság

Az információbiztonság alatt általában az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzési képességét értjük, mely kiegészülhet további olyan egyéb tulajdonságokkal, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság.

Az információbiztonság három alapdimenziójának általánosan elfogadott értelmezése több szerző és szakmai anyag (Molnár és Kő (2009), Muha (2008), 2013. évi L. törvény (2013)) nyomán:

- *Bizalmasság*, annak biztosítása, hogy az információ csak az arra felhatalmazottak számára legyen elérhető.
- *Sértetlenség (integritás)*, az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése olyan módon, hogy illetéktelen ne tudjon kontroll nélkül változásokat eszközölni sem az információk halmazában, sem pedig feldolgozási módszereikben.
- *Rendelkezésre állás*, annak biztosítása, hogy a felhatalmazott felhasználók mindig hozzáférjenek az információkhoz és a kapcsolódó értékekhez, amikor az szükséges számukra az információfeldolgozási folyamatban.

Ezt a három egyenrangú dimenziót szokták még további kiegészítő jellemzőkkel (pl. számon-kérhetőség, letagadhatatlanság stb.) körül írni.

2.2.2 A TUDATOSSÁG

A tudatosság fogalmát az ISACA Glossary of Terms (2015) a következőképpen határozza meg:

„Értesültnek lenni, figyelembe venni, tudatosnak és jól informáltnak lenni egy olyan szakmai tárgykörben, mely magába foglalja az adott témakör tudását és megértését és az annak megfelelő cselekvést." *("Being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly.")*

Ez a definíció tartalmaz néhány fontos kiegészítő gondolatot:

- Valaminek a tudásáról és külön a megértéséről beszél, azaz különbséget tesz egy tárgykörhöz kapcsolódó betanítás (training) és a képzés (education) között, ahol
    - a betanítás alatt annyit értünk, hogy az emberek azt tanulják meg, hogy mit és hogyan kell végrehajtani,
    - a képzés pedig arra fókuszál, hogy elmondja az embereknek, hogy valamely intézkedésnek mi az értelme, és még a tennivaló egyéb kontextusát is feltárja.
- A tudatosság feltételezi, hogy a szabályokat nem csak azért követik, mert ismertek az egyének előtt, hanem azért, mert megértették, hogy miért fontos úgy cselekedni, ahogy elő van írva.

Ez a megközelítés segít nekünk arra rájönni, hogy milyen tartalmakat és milyen módon érdemes kommunikálni, ha aktív részvételt akarunk elérni az információbiztonsági tudatossággal kapcsolatos tevékenységekben.

2.2.3 AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG

Lebek (2014) és szerzőtársai egy elmélet-alapú irodalmi áttekintést végeztek el az információbiztonsági tudatosság és magatartás témakörében. 10 adatbázist és 113 publikációt vizsgáltak át 2014-ben mintegy 10 éves visszatekintéssel. A hivatkozott cikkükben 54 használt elméletet sorolnak fel, de ezek közül csak négyre mondják azt, hogy azok alkalmazottak a gyakorlatban elsődlegesen:

- Theory of Planned Behaviour (TPB) – A tervezett viselkedés elmélete
- General Deterrence Theory (GDT) – Az általános elrettentés elmélete
- Protection Motivation Theory (PMT) – A védelmi motivációs elmélet
- Technology Acceptance Model (TAM) – A technológia elfogadási modell

A tanulmány az elméletek két fő típusát különbözteti meg:

- A viselkedési elméletek
- A tanulási elméletek

A négy elsődlegesen használt elmélet (TPB, GDT, PMT, TAM) alapvetően a viselkedési elméletek közé sorolandók. Mindegyik ugyanazt a kérdést közelíti meg különböző nézőpontokból: Az alkalmazottak miért akarnak megfelelni a cégük információbiztonsági szabályzatának?

Ez a tanulmány egy nagyon széles áttekintést nyújt egy viszonylag szűken értelmezett információbiztonsági tudatossági fogalom mentén: az alkalmazottak kikényszerített információbiztonsági megfelelősége alapján. A tanulmány nem foglalkozik az alkalmazottakon túli érdekelt felekkel (pl. ügyfelek, menedzsment, állam stb.) pedig a szervezet információbiztonsági tudatosságához ezek a partnerek is jelentős mértékben hozzájárulnak.

Parsons és szerzőtársai (2013) az információbiztonságnak egy nagyon számítógép fókuszú nézetét írják le. Ez a megközelítés sokkal inkább foglalkozik IT biztonsággal, mint általános információbiztonsági tudatossággal. Az információbiztonsági tudatosság fókusz területei ebben a tanulmányban a következők:

- Jelszómenedzsment
- Email használat
- Internet használat
- Közösségi hálózatok használata
- Incidensek jelentése
- Mobil számítástechnika
- Információkezelés

Ez a lista jórészt számítógéphez köthető ügyekkel foglalkozik, ugyanakkor az információbiztonság számos egyéb fontos aspektusa hiányzik belőle. Néhány ilyen fontosabb hiányzó témakör Parsons információbiztonsági tudatossági területeiből:

- Adminisztratív kontrollok (írott szabályok és adatosztályozási elvek ismerete és betartása a vonatkozó joganyag ismeretében)
- A fizikai formában létező média kezelése (az információ hagyományos reprezentációja – papírok, dokumentumok, termékminták stb.)
- Az elvárt viselkedés és információbiztonsági szabályok az otthoni munkavégzés és utazás során
- Látogatók fogadása a cég telephelyén
- Az ún. „tiszta asztal" politika

Természetesen ez a lista sem teljeskörű, hanem csak megmutatja az információbiztonsági tudatosság egyéb vonatkozásait is.

Nemeslaki és Sasvári (2015) az információbiztonsági tudatosság gyakorlati vizsgálatát végezte el magyarországi üzleti és közszolgálati szférájában. 300 főt kérdeztek meg és az információbiztonsági tudatosságot a következőképpen definiálták: „egy munkavállaló általános tudása az információbiztonságról és az információbiztonsági szabályzat tudomásul vétele a szervezetben" *(„an employee's general knowledge about information security and his cognizance of the information security policy in the organization.")*

Az ebben a cikkben hivatkozott információbiztonsági tudatosság fogalma Bulgarcu-tól (2010) és szerzőtársaitól származik.

Ez az interpretáció megint szűkíti a fogalmat, mert csak alkalmazottakról beszél, habár vannak más érdekelt felek a szervezet körül (pl. ügynökök, ügyfelek stb.), akiknek lehet komoly hatása az információbiztonsági tudatosság állapotára. A tudomásul vétel pedig az észlelés és elfogadás különleges fajtájaként fogható fel és természetét tekintve passzív megközelítést hordoz. Az információbiztonsági tudatosság jó (érett) szintje feltételez egy poraktív hozzáállást minden érdekelt fél részéről, és emiatt a hivatkozott definíció nem felel meg az elvárásainknak.

Sasvári és szerzőtársai (2015) egy gyakorlati felmérést végeztek osztrák és magyar vállalkozások körében. Néhány nagyon érdekes észrevételt tettek az információbiztonsági tudatosság szintjének különbözőségeivel kapcsolatban a cégméret függvényében, de a mi nézőpontunkból még érdekesebb az általuk használt információbiztonsági tudatossági modell. Az információbiztonsági tudatosság három dimenzióját említik:

- A szervezeti dimenzió, ahol a szervezeti szokásokat és eljárásokat mérik.
- Az infrastrukturális dimenzió, melybe a szervezet környezeti és informatikai állapotát értik bele.
- Az egyéni dimenzió, ahol az általános szervezeti tudást és munkavégzési szokásokat mérik és elemzik.

A szervezeti dimenzióba értik bele az információbiztonsági tudatosság irányítási részét (különösen az információbiztonsági vezető szerepére, a munkaköri leírásokra, és egyéb meghatározott szerepekre fókuszálva). Az egyéni dimenzió foglalkozik a munkavállalókkal, mint egyénekkel, és erősen az információbiztonsági incidensek kezelésére fókuszál.

Az infrastrukturális dimenzió képviseli azokat a személyeket, akik működtetik az infrastruktúrát és biztosítják az információ áramlását, valamint az információbiztonsággal kapcsolatos tevékenységeket végzik.

Ez a háromdimenziós megközelítés megfelel a hivatkozott kutatók céljainak, de nem teljes mértékben teljesítik elvárásaimat: Ez az információbiztonsági tudatosság modell minden dimenziójában vezetőkről és munkavállalókról beszél és emiatt ez az interpretáció is túl szűk, hiszen nem fed le minden érdekelt felet.

Maqousi (2013) és szerzőtársai az információbiztonsági tudatosság egy folyamatorientált nézetéről beszélnek: „Az információbiztonsági tudatosság egy olyan folyamatos tanulási folyamat, melynek értelme van a fogadó fél számára és mérhető hasznot hajt a szervezetnek a tartós viselkedésváltozáson keresztül." *("Information security awareness is an ongoing process of learning that is meaningful to recipients and delivers measurable benefits to the organization from lasting behavioural change.")* Ez a megközelítés új dimenziókat nyit a fogalom meghatározásában:

- Megjelenik a folyamatosság a tevékenységben,
- Egy folyamat alapú nézőpontot képvisel,
- A tanulás és annak képessége egy kulcsmomentum,
- És hosszútávú változásokat tételez fel a viselkedésben.

Nehéz vitatkozni ezekkel mondatokkal, de ez a lista csak színezi az információbiztonsági tudatosságról rajzolt képet, és nem ad több támogatást ahhoz, hogy egy jólmegalapozott koncepciót alkothassunk.

Végül, de nem utolsó sorban Siponen (2000) mondja a következőket az információbiztonsági tudatosságról: „ez egy olyan állapot, amikor a felhasználók tisztában vannak szervezetük biztonsági küldetésével". Habár cikke a motivációs / viselkedési elméletekkel foglalkozik, a szövegezése alapján az információbiztonsági tudatosság koncepciója nála is az informatikai tárgyú esetekre korlátozódik.

Ahogy azt már korábban is megfogalmaztam, az információbiztonsági tudatosság nem csak az IT felhasználókról szól: A fizikai dolgozók is veszélyeztethetik a céget, ha rossz gyakorlatot követnek és például rajtuk keresztül szenzitív információk szivárognak ki a szervezettől.

Levonva a következtetéseket ebből a természetszerűleg korlátozott mértékű szakirodalmi áttekintésből, megállapíthattam, hogy nincsen egy egységesen elfogadott információbiztonsági tudatosság definíciónk, de minden egyes cikk hozzátesz valamit a koncepcióhoz.

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.

2.2.4 Az információbiztonsági tudatosságra ható kontrollok

Az információbiztonság szakterületének egyik kulcsfogalma a „kontroll”, melyet többféle értelemben és megfogalmazásban használunk a szakmában és a hétköznapokban.

Az értekezésem egyik sarokpontja azoknak a kontrolloknak az azonosítása, melyek befolyással lehetnek a szervezet információbiztonsági tudatosságának érettségi szintjére. Ehhez szükségünk van egy a szakma által széles körben elfogadott definícióra. Ilyen definíció lehet az ISACA COBIT 4.1 (2007) által használt fogalom:

„A kontrollok azok a szabályozások, eljárások, gyakorlatok és szervezeti struktúrák, melyeket arra terveztek, hogy megfelelő módon biztosítsák a működési (üzleti) célok elérését és a nemkívánt eseményeket megelőzzék, érzékeljék és kijavítsák."

(„Controls are the policies, procedures, practices, and organizational structures that are designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.") (COBIT 4.1)

A 2007-ben publikált definíciót némiképpen felülírja a 2012-ben megjelent COBIT 5, mely ugyanezt a fogalmat kicsit más megvilágításba helyezi, más hangsúlyokat képez:

„Aminek révén a kockázatokat menedzseljük, beleértve a szabályozásokat, eljárásokat, vezérfonalakat, gyakorlatokat vagy szervezeti struktúrákat, melyek adminisztratív, műszaki, menedzsment vagy jogi természetűek lehetnek. Használjuk még a védelmi vagy ellenintézkedések szinonimájaként is."

(„The means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of an administrative, technical, management or legal nature. Also used as a synonym for safeguard or countermeasure.") (COBIT 5.0)

A szervezeti kontrollok (védelmi intézkedések) léte és minősége meghatározza a szervezeti tudatosságot és így annak érettségét is. Az ilyen kontrolloknak többféle csoportosítása létezik a szakirodalomban.

Egy klasszikus csoportosítást vázol fel Yau (2014), aki más szerzők nyomán megkülönböztet

- fizikai
- technikai (műszaki) és
- adminisztratív kontrollokat.

Fizikai kontrollok között tartjuk számon a területi határokat védő eszközöket és személyzetet (biztonsági őr, recepciós stb.), a kamerás megfigyelő rendszereket, a különleges védelmet igénylő területek (pl. szerver szobák) biztonsági elemeit (pl. tűzjelző berendezések, oltó rendszereket, behatolás detektáló eszközöket. Ezek a kontrollok az esetek döntő többségében jól láthatók vagy létükre felhívják a figyelmet különféle tájékoztató táblák, ezért különösen alkalmasak a tudatosság megteremtésére a szervezetben „közlekedő" személyek számára.

A technikai vagy műszaki kontrollokat szokás még algoritmikus kontrolloknak is nevezni, mert itt olyan kontrollokról beszélünk, melyek hordoznak magukban valamiféle algoritmust, kódot, kódrészletet. Ezen kontrollok számossága igen nagy, és beleértjük az azonosságkezelés, hitelesítés, jelszómenedzsment eszközeit, de ugyanitt tartjuk számon a tűzfalakat és egyéb forgalomszűrő alkalmazásokat, és ide értjük a különböző tokenek, intelligens kártyák és biometrikus azonosításra alkalmas eszközök világát is. A lényeg, hogy ezek a kontrollok valamilyen algoritmus mentén működnek.

Az adminisztratív kontrollok jelentik a szervezetek szabályozásainak együttesét, a különböző szabályzatokat, előírásokat, vezérfonalakat, utasításokat melyek tartalmazzák a kívánatos viselkedésmódokat a szervezetben. Ebbe a csoportba szokás érteni a különböző tudatosságot támogató tréningeket, képzéseket, gyakorlatokat is.

Természetesen az említett kontrollfajták között nincsenek éles határok és szorosan egybefonódva fejtik ki hatásukat. Egy beléptető rendszer tartalmaz fizikai elemeket (pl. forgóvilla a bejáratnál és kártya a munkatársnál) és műszaki, algoritmikus elemeket (pl. a beléptető rendszer vezénylő szoftvere), melyek kiegészülhetnek adminisztratív szabályokkal (pl. mit kell tenni, ha valaki otthon hagyja a kártyáját, de szeretne bejutni a munkahelyére).

A kontrollok egy másik csoportosítási lehetőségét kínálja Merkow és Breithaupt (2014), akik azt a hagyományos megközelítést elevenítették fel, melyben a csoportosítás alapját az adja, hogy az adott kontroll egy biztonsági eseményhez képest időben hol fejti ki hatását. Ebből a szempontból három kontrolltípust különböztetünk meg:

- Megelőző kontroll (preventative, preventive control): Olyan intézkedés, mely egy biztonsági esemény bekövetkezését előzetesen hivatott megakadályozni (pl. egy tudatosító képzés, mely a social engineering veszélyeire hívja fel a figyelmet a szervezet tagjai számára)
- Észlelő kontroll (detective control): Olyan intézkedés, mely biztosítja a biztonsági esemény észlelhetőségét (pl. riasztást ad, ha kártékony kód megjelenésének gyanúja merül fel egy informatikai rendszerben)
- Javító kontroll (responsive, corrective control): Olyan intézkedés, mely egy biztonsági esemény bekövetkezése után képes az esemény következményeit viszonylag gyorsan és hatékonyan felszámolni (pl. egy dokumentált, tesztelt és bevezetett katasztrófa-elhárítási terv (DRP – Disaster Recovery Plan)

Az értekezés kutatási céljai felől közelítve adódik egy harmadik csoportosítási szempont, mely azt hivatott feltárni, hogy a tudatosság milyen dimenziókból rakható össze. Ha elfogadjuk azt, hogy önmagában a szabályok ismerete nem védi a szervezetet, hanem az aktív védelemhez az is szükséges, hogy a szervezet tagjainak hozzáállása is megfelelő legyen, akkor meg kell különböztetnünk olyan kontrollokat, melyek a tudást (ismeretet) és olyanokat, melyek pedig a helyes attitűdöt (hozzáállást) támogatják. Ilyen alapon megkülönböztethetünk:

- Tudást (ismeretet) támogató kontrollokat (pl. egy jól szerkesztett intranet felület megkönnyíti a szükséges tudás megszerzését),
- Attitűdöt (hozzáállást) támogató kontrollokat (pl. egy fegyelmi szabályzat szembesíti a szervezet tagjait esetleges rossz attitűdjük következményeivel).

Természetesen itt sem lehetséges ezeknek a kontrolloknak az abszolút egyértelmű szétválasztása. A tudást támogató kontrollokról tudjuk, hogy a szabályok, eljárások és utasítások ismerete ugyan alapvető az információbiztonsági tudatosság szempontjából, de önmagában ez a fajta tudás még nem biztosít aktív védelmet az információs vagyonelemek felett. Az attitűdöt támogató kontrollok létrehozzák, megerősítik azt a pozitív hozzáállást, mely szükséges ahhoz, hogy az emberek ne csak megértsék, hogy mit kell csinálni és az miért helyes, hanem aktívan részt is vegyenek a megelőző és helyesbítő intézkedésekben. Jelentsék az észlelt gyanús eseményeket, részt vegyenek a mentési és helyreállítási műveletekben, kövessék a szabályokat és aktívan adjanak egymásnak segítséget, ha váratlan biztonsági eseményekkel szembesülnek.

A 2.5 fejezetben tárgyalt saját (tovább)fejlesztésű érettségi modell ezt a két dimenziót is próbálja megjeleníteni. A primer kutatásban alkalmazott kérdőív is tartalmaz olyan elemeket, melyek részben a tudást, részben az attitűdöt támogató kontrolokat próbálja azonosítani a szervezet különböző érettségi állapotaiban.

2.3 A mérési probléma

Az információbiztonsági tudatosság érettségének mérése számos probléma forrása. Az első megválaszolandó kérdés, hogy a tudatosság érettségét milyen szinteken próbáljuk mérni? Mérési lehetőségeket és szakirodalmi hivatkozásokat a következő szinteken találhatunk:

- Az egyén szintjén: Nemeslaki és Sasvári (2015) korábban már hivatkozott felmérése egy az egyén szintjén megvalósuló értékelést körvonalaz.
- A (tudatosító) programok szintjén: A SANS Institute Információbiztonsági Tudatossági Érettségi Modellje Spitzner (2012) szintén már hivatkozott publikációjában kifejezetten a tudatosító programok érettségét hivatott mérni.
- Szervezeti szinten: A szervezet egészére vonatkozó értékelést a szakirodalmi áttekintés során nem találtam, de a SANS Institute által publikált érettségi modellt szinte minden éves riportjukban finomították és a legújabbak (2017, 2018) már erősen szervezeti fókuszúak (SANS (2017, 2018)).

Mindhárom szinten végzett mérés rejt kihívásokat magában:

- Az egyén szintjén végzett mérés etikai problémákat vet fel: Gyakorló auditorként elmondhatom, hogy rendkívül veszélyes az egyes egyének szintjén kijelentéseket tenni az adott személy információbiztonsági tudatosságáról, mert
    - Egy személy nem lehet büntetés alanya egy információbiztonsági audit következményeképpen,
    - Az auditor ilyen módon sem sértheti az auditra vonatkozó etikai standardokat.
- A programok szintjén folyó mérés nem ad teljes képet a szervezet egészének tudatossággal kapcsolatos működéséről, hanem csak egy önkényesen kiválasztott szelete, a programmenedzsment képessége kerül górcső alá,
- A szervezeti szinten zajló mérés az egyértelmű mérőszámok hiányától kezdve, a részmérőszámok zavarba ejtő bőségén át a méréselméleti kérdéseikig hordoz kihívásokat.

A szervezeti szinten zajló mérés segíthet a személyes konfliktusok elkerülésében és egyéb előnyöket is kínál a szervezet számára:

- A szervezet, mint egész, egy holisztikus képet kap az információbiztonsági tudatosság szintjéről
- A vezetők világos képet kapnak arról, hogy hol vannak hiányzó vagy rosszul működő kontrollok vagy lehetőségek a továbbfejlesztésre.

A következő méréselméleti megfontolások nagyon lényegesek, ha egy megfelelő érettségi modellt akarunk kidolgozni az információbiztonsági tudatosság szervezeti szintű értékeléséhez.

A statisztika tudománya alapvetően négyféle mérési skálát ismer, de a skálák tulajdonságainak értelemzése felett már egy több évtizedes szakmai vita dúl, mióta Stevens (1946) 1946-ban leírta a használatos skálák alapvető tulajdonságait.

Ezt a vitát foglalja össze Kehl (2011) anélkül, hogy állást foglalna a vitatott kérdésekben. Ha egy használható érettségi modellt szeretnénk összerakni, akkor nem kerülhetjük meg, hogy néhány méréselméleti megfontolást is tegyünk. Kehl cikke körül járja a méréselméleti vita történetét és Stevens legfontosabb megállapításának tekinti, hogy a mérésnek számos formája létezik, és ennek megfelelően definiálhatók mérési skálák (alapvetően négy: nominális / névleges, ordinális / sorrendi, intervallum, arány), és ezeknek a skáláknak a milyenségétől függ, hogy a mérés folyamán milyen konkrét eljárásokat alkalmazhatunk és milyenek lesznek az adott skála matematikai tulajdonságai. Másképpen szólva, a mérési skálától függ, hogy az adott empirikus adatok vonatkozásában mely statisztikai módszerek, eljárások alkalmazhatók, és melyek pedig nem.

A négy alapskála számának növelésére, bővítésére több kísérlet is született. Az intervallumskála mellett (amelyet szokás egyenlő intervallumok skálájának is nevezni) a nem egyenlő intervallumok skáláit is megkülönböztetik a szakirodalomban. Ilyen például a logaritmikus skála, ahol tízes alap esetén minden intervallum a tízszerese az őt megelőzőnek. Az ilyen skálákat végül csak azért nem tekintjük külön típusnak, mert megfelelő matematikai művelettel hagyományos intervallumskálává transzformálhatók. A megengedhető statisztikai műveletek ebben az esetben a hatványtranszformációk.

Az elképzelhető skálatípusok matematikai meghatározásával a modern méréselmélet foglalkozik, melynek alapvető megállapítása, hogy Stevens besorolása többé-kevésbé teljesnek tekinthető, és más jelentős struktúrák (skálák) bizonyíthatóan nem léteznek.

Az említett mérési skálák néhány a méréshez kötődő tulajdonságuk alapján osztályozhatók:

- Azonosság: A mérési skálán minden értéknek van saját és egyedi jelentése.
- Nagyság: A mérési skálán elhelyezkedő értékek sorrendi kapcsolatban vannak egymással, azaz egyes értékek nagyobbak mások pedig kisebbek.
- Egyenlő intervallumok: A skála egységek (pl. fokok) az egész skálán egyforma nagyok egymáshoz képest.
- Van-e létező nullapont: A skálának van tényleges nulla pontja, azaz annál kisebb értékek nincsenek.

A négy alap skálafajta a fenti jellemzők tükrében:

- Nominális vagy névleges skála: Ez a skála csak az azonosság kritériumának felel meg, a skála igazából csak megcímkézi a mérni kívánt objektumokat (pl. férfi / nő „osztályozás”). Nincs saját számszerű értéke és így a nagyság kérdésére már nem ad választ. Ennek tükrében kimondhatjuk, hogy a nominális vagy névleges skála nem igazán alkalmas a szervezeti információbiztonsági tudatosság mérésére.
- Ordinális vagy sorrendi skála: Ez a skála mind az azonosság, mind a nagyság tulajdonságának eleget tesz. A sorrendi skálán minden értéknek van egyedi jelentése és az egyes skálaértékek sorba rendezhetők (lásd az iskolai osztályozás sémáját). Az érettségi modellek tipikusan ilyen skálát használnak, ezért a továbbiakban majd erre a skálatípusra fogunk fókuszálni.

- Intervallum skála: Az intervallum skálán történő mérés során értelmezhető tulajdonságok az azonosság, a nagyság és az egyenlő intervallumok. Az intervallum skálával nem csak arról kaphatunk információt, hogy az egyes értékek nagyobbak vagy kisebbek, hanem azt is megtudhatjuk, hogy hányszor nagyobbak vagy kisebbek. Az érettségi modellek esetében ezt a tulajdonságot nem tudjuk értelmezni, mert annak a kérdésnek, hogy az „A" szervezetnél hányszor nagyobb az információbiztonsági tudatosság mint „B" szervezetnél, igazából nincs valós és értelmezhető jelentése.
- Arányskála: Az arányskála a mérés mind a négy tulajdonságának megfelel, mert értelmezhető az azonosság, a nagyság, az egyenlő intervallumok fogalma, és van létező nullapont. Ez a mérési szint megint csak nem áll rendelkezésünkre ebben az esetben, amikor az információbiztonsági gyakorlat erősségét (az információbiztonsági tudatosságot) szeretnénk értékelni egy szervezetben, hiszen nem tudunk egy abszolút zérus pontot, mint kezdőpontot, megadni.

Mivel a négy alap skálafajtából kizártunk kettőt (az intervallum és az arány skálát), a maradék kettőre kell fókuszálnunk, hogy az érettség mérésére használható statisztikai eszköz-készletet meghatározzuk.

A nominális (névleges) skála a legalacsonyabb olyan mérési szint, amit statisztikai elemzések céljára használhatunk. A nominális skála, ahogy a neve is jelzi, semmi mást nem jelent, mint hogy adatokat sorolunk bizonyos kategóriákba bármiféle különleges rendezési elv vagy meghatározott struktúra nélkül. Kutatási szempontból egy igen/nem típusú skála nominálisnak tekinthető. Ezen a skálán nincs sorrendiség és nincs mérhető távolság az „igen" és a „nem" kategória között.

Az ordinális (sorrendi) skála már egy jobb mérés erősséget jelent a listánkon. A legegyszerűbb sorrendi skála a szimpla rangsor. Nem véletlen, hogy az ún. érettségi modellek jellemzően ezt használják. Ebben az esetben nincs objektív távolság az ezen a szubjektív skálán elhelyezett két pont között. Az ordinális skála csak az abszolút sorrendet mutatja és nem utal semmilyen relatív távolságra.

Kutatási szempontból a sorrendi adatok csak az ún. nem-paraméteres statisztikai módszerek és eszközök használatát engedik meg. Ilyenek a medián és a módusz, a rang-korrelációs tesztek, és a nem-paraméteres variancia-analízis. Ezek a statisztikai módszertani korlátaink ilyen módon jól meghatározottak, és az érettségi modellünk validálási folyamata során csak a fenti módszereket használhatjuk.

Ahogy már utaltam rá, a szervezeti szinten elvégezhető mérés egyik lehetséges és gyakorlatias eszköze az ún. érettségi modelleknek a használata, melyek segítségével a szervezet egésze sorolható be valamiféle érettségi osztályba és viszonylag egyszerűen tudjuk jellemezni a szervezetben uralkodó információbiztonsági tudatosság általános állapotát. Módszertani szempontból szükséges egy kicsit körül-járnunk az érettségi modellek témakörét.

2.4 Az érettségi modellek

Általában szólva az érettségi modellekről, Klimkó (2001) gondolatait érdemes idéznem. Állítása szerint „az érettségi modellek egy entitás időbeni fejlődését írják le" és ehhez van néhány további általánosító megállapítása az érettségi modellekkel kapcsolatban:

- Az említett entitás fejlődési stációit jellemzően korlátozott számú (általában 4-6) érettségi szinttel szokták leírni.
- Az egyes érettségi szinteket néhány olyan követelménnyel írják körül, melyeket az entitásnak el kell érnie az adott szinten.
- Az érettségi szintek sorbarendezettek (sorrendi skála!) egy induló szintről egy végső szintig, mely általában a „tökéletességet" reprezentálja.
- A fejlődési folyamat során az entitás felfelé (vagy lefelé) mozog az egyik szintről a másikra, de a mozgás közben nem hagyhat ki egy szintet sem – más szavakkal: az entitás nem tud „ugrálni" egy meghatározott szintről egy jóval magasabb (vagy alacsonyabb) szintre anélkül, hogy a közbenső szinteket ne érintené.

Ha az információbiztonsági tudatosság szervezeti szintjeit leíró érettségi modellt akarunk alkotni, akkor ezeket az egyszerű szabályokat kell követnünk a modell megalkotásakor.

Ugyanakkor az érettségi modellek megalkotása és használata során mindig szem előtt kell tartanunk, hogy az egyes érettségi szintek (stációk) egy idealizált állapot, egyfajta tökéletesség felé haladás mérföldköveit szimbolizálják és egy fejlődési pálya felrajzolásához szükséges utat hivatottak bemutatni azzal, hogy intézkedéseket segítenek megfogalmazni egy elérendő jövőkép (egy újabb stáció) felmutatásával. Az érettségi modellek mechanikus alkalmazása azzal a veszéllyel is járhat, hogy az adott modell túlságosan megvezeti a gondolkodást, és ilyenkor az egyetlen és egyedüli üdvözítő út hamis ígéretével helyettesítjük a szervezetspecifikus megoldások keresését.

2.4.1 Érettségi modellek a menedzsment irodalomban

Az érettségi modellek behálózzák a vezetéstudomány szinte minden területét. Néhány jellemző terület:

- Projektmenedzsment (Organizational Project Management MM – OPM3), Project Management Institute (2008),
- Üzleti elemzések az ún. „Big Data" jelenség kapcsán (IBM Big Data MM), IBM (2014),
- Szoftverfejlesztés (Capability Maturity Model for Software), Paulk (1993),
- Humánerőforrás menedzsmentje (People Capability Maturity Model), Curtis (2002),

Természetesen ez a lista közel sem teljes, csak azt hivatott bemutatni, hogy a témakör milyen erőteljesen van jelen a menedzsment szakirodalomban.

2.4.2 Érettségi modellek az informatikai működés-irányítás területén

Az informatikai működés-irányítás területén is a bőség zavarával küszködünk, ha az érettségi modellek körében szeretnénk válogatni, de itt van két olyan kiemelkedő és emiatt elterjedt érettségi modell, melyek nem megkerülhetők egy érettségi modelleket elemző értekezésben.

2.4.2.1 Az ITIL Érettségi Modellje

Az ITIL (2013) Érettségi Modellje egy hatfokozatú skálát alkalmaz a szervezeti informatikai folyamatok és funkciók értékelésére. Az itt meghatározott érettségi szintek összhangban vannak a COBIT definícióival, melyre szintén hivatkozunk ebben a fejezetben később.

Az ITIL (2013) két kulcsfogalommal operál:

Folyamat = Egy meghatározott cél érdekében létrehozott strukturált tevékenységek halmaza. A folyamat egy vagy több meghatározott bemenetet alakít át meghatározott kimenetekké. *(process = A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs.)*

Funkció = egy emberekből álló csoport vagy csapat és eszközeik vagy egyéb erőforrásaik, melyeket arra használnak, hogy egy vagy több folyamatot vagy tevékenységet elvégezzenek – ilyet például egy ügyfélszolgálati egység. *(function = A team or group of people and the tools or other resources they use to carry out one or more processes or activities – for example, the service desk.)*

Az ITIL érettségi modellje ehhez a két fogalomhoz kötődően az alábbi érettségi szinteket definiálja:

0. Szint (hiány / káosz) – A folyamatok vagy funkciók ad hoc módon működnek, szervezetlenek vagy kaotikusak.

1. Szint (kezdeti / reaktív) – A folyamatok vagy funkciók egy szokványos sémát követnek, de a folyamatok vagy a funkciók irányítása nem létezik.

2. Szint (megismételhető / aktív) – A folyamat vagy a funkció bevett módon működik és az eljárások standardizáltak, dokumentáltak és képzési eseményeken keresztül kommunikáltak.

3. Szint (meghatározott / proaktív) – A tevékenységek megfelelő módon el vannak látva erőforrásokkal, de alkalmanként, és nemszokványos körülmények között nem megfelelő módon működnek.

4. Szint (menedzselt / kezdeményező) – A folyamat vagy a funkció és a kapcsolódó tevékenységek szilárdak és csak nagyon ritkán nem teljesítenek az elvárt szinten.

5. Szint (optimalizált) – Minden tevékenység jól kontrollált, menedzselt és irányított.

Az ITIL érettségi modellje szolgáltat néhány ötletet ahhoz, hogy létrehozzuk a saját érettségi modellünket az információbiztonsági tudatosság mérésére:

- A legalacsonyabb szint képviseli az érettség teljes hiányát, így a mi kezdő szintünk az információbiztonsági tudatosság teljes hiányát fogja jelölni.
- Az ITIL érettségi modellje a legmagasabb szinthez köti a kontroll, a menedzsment és az irányítás teljességét, és a mi modellünkben is ezt fogjuk beépíteni a legmagasabb érettségi szintbe.
- Maximum 5-6 szintet definiálunk az információbiztonsági tudatosság szervezeti szintű érettségi modelljében.

2.4.2.2 A COBIT2019 folyamatképességi szintjei (Process Capability Levels)

Az Informatika Ellenőrök Nemzetközi Szervezetének (ISACA – Information Systems Audit and Control Association) talán legfontosabb módszertani terméke a COBIT (Control Objectives for Information and Related Technologies), mely egy jó gyakorlatokon alapuló irányítási keretrendszer.

Az ISACA (2018) COBIT2019 keretrendszere, a legújabbnak tekinthető COBIT verzió, mely meghatároz egy olyan informatikai irányítási keretrendszert, melyben kiemelt szerepe van egy folyamatképességi szinteket meghatározó modellnek. Ez a modell a folyamatokat hat szintre sorolja be:

- 0. Szint: Az alap képességek hiánya. Hiányos megközelítés az irányítási és a menedzsment célok vonatkozásában. A folyamat egyáltalán nem, vagy lehet, hogy nem teljesíti be a folyamattól elvártakat.
- 1. Szint: A folyamat többé kevésbé eléri céljait olyan hiányos tevékenységek alkalmazásán keresztül, melyek kezdetlegesnek vagy intuitívnak tekinthetők és nem túlságosan szervezettek.
- 2. Szint: A folyamat eléri céljait egy olyan tevékenység halmaz eredményeképpen, mely már teljesnek és teljesítőképesnek tekinthető.
- 3. Szint: A folyamat egy már jobban szervezett módon éri el céljait a szervezet erőforrásainak felhasználásával. A folyamatok jellemzően jól definiáltak.
- 4. Szint: A folyamat eléri céljait, jól definiált és a teljesítménye mennyiségi szempontból mért.
- 5. Szint: A folyamat eléri céljait, jól definiált és a teljesítménye mért a teljesítmény fejlesztése céljából és a folyamatos fejlődés megvalósul.

A COBIT2019 elődje az ISACA COBIT 5 (2012) és ennek a keretrendszernek az egyik fontos szabálya volt, hogy egy bizonyos képességi szint eléréséhez az előző szintet teljes mértékben teljesíteni kell, tehát érettségi szinteket részben átlapolva nem létezhetnek folyamatok. Ez a szabály találkozik az érettségi modellek azon elvével, hogy az entitás (jelen esetben a folyamati érettség) előre (vagy hátra) mozog az egyik szintről a másikra, de mozgása közben nem hagyhat ki egy szintet sem.

Pasquini és Gallé (2013) azt mondják, hogy ez a fejlettebb modell erősen igényli a nem-szubjektív értékelést és ennek bizonyítékait, valamint biztosítják a folyamatképesség értékelési tevékenységek megbízhatóságát és megismételhetőségét, ezáltal csökkentve a nézetleltérést az értkelési eredmények felett.

A COBIT2019 (2018) folyamat érettségi szintjei igazolják mindazt, amit már megtanultunk az ITIL érettségi modelljéből. Az információbiztonsági tudatossághoz és a már vele kapcsolatban publikált érettségi modellekhez közelítve már találkozhatunk néhány olyan modellel, melyek a tudatossággal kapcsolatos témaköröket tárgyalják:

2.4.3 Érettségi modellek az információbiztonság területén

Fókuszomat még szűkebbre véve, áttekintem, hogy az információbiztonság területén milyen megközelítésű érettségi modellekkel találkozhatunk, és ezek a modellek milyen módon használhatók fel egy saját modell készítéséhez és majdani validálásához.

2.4.3.1 Az Osterman Research képzés érettségi modelljei az információbiztonsági tudatosság területén

Az Osterman Research (2013) tanulmányában az információbiztonsági tudatosító képzések öt alaptípusát azonosítja az adathalász és hasonló típusú támadások kivédése céljából. A publikáció fókusza egyértelműen szűkebb, mint az általános információbiztonsági tudatosítás témaköre, de megközelítésében az érettségi modellek által követett szemlélet és gyakorlat köszön vissza. A belső képzések öt szintje az Osterman Research szerint (2013):

- The Do Nothing Approach (A „ne tegyünk semmit" megközelítés):
  Ekkor a szervezet nem folytat semmilyen biztonságtudatosságot erősítő képzési tevékenységet.
- The Break Room Approach (A „gyűljünk össze az ebédlőben" megközelítés):
  A munkatársakat időnként összehívják egy ebédre vagy egy gyors találkozóra, ahol elmondják nekik, hogy mit kerüljenek a weben szörföléskor vagy ismeretlen forrásból származó e-mailek esetében.
- The Monthly Security Video Approach (A „havonkénti biztonsági videó" megközelítés):
  A munkatársak rövid információbiztonsági tudatosító videókat néznek meg, hogy megtanulják, hogyan tartható a hálózat és a szervezet biztonságos állapotban.
- The Phishing Test Approach (Az „adathalászati tesztelő" megközelítés):
  Bizonyos előre kiválasztott munkatársak egy szimulált adathalász támadást szenvednek el, és a levelet indító szervezeti egység (az informatika vagy egy külső megbízott fél) értékeli és visszacsatolja a megtámadott személy számára, hogy jól vagy rosszul reagált az eseményre.
- The Human Firewall Approach (Az „emberi tűzfal" megközelítés):
  Itt a munkatársakat folyamatosan tájékoztatják a jellemző támadási vektorokról, azaz a számítógépes felhasználók rendszeres tájékoztatást kapnak az éppen aktuális fenyegetésekről. A szimulált adathalász támadásokba a szervezet minden munkatársát bevonják, és az eredményekből meghatározzák azokat a személyeket, akik hajlamosak áldozatául esni az ilyen támadásoknak.

Ebben a tanulmányban világosan kirajzolódik az a kép, amit a többi érettségi modell is sugall: Alkoss egy nagyjából ötfokozatú skálát, ahol a szervezet által követett gyakorlat jól tetten érhető és ezek a gyakorlatok az egyes szinteken egyre fejlettebb szervezeti tudatosságot képviseljenek. A fenti modell megközelítése meglehetősen pragmatikus és egyszerűen értékelhetővé teszi a szervezet által követett gyakorlat minőségét, érettségét. A modell erősen azt sugallja, hogy a munkatársak bevonása, a szokványostól eltérő gyakorlat, és a napi életesemények minél pontosabb szimulációja vezethet egy magasabb szintű érettséghez az információbiztonsági tudatosság területén.

A modell egy nagyon szűk területre (adathalászat) fókuszál, de megközelítése hasznos a saját modellem megalkotásához.

2.4.3.2 Az Information Security Awareness Capability Model (ISACM)

Az ISACM Poepjes és Lane (2012) által publikált modell. Ők összekapcsolták a szituációs tudatosság elméletet az ISO 27002-es szabvánnyal. Erősen kontroll alapú a megközelítésük és az ISO/IEC 27002-es szabványt vizsgálták az információbiztonsági tudatosság aspektusából.

Meghatároztak három olyan tudatossági dimenziót, melyet befolyásolnak a hivatkozott szabvány kontrolljai:

- A tudatosság fontossága: Mennyire fontos a tudatosság egy bizonyos folyamat vagy kontroll megfelelő működése szempontjából
- A tudatossághoz kapcsolódó döntésképesség: Mennyire döntésképes egy személy, amikor egy döntési helyzettel szembesül
- A tudatosság kockázata: Ez tulajdonképpen egy olyan rés lehet, ami abból ered, ha a szükséges tudatosság mértéke (Fontosság) nagyobb, mint amilyennek a kapcsolódó és szükséges döntési képesség tűnik.

A modellben ez a három dimenzió van összekapcsolva az ISO/IEC 27002 által elvárt és azonosított kontrollokkal. A modell részeként azonosítottak az érdekelt felek csoportjai is, és össze vannak kapcsolva a kontrollokkal. Ezt az érettségi modellt mutatja be a 3. ábra.

Information Security Awareness Capability Model

ISO/IEC 27002 Controls Standard	Stakeholder Group	Awareness Importance							Awareness Capability							Awareness Risk
		Importance (influence) that awareness provides to the controls for each stakeholder group. How much awareness is required?							Level of Awareness being displayed by each Stakeholder category.							Highlights gap in required awareness - Interface with Risk Assessment matrix
ISO/IEC 27002 list of controls		None		Slightly		Moderate	Very	Extremely	None		Slightly	Moderate		High	Expert	Overall Rating
5 Security policy																
	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.															
5.1 Information security policy	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
6 Organization of information security																
	Objective: To manage information security within the organization.															
6.1 Internal organization	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.															
6.2 External parties	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
7 Asset management																
	Objective: To achieve and maintain appropriate protection of organizational assets.															
7.1 Responsibility for assets	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Objective: To ensure that information receives an appropriate level of protection.															
7.2 Information classification	IT Staff	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	Senior Management	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None
	End Users	1	2	3	4	5	6	7	1	2	3	4	5	6	7	High/Medium/Low/None

3. ábra: Az Information Security Awareness Capability Model (ISACM) (2012)

Az ISACM javára írandó, hogy a tudatosság három fontos dimenzióját határozza meg: a fontosságot, a döntésképességet és a kockázatot. Ugyanakkor létrehozza az érdekelt felek csoportjait is (IT személyzet, vezetők és végfelhasználók), de ez a csoportosítás rögtön jól mutatja a modell korlátait is: Csak az informatika szemszögéből tekint a tudatosságra (holott az információbiztonsági tudatosság nem csak az informatikáról szól!) és a külső érdekelt felek egyáltalán nincsenek figyelembe véve ebben a modellben.

Az ISACM ad néhány ötletet ahhoz, hogy létrehozzam a saját érettségi modellemet az információbiztonsági tudatosság mérésére:

- Az ISO 27000-es szabványcsalád néhány eleme (néhány ott azonosított kontroll) felhasználható egy „kontroll-leltár” készítéséhez, ami hozzákapcsolható az információbiztonsági tudatossági érettségi modellünk egyes meghatározott szintjeihez.

- A tudatosság több dimenzióját kell figyelembe vennem a saját modellem megalkotásához.
- Az érdekelt felek csoportjainak teljessége szintén fontos eleme egy létrehozandó érettségi modellnek.

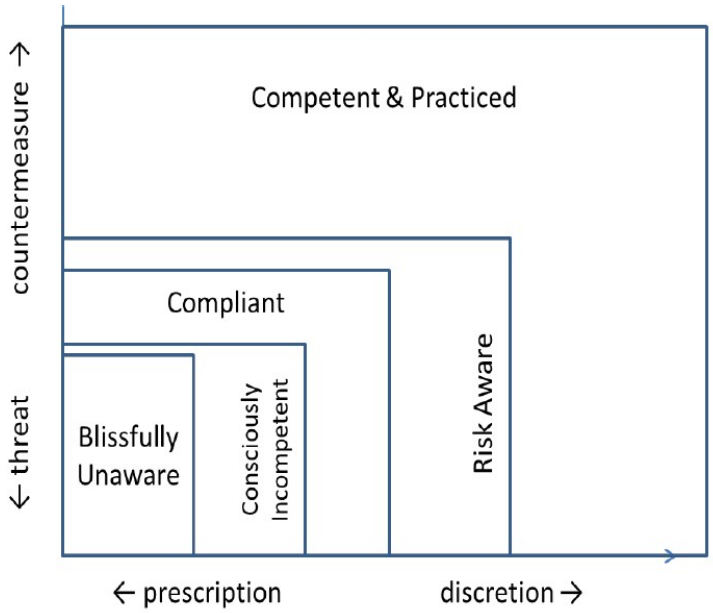
Minután röviden áttekintettük a bemutatott szervezeti érettségi modelleket, érdemes azokra az egyénekre fókuszálnunk, akiket szintén értékelünk érettségi modellek keretei között.

2.4.3.3 A Felhasználói Tudatosság Érettségi Modellje (User Awareness Maturity Model)

A Felhasználói Tudatosság Érettségi Modelljét (User Awareness Maturity Model - UAMM) Steve Kruse és Bill Pankey (2018) mutatta be. A modellt nem publikálták semmilyen tudományos cikkben, de prezentációjuk hozzáférhető az interneten. Ők az informatikai felhasználókat sorolták be tudatosság szempontjából egy ötfokozatú skálán:

1. Fokozat: „a szerencsés tudatlan” (blissfully unaware)
    - Ő az, aki mindenféle eszközt és erőforrást, amit csak kap, használ anélkül, hogy az információbiztonsági fenyegetések közül bármelyiket is felismerné vagy elfogadná létezésüket
    - Ez az a szint, ahol az az uralkodó nézet, hogy az információbiztonság az IT rendszerek tulajdonsága és nagymértékben az architektúra és a konfiguráció kérdése. A biztonság jórészt független a felhasználói viselkedéstől.
2. Fokozat: „a tudatosan inkompetens” (consciously incompetent)
    - A túl kockázatosnak ítélt tevékenységeket kerüli, még akkor is, ha az termelékenységvesztéshez vezetnek.
3. Fokozat: „a megfelelőségre törekvő” (compliant)
    - A szervezeti szabályozásokban azonosított kockázatokkal tisztában van
    - A szabályzatban leírt módon jár el, ha olyan eseménnyel találja magát szemben, amire van szabályozás
4. Fokozat: „a kockázat tudatos” (risk aware)
    - A szervezeti működéssel kapcsolatos információbiztonsági kockázatokat figyelembe veszi, de néha bizonytalan a megfelelő cselekvés felől, és néha jelent incidenseket
5. Szint: „a kompetens és gyakorlott” (competent & practiced)
    - Információbiztonsági kockázatokat menedzsel (érzékel és csökkent) miközben munkaköri kötelezettségeit teljesíti.

Kruse és Pankey (2018) az UAMM esetében két dimenziót alkalmaz akkor, amikor embereket helyez el a megfelelő érettségi szinten:



4. ábra: A Felhasználói Tudatosság Érettségi Modellje - UAMM (2018) p. 7

Az ábrán láthatjuk, hogy

- vízszintesen a felhasználói viselkedést kell értékelnünk a felhasználó megfontoltsága alapján, és több rugalmasságot engedhetünk meg a felhasználóknak ahogy az érettségük növekszik
- függőlegesen pedig a nagyobb kockázatmenedzselési felelősséget értékelhetjük, ahogy növekszik az érettség szintje.

Az UAMM az érettségi szinteket a személyekhez köti és megerősít engem abban, hogy több dimenziót használjak saját modellem megalkotásakor.

A szerzők által használt szófordulatok ugyanakkor azt az üzenetet hordozzák, hogy ők is csak IT felhasználókról beszélnek, amikor az emberekre gondolnak. Az én tudatosság felfogásom nem csak azokhoz a személyekhez kapcsolódik, akik informatikai eszközökkel, berendezésekkel dolgoznak.

Természetesen a szerzők „kétdimenziós" megközelítése támogatja a saját érettségi modellem megalkotását.

2.4.3.4 A NISTIR 7385 – PRISMA (Program Review for Information Security Management Assistance)

Bowen és Kissel (2007) PRISMA néven publikált egy NIST Interagency Report-ot, mely a NISTIR 7385-ös jelzést kapta az információbiztonsági szabványok és ajánlások publikálásában igen aktív Amerikai Szabványügyi Hivataltól (NIST – National Insitute of Standards and Technology). A PRISMA (Program Review for Information Security Management Assistance) egy olyan módszertan, mely arra lett kitalálva, hogy az USA szövetségi információbiztonsági programját támogassa olyan módon, hogy legyen egy objektív mérőrendszer az egyes szövetségi szerveztek információbiztonsági állapotának értékelésére és a szükséges fejlesztési lépések meghatározására.

A PRISMA elsődleges céljai között szerepel, hogy

- segítse a szövetségi kormányzati szervezeteket saját biztonságuk növelésében (beleértve a szerződött partnereket és a helyi kormányzatokat),
- csökkentse a kritikus szövetségi rendszerek és vagyonelemek sérülékenységét
- segítse a kritikus infrastruktúra elemek védelmének tervezési és megvalósítási erőfeszítéseit,
- és támogassa a kockázat alapú költséghatékony információbiztonsági keretrendszerek és stratégiák létrejöttét.

Ennek érdekében kilenc kulcsterületen vizsgálja az adott szervezet érettségét egy ötfokozatú érettségi skálán. A kilenc kulcsterület jól reprezentálja az információbiztonsági szempontból kritikus elemeket (zárójelben a kilenc kulcsterülethez tartozó alterületek száma):

- Az információbiztonság menedzsmentje és kultúrája (41)
- Az információbiztonság tervezése (5)
- Információbiztonsági tudatosság, tréning és képzés (27)
- Biztonsági költségvetés és erőforrások (40)
- Életciklus menedzsment (21)
- Tanúsítás és akkreditáció (6)
- A kritikus infrastruktúra védelme (6)
- Incidensek és vészhelyzetek kezelése (30)
- Információbiztonsági kontrollok (40)

A kilenc kulcsterület további alterületekre és kritériumokra bomlik (összesen 216 alterület!), és mind a kilenc területet egy ötfokozatú skálán értékelnek. Az ötfokozatú érettségi skála elemei:

- „Policy” – Van-e a területre vonatkozó szabályozás?
- „Procedures” – Léteznek-e eljárások az adott szabályozási területre?
- „Implemented” – Bevezették-e ezeket az eljárásokat?
- „Tested” – Tesztelték-e az eljárások működését, működési hatékonyságát?
- „Integrated” – Az eljárások mennyire integrálódnak a szervezet egyéb tevékenységeibe?

A nagyon pragmatikus átvizsgálás végeredménye egy táblázat, mely színkódokkal jelzi az adott szervezet érettségét, teljesítményét az egyes kulcsterületeken. A színkódok egészen egyszerűek, nyilvánvalók: A piros jelzi, ha az adott kulcsterület nem teljesíti az adott érettségi szintet. A sárga jelzi, hogy vannak teljesült érettségi kritériumok az adott kulcsterületen, és a zöld szín mutatja, hogyha a terület mindenben megfelel az adott érettségi szintnek. A sárga mezőket pedig még egy készültségi fokot is jelző számmal is ellátják, hogy még jobban értelmezhető legyen a szervezet állapota. Ezek a számok azt a belső logikát is hordozzák, hogy a táblázatban balról jobbra haladva a készültségi fokot jelző számok csak kisebbek vagy egyenlők lehetnek, azaz például, ha az eljárások 60 %-a kész, akkor az implementáció értéke maximum 0,6 lehet, ami egyben azt is jelzi, hogy minden elkészült eljárás be lett vezetve.

Az egész PRISMA módszertan kiváló példája annak, hogy hogyan próbálják meg a menedzsment számára egyszerű és áttekinthető formában vizualizálni a szervezet általános információbiztonsági helyzetét.

Hozzá kell még tennem, hogy a PRISMA módszertan létrejöttét erősen támogatta az a tény, hogy a FISMA (2002) mint szövetségi törvény felhatalmazta a NIST szervezetét, hogy szövetségi szinten információbiztonsági szabványokat alkosson.

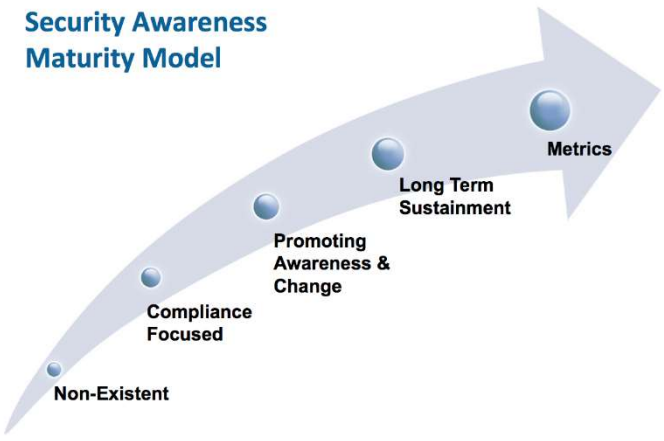
Menedzsment, működési és műszaki területek	Policy	Procedures	Implemented	Tested	Integrated
Az információbiztonság menedzsmentje és kultúrája	0,80	0,70			
Az információbiztonság tervezése	0,90	0,60	0,40	0,20	
Információbiztonsági tudatosság, tréning és képzés				0,60	
Biztonsági költségvetés és erőforrások		0,80	0,60		
Életciklus menedzsment	0,80	0,60			
Tanúsítás és akkreditáció	0,80	0,50	0,20		
A kritikus infrastruktúra védelme			0,80	0,60	
Incidensek és vészhelyzetek kezelése					
Információbiztonsági kontrollok			0,70	0,30	

5. ábra: Egy PRISMA riport egy fiktív szervezetre (saját ábra Bowen és Kissel (2007) p. 1 nyomán)

A FISMA modellje is alátámasztja azt az elképzelésemet, hogy a saját érettségi modellemet is célszerű lesz öt fokozatúként megalkotni.

2.4.3.5 A SANS Institute Információbiztonsági Tudatossági Érettségi Modellje (Security Awareness Maturity Model)

A SANS Institute Információbiztonsági Tudatossági Érettségi Modelljét Spitzner (2012) publikálta először egy blogbejegyzésben 2012. május 22.-én. Az azóta több átalakuláson átment modell eredeti „ötlépcsős” megközelítését mutatja be ez az ábra:



6. ábra: Az Információbiztonsági Tudatossági Érettségi Modell (Spitzner (2012))

A hivatkozott modell tömören:

- 1. szint: Nincs információbiztonsági tudatosító program

„Nincs biztonsági tudatosító program, nincs kísérlet sem arra, hogy a szervezetet képezzék. Ennek eredményeképpen az emberek nem ismerik vagy nem értik a szervezeti szabályzatokat, eljárásokat, és nem realizálják, hogy célpontok lehetnek és emiatt a szervezet erősen sérülékeny az emberi alapú támadásokkal szemben.”

- 2. szint: Megfelelőségre fókuszáló program

„Ez egy olyan tudatosító program, melyet a megfelelőségi és felülvizsgálati követelmények teljesítésére alkottak meg. A képzési alkalmak éves vagy ad hoc gyakoriságúak, és jellemzően egy évenként egyszeri tantermi előadást vagy egy negyedévenkénti hírlevelet jelentenek. Nem célja a viselkedés megváltoztatása. Ennek eredményeképpen az alkalmazottak bizonytalanok a szervezeti szabályzatokkal kapcsolatban, nem ismerik szerepüket a szervezet információvagyonának védelmében, és hogy hogyan tudnának megelőzni, azonosítani vagy jelenteni biztonsági incidenseket."

- 3. szint: A tudatosítás és változás promóciója

„Ezen a szinten az a cél, hogy a viselkedésre legyünk hatással, és csökkentsük általa a szervezeti kockázatokat. Ez a szint már lényegesen nehezebben elérhető, mint az első kettő, és emiatt a szervezetek többsége nem éri el ezt a szintet. Ahelyett, hogy véletlenszerűen ad hoc anyagokat osztogatnánk, a tudatosító program azonosítja azokat a témaköröket, melyeknek a legnagyobb hatása van a szervezeti célok támogatására és alapvetően ezekre fókuszál. Ráadásul, a program már túlmegy az éves tréning eseményeken és a folyamatos ráerősítést alkalmazza. A kommunikált tartalom összehangolt és pozitív módon bátorítja a viselkedésváltozást a munkahelyen, otthon és utazás közben. Ennek eredményeképpen, az alkalmazottak, a megbízással dolgozók, és az egyéb személyzet is tisztában vannak a szervezeti szabályzatokkal, folyamatokkal és aktív módon előzik meg, észlelik és jelentik az incidenseket."

- 4. szint: A hosszútávú fenntarthatóság állapota

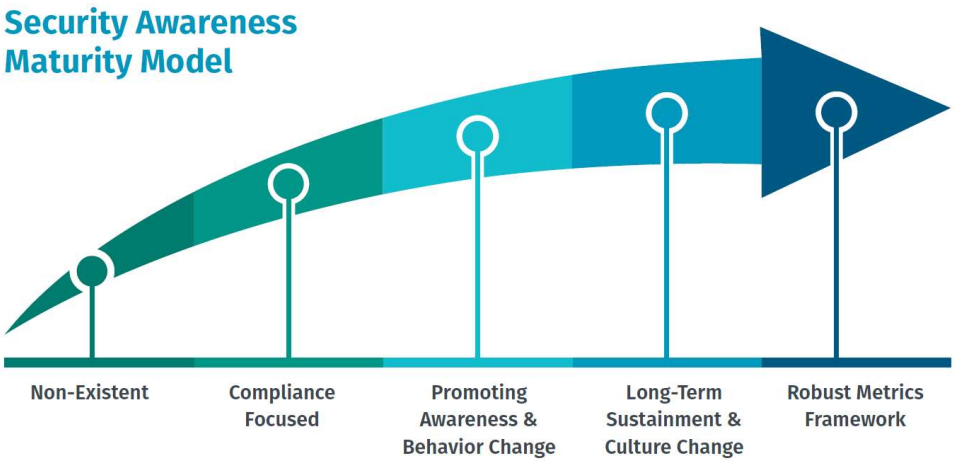
„A hosszútávú fenntarthatóság olyan létező programra épít, mely a tudatosságot és a változást segíti elő. A folyamatokat és erőforrásokat hosszútávú ciklusokban rendeli hozzá a programhoz és minimálisan évente felülvizsgálják és aktualizálják a kommunikált tartalmat és a kommunikációs módszereket. Ennek eredményeképpen a program a szervezeti kultúra megalapozott részévé válik, mindig aktuális és vonzó."

- 5. szint: Mérőszámok

„Ez a legfelsőbb szint, ahol a biztonság tudatosító programhoz már meghatározott mérőszámok vannak bevezetve, hogy az előrehaladást nyomon lehessen követni és ennek mérhető legyen a hatása. Eredményeképpen a program folyamatosan fejlődik és a beruházás megtérülését is képes bemutatni. Ezzel nem mondjuk azt, hogy az alacsonyabb érettségi szinteken ne használhatnánk mérőszámokat, hanem ez csak azt jelenti, hogy már van egy formalizált mérési programunk is."

(Spitzner (2012))

Ugyanezt a modellt mutatja be a SANS Institute (2017), 2017-es Információbiztonsági Tudatossági Jelentése (Security Awareness Report 2017) is, néhány kisebb változtatással az egyes szintek megnevezésében, ahogy azt a következő ábra is mutatja:



7. ábra: Az Információbiztonsági Tudatossági Érettségi Modell, SANS (2017)

Eredetileg ezt a modellt az információbiztonsági tudatosító *programok* érettségi szintjének értékelésére alakították ki, de a modell megközelítése, kialakítása, eszköztára teljesen megfelel céljainknak: Jól használhatjuk saját érettségi modellünk kialakításához, csak azokat a dimenziókat kell hozzáadnunk, melyek megfelelnek az információbiztonsági tudatosság fogalmára készített definíciónknak.

2.5 Egy saját érettségi modell az információbiztonsági tudatosság szintjének mérésére

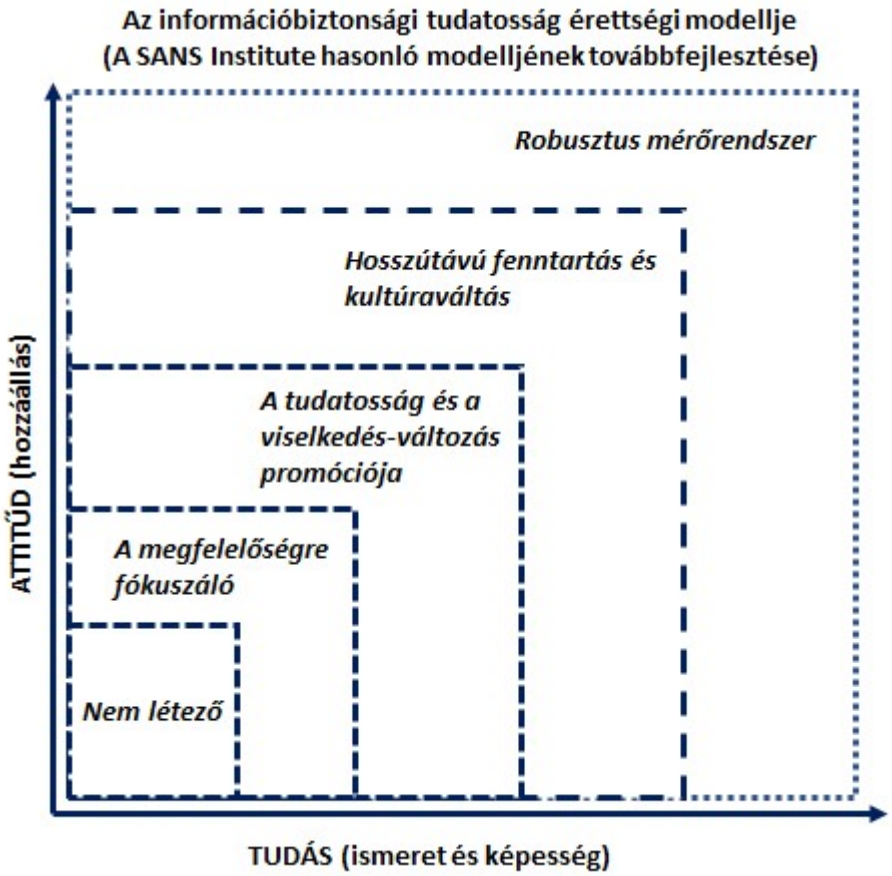
Ahogy azt az értekezés korábbi fejezeteiben is bemutattuk, számos különböző érettségi modell létezik, mely alkalmas lehet az információbiztonsági tudatosság mérésére.

A 2.2.3 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 kell megtennünk:

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

Ha mindezeket a feladatokat elvégezzük, akkor a rendelkezésünkre fog állni egy olyan modell, mely alkalmas lehet a validálásra. Nem feledve a fő célunkat, hogy egy auditálható, mérhető modellt kell alkotnunk, szükségünk van azoknak az objektív bizonyítékoknak az összegyűjtésére, melyek alkalmasak lehetnek az információbiztonsági tudatosság érettségi szintjének mérésére egy szervezetben.

Az alábbiakban leírt modellt alkalmasnak gondolom erre a célra. Az ajánlott modell vizualizált formában:



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

Ahogy azt már korábban is jeleztem, a „tudás" dimenzió magába foglalja mindazokat a képességeket is, melyek megadják az érintettek számára annak lehetőségét, hogy azt cselekedjék, amit a szervezetben egy létező kontroll elvár tőlük. Az „attitűd" dimenzió az aktív és pozitív viszonyulás mértéket mutatja meg az egyes információbiztonsággal kapcsolatos kontrollok és védelmi intézkedések kapcsán.

A szervezeti szintű információbiztonsági érettségi modell részletes leírása:

1. szint – A nemlétező: Információbiztonsági tudatosság gyakorlatilag nem létezik.
    - Tudás: A munkatársak nem gondolják, hogy célszemélyek lehetnek, és hogy tevékenységüknek lenne bármilyen közvetlen hatása a szervezet biztonságára, nem ismerik vagy nem értik a szervezeti szabályzatokat és könnyen lesznek áldozatai egy információbiztonsági természetű támadásnak.
    - Attitűd: A munkatársak semleges módon vagy ellenségesen viszonyulnak a biztonsággal kapcsolatos kötelezettségekhez / ügyekhez / potenciális incidensekhez.
    - Kontrollok: Nincsenek támogató kontrollok.
    - Érdekelt felek nézőpontja: Az érdekelt felek nincsenek meghatározva.
    - Audit bizonyítékok: Nincsenek.

2. szint – A megfelelőségre fókuszáló: Információbiztonsági tudatosító program már létezik, de kifejezetten a megfelelőségre vagy külső audit követelmények teljesítésére készült.
    - Tudás: A képzés éves vagy ad-hoc jellegű képzési eseményekre korlátozott.
    - Attitűd: A munkatársak bizonytalanok a szervezeti szabályzatok és/vagy saját szerepüket illetően a szervezet információs vagyonának védelme kapcsán.
    - Kontrollok: A beléptetési, kiléptetési, és a rendszeres képzési folyamat meghatározott, belső auditokat végeznek és dokumentálják is őket.
    - Érdekelt felek nézőpontja: Az ügyfelek, a beszállítók és az állam, mint érdekelt fél azonosítottak.
    - Audit bizonyítékok: 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. szint – A tudatosítás és a változás promóciója: Ez az információbiztonsági tudatossági szint egy olyan részletes kockázatérétkelésen alapul, mely egyértelműen megmutatja, hogy mely biztonsági témaköröknek van a legnagyobb hatása a szervezeti célok megvalósítására, és az információbiztonsági erőfeszítések ezekre a kulcstémakörökre fókuszálnak.
    - Tudás: A képzési program tovább megy az éves képzési eseményeken és folyamatos megerősítést biztosít az egész év során. Az érdekelt felek tudását, ismereteit rendszeresen tesztelik.
    - Attitűd: Az információbiztonsággal kapcsolatos tartalmak kellemes és pozitív módon vannak kommunikálva és bátorítják a viselkedésváltozást a munkában és otthon. Ennek eredményeképpen az emberek értik és követik a szervezeti szabályzatokban leírtakat és aktív módon észlelik, megelőzik és jelentik az incidenseket.
    - Kontrollok: Rendszeres vezetői áttekintéseket hajtanak végre. Az információbiztonsággal kapcsolatos projektek ellenőrzött körülmények között folynak.
    - Érdekelt felek nézőpontja: A munkatársak is érdekelt félként vannak figyelembe véve.
    - Audit bizonyítékok: 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. szint – A hosszútávú fenntarthatóság és szervezeti 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.

- Tudás: A változó kockázatokra és az észlelt incidensekre reflektáló és folyamatosan változó tananyag.
- Attitűd: Erős és pozitív megközelítés minden érdekelt fél részéről, a szabályok és szabályozások aktív módon követettek a munkahelyen, utazás közben és otthon.
- Kontrollok: Létezik egy hosszútávú tervezési folyamat és dokumentált eljárás, az információbiztonsági tudatossághoz kapcsolódó tananyagok, ismeretanyagok és kommunikálásuk módja pedig rendszeresen felülvizsgált.
- Érdekelt felek nézőpontja: Minden érdekelt fél azonosított és bevont a programba.
- Audit bizonyítékok: A programhoz kapcsolódó dokumentáció (projektek definiált halmaza, projekt és program jelentések), az információbiztonsági tudatosításhoz rendelt részletes költségvetés hosszabb időtávra (pl. három évre).

5. szint – Erős mérőszám rendszer: 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.
    - Tudás: A szervezet információbiztonsági tudatosítással kapcsolatos céljai ismertek minden érdekelt fél számára.
    - Attitűd: A szervezeti célokat minden érintett fél magáénak érzi és ezek a közös értékek a napi gyakorlatot is befolyásolják.
    - Kontrollok: Konzisztens mérőszám rendszer.
    - Érdekelt felek nézőpontja: Nincs mit hozzátenni az előző szinten megfogalmazottakhoz.
    - Audit bizonyítékok: 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.

Néhány fontos megjegyzés a bemutatott információbiztonsági érettségi modellhez:

- Nincsenek merev és éles határok az egyes szintek között. Néhány esetben a jó és rossz gyakorlatok átfedésbe lehetnek egymással és emiatt nem könnyű eldönteni, hogy melyik szint az igazán megfelelő egy szervezet jellemzésére.
- Egy magasabb szint mindig magába foglalja a jó gyakorlatokat a megelőző szintről. Ha valahol azt tapasztaljuk, hogy egy magasabb szint legjobb gyakorlata párhuzamosan létezik egy alacsonyabb érettségi szint rossz gyakorlatával, akkor az alacsonyabb érettségi szintbe kell besorolni az adott szervezetet.

Habár a „mérőszám rendszer” kifejezés csak a legmagasabb érettségi szinten említett, ez nem jelenti azt, hogy méréssel csak ezen az érettségi szinten lehet találkozni a modellben. A mérés minden érettségi szinten fontos. Az a tény, hogy a mérést csak a legmagasabb szinthez kötötten emlegetjük, pusztán csak azt üzeni, hogy egy igazán érett tudatosító program azt feltételezi, hogy nem csak képesek vagyunk a szervezeti magatartást és kultúrát megváltoztatni, de a változtatás képességét is demonstrálni tudjuk a mérőszám rendszer létével és működésével.

Mivel modellem alapstruktúráját tekintve megegyezik a SANS Institute (2018) által évente publikált jelentésben használt modellel, ezért adja magát a lehetőség, hogy közvetlenül összevessem az általuk publikált adatokat (pl. az egyes szervezeteknek az egyes érettségi szintek közötti megoszlását) a magyarországi felmérés adataival.

A témakör egy másik reprezentatív tudományos publikációja (Dzazali és Zolait (2012)) a strukturális egyenletek modelljeihez (SEM) nyúl, és azokat használja az érettségi szintek meghatározásához, ezért ebben a disszertációban sem kerülhetem meg, hogy ne próbáljam meg modelljüket – legalább részlegesen – értékelni egy hazai minta tükrében.

2.6 A strukturális egyenletek modelljei (SEM)

Már a kutatás viszonylag kezdeti stádiumában felmerült annak igénye, hogy a klasszikus ún. elsőgenerációs statisztikai módszereket (pl. faktoranalízis, regresszió elemzés) meghaladó módon foglalkozzak a szervezetek információbiztonsági tudatosságának érettségi szintjével, azaz találjak olyan sokváltozós statisztikai módszereket, melyek képesek számos változó egyidejű elemzésére.

Füstös és Tárnok (2017) nyomán az első- és másodgenerációs sokváltozós adatelemzési módszerek egy lehetséges osztályozását mutatja be a következő táblázat:

1. *táblázat: A sokváltozós adatelemzés módszereinek osztályozása (Füstös és Tárnok (2017) p. 1)*

A sokváltozós adatelemzés módszerei	**Elsődlegesen felderítő jellegű (exploratív)**	**Elsődlegesen megerősítő jellegű (konfirmatív)**
Elsőgenerációs módszerek	Klaszterelemzés	Varianciaelemzés
	Exploratív faktorelemzés	Logisztikus regresszió
	Sokdimenziós skálázás	Többváltozós regresszió
		Konfirmatív faktorelemzés
Másodgenerációs módszerek	Strukturális egyenletek modellje a parciális legkisebb négyzetek módszerével (SEM-PLS)	Kovariancián alapuló strukturális egyenletek modellje (SEM-ML)

A strukturális egyenletek modellezés során a kutatási kérdés alapján és a rendelkezésre álló adatoktól függően kell választanunk a megfelelő sokkváltozós adatelemzési módszerek közül. Konkrét esetünkben (lásd 2.5 fejezet) az információbiztonság tudatosság érettségi szintjét szeretném meghatározni olyan módon, hogy megvizsgálom, az adott szervezetben milyen kontrollok léteznek, működnek, és ennek alapján próbálom meg besorolni az öt előre definiált érettségi szint valamelyikébe a szervezetet.

Füstös és Tárnok (2017) szerint a módszerválasztás során a következőket kell figyelembe vennünk:

- melyek, milyenek a képzett változók
- milyen sajátosságai vannak a mérésnek
- milyen mérési skálát használunk
- hogyan folyik a kódolás
- és milyen lesz a változók eloszlása

A képzett változók a manifeszt változók lineáris kombinációi (Hair, Black, Babin, & Anderson, (2010)) és ez képletben kifejezve:

$$Y = w_1x_1 + w_2x_2 + \dots + w_mx_m$$

ahol x_i: a megfigyelt, manifeszt változók

w_i: a lineáris kombináció súlya

y: képzett, látens változó

A modellezés során nem csak egy képzett (látens) változónk lehet, és a megfigyelt (manifeszt) változók (m számú!) megfigyelési egységekre (n számú!) vonatkozó értékeit tartalmazza az adatmátrix, melynek struktúráját a következő táblázat mutatja be:

2. táblázat: Egy általános adatmátrix (saját szerkesztés)

Megfigyelési egységek	X_1	X_2	…	x_m	Képzett változó
1	X_{11}	X_{12}	…	X_{1m}	Y_1
⋮	⋮	⋮	⋮	⋮	⋮
i	X_{i1}	X_{i2}	…	X_{im}	y_i
⋮	⋮	⋮	⋮	⋮	⋮
n	X_{n1}	X_{n2}	…	x_{nm}	y_n

Esetünkben az egyes megfigyelési egységek az egyes kitöltött kérdőívek lesznek, ahol a tudatosság érettségi szintjét befolyásoló tényezőkre (x_1, x_2,…x_n) kérdezünk rá, és a képzett változónk pedig a tudatosság mértéke (érettségi szintje).

Modellünkben az érettségi szint (egytől ötig osztályozva) egy nagyon egyszerű sorrendi (ordinális vagy rendező) skálán értelmezhető: Azt tudjuk, hogy pl. a 3-as szinten lévő szervezet magasabb szinten áll, mint egy 2-es szintet képviselő szervezet, de nem fogjuk tudni megmondani, hogy mennyivel. Annyit viszont mindenképpen szeretnénk kimondani, hogy a 3-as szinthez milyen jellemző kontrollok és audit bizonyítékok tartoznak és ugyanerre a kérdésre tudnunk kell válaszolni a többi szint esetében is. Ugyanakkor az érettségi modellekre jellemző módon elvárjuk, hogy az alacsonyabb szint minden attribútuma legyen jelen a magasabb szint esetében is, azaz a jellemző kontroll és audit bizonyíték készletek minden egyes szinthez hozzárendelhetők legyenek.

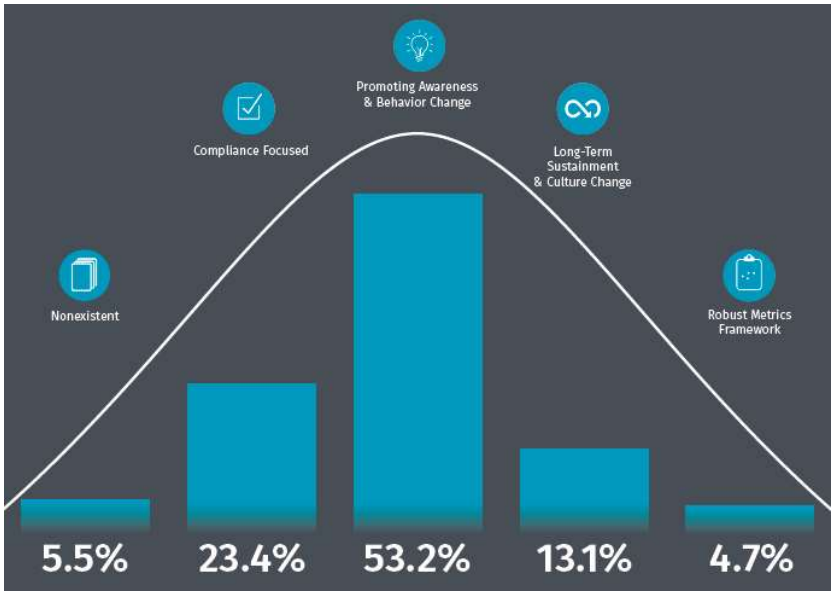
A társadalomtudományi mérésekre nagyon jellemző bizonytalanság miatt szinte minden esetben lesznek kivételek, mert nagyon nehéz az elmélet és a megfigyelés közötti egyértelmű kapcsolat bizonyítása: Minden konkrét esetben lehetnek olyan kontrollok és audit bizonyítékok, melyek jellemzően egy másik érettségi szinthez köthetők, de az adott szervezet specialitása miatt mégis megjelennek a vizsgált szervezet életében. Ugyanez fordítva is igaz állítás lehet, mert lesz majd olyan magasabbra taksált szervezet, melyben hiányozhatnak egy alacsonyabb érettségi szinthez tartozó kontrollok és audit bizonyítékok, de mégis a magasabb szintbe tudjuk sorolni bizonyos meghatározóan fontos kontrollok és audit bizonyítékok működése és létezése miatt.

A mérési problémát a 2.3 fejezetben járom körül részletesebben.

Hasonló kihívás a kódolás kérdése, amikor a mérés megkönnyítése érdekében a válaszok lehetséges kategóriához számokat rendelünk hozzá. A 2.6.2 fejezetben bemutatom annak a skálának a kódolását, melyet Dzazali és Zolait (2012) modelljének teszteléséhez használtam. Ott egy hétfokozatú Likert skálához rendeltem számokat úgy, hogy tudatában voltam annak, hogy ez egy ordinális mérési szintű skála lesz, ahol a szimmetrikusság és az attribútumok egyenlő távolsága sem biztosítható, tehát semmiképpen sem lesz közelítőleg intervallum mérési szintű a skálám.

Ráadásul olyan válaszlehetőséget is kódolnom kellett, amikor a válaszadó ismerethiány miatt nem tud a kérdésre válaszolni, tehát számára a hétfokozatú skálám egyetlen eleme sem értelmezhető. A problémát és vélelmezett megoldását a 3.3 fejezetben tárgyalom.

A 2.5 fejezetben ismertetett érettségi modellem ötfokozatú sorrendi skálát használ. A SANS Institute (2018) megegyező modellt alkalmazó 2018-as felmérése bemutatja egy 1700 megfigyelést tartalmazó nemzetközi mintán az egyes érettségi szintek közötti megoszlást:



9. ábra: A válaszok megoszlása az egyes érettségi szintek között a SANS Institute mérése alapján (SANS Institute (2018) p. 10)

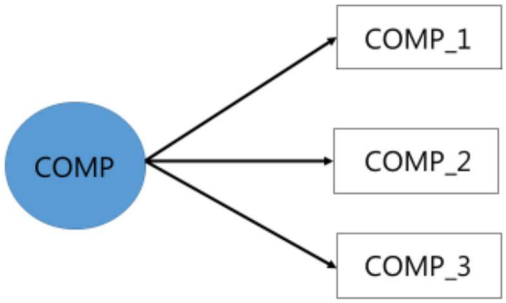
Az ábrán is látható, hogy hisztogrammjuk a normális eloszláshoz közelítő valószínűségeloszlást mutat. Hasonló, de statisztikai próbával alátámasztott, eloszlásvizsgálatot végzünk el a magyarországi mintán is a disszertáció 4.1.3 fejezetében.

Füstös és Tárnok (2017) felhívja arra is a figyelmet, hogy létezik egy ún. 10-szeres szabály, miszerint „a minta mérete nem lehet kisebb, mint 10-szer az indikátorok (látens változók) legnagyobb száma, amit a mérési modellekben találunk”. Mivel modellünkben több mint 10 különféle kontrollt (és audit bizonyítékot), azaz látens változót kívánunk a szervezeti érettségi szinthez kapcsolni, ezért a mintánknak (a megfigyelések számának) 100-as nagyságrendűnek kell lennie. Ez komoly kihívás, hiszen nehéz ilyen elemszámot elérni egy olyan kutatásban, mely egy viszonylag szűk szakmai közönséget céloz meg.

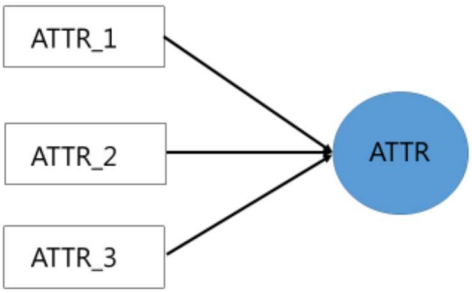
A strukturális egyenletek modelljének világában fontos szempont a modellválasztásnál, hogy reflektív vagy formatív modellel dolgozunk.

A reflektív mérési modell esetében a klasszikus mérési modell logika mentén azt tételezzük fel, hogy a mért manifeszt változókat egy látens, szisztematikus komponens hozza létre olyan módon, hogy némi véletlen hibával „gyártja le” a megfigyelt változókat (így működik pl. a faktorelemzés). Az érettségi modellünk pont fordítva működik, mert itt a látens változó (esetünkben az érettségi szint) a manifeszt változók (kontrollok és audit bizonyítékok együttese) lineáris kombinációjaként állíthatók elő.

A reflektív és formatív mérési modell különbségét érzékelteti a következő két ábra:



10. ábra: Reflektív mérési modell (forrás: Füstös és Tárnok (2017) p. 27)



11. ábra: Formatív mérési modell (forrás: Füstös és Tárnok (2017) p. 27)

A következő fejezetben egy formatív mérési modellen alapuló kísérletet mutatok be. Az ismertetett kísérlet részleges megismétlését egy magyarországi mintán a 2.6.2 és a 4.1.2 fejezetekben írtam le.

2.6.1 Egy kísérlet a szervezetek információbiztonsági tudatossági szintjének, érettségének meghatározására (Dzazali és Zolait modellje)

Dzazali és Zolait (2012) tanulmányukban malajziai közszolgálati szervezetek információbiztonsági tudatosságának érettségét vizsgálták és egy kovariancia-alapú strukturális egyenlet modelljét (Covariance Based Structural Equation Modeling – CB SEM) is alkalmazták eredményeik kinyerésére és bemutatására. Keresték a kapcsolatot a szervezeti tudatosság érettségi szintje és bizonyos szervezeti tényezők között. Ennek kapcsán hat hipotézist állítottak fel és vizsgáltak:

DZ-H1: A kockázatelemzési mechanizmusnak (Risk Management Mechanism - RM) pozitív hatása van az információbiztonsági tudatosság érettségére. (Information Security Maturity - ISM)

DZ-H2: A szervezeti struktúrának (Organisation Structure - OS) pozitív hatása van az információbiztonsági tudatosság érettségére. (ISM)

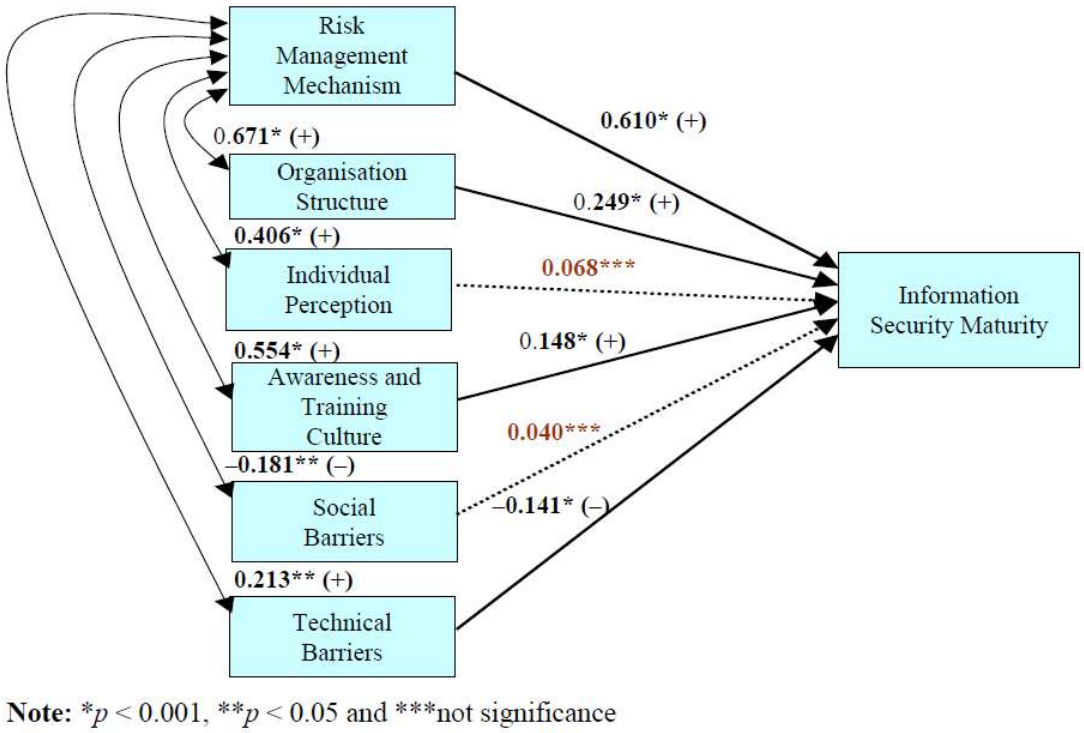
DZ-H3: Az információbiztonsági tudatosság fontosságnak személyes érzékelésének (Individual's Perceptions - IP) pozitív hatása van az információbiztonsági tudatosság érettségére. (ISM)

DZ-H4: A szervezeti tudatossági és képzési kultúrának (Awareness and training culture – AT) pozitív hatása van az információbiztonsági tudatosság érettségére. (ISM)

DZ-H5: A társadalmi korlátok (Social barriers – SB) negatív hatással vannak az információbiztonsági tudatosság érettségére. (ISM)

DZ-H6: A technikai (műszaki) korlátok (Technical barrier's – TB) negatív hatással vannak az információbiztonsági tudatosság érettségére. (ISM)

Modelljüket és eredményeiket az alábbi ábra foglalja össze:



12. ábra: Dzazali és Zolait mérési modellje és eredményei (2012)

Az eredményeik egy általuk konstruált regressziós modellben kifejezve (ISM – Information Security Maturity – Információbiztonsági érettség):

$$ISM = 7.426 + 1.060\ (RM) + 0{,}807\ (OS) + 0{,}426\ (AT) - 1{,}015\ (TB)$$

A képzett, látens változó (ISM) a manifeszt változók (RM, OS, AT, TB) lineáris kombinációi. Ez egy jellemzően exploratív modell, melyben a függő változó (ISM) varianciáját próbálja a lehető legjobban megmagyarázni, reprodukálni.

A kapott regressziós modell több érdekes következtetést hordoz:

- A szervezet kockázatértékelési mechanizmusa és a szervezeti struktúra erősen meghatározza az információbiztonsági tudatosság érettségét, miközben a két tényező egymásra gyakorolt hatása is jelentős.
- A szociális korlátok és a személyes érzékelés minősége nem igazán van hatással az érettségre.
- Közepesen erős és pozitív hatást hordoz a szervezeti tudatosság és tréning kultúra.
- A technikai (műszaki) korlátok enyhe negatív kapcsolatot mutatnak az érettséggel.

Dzazali és Zolait (2012) tanulmányukban a hat tényezőcsoportot számos alkérdésre bontva vizsgálták. A disszertációban kísérletet teszek ennek a modellnek a részleges magyarországi reprodukciójára és vizsgálatára egy kérdőíves felmérés formájában. A mérés lefolyását és az eredményeket a 4.1.2 fejezet tárgyalja.

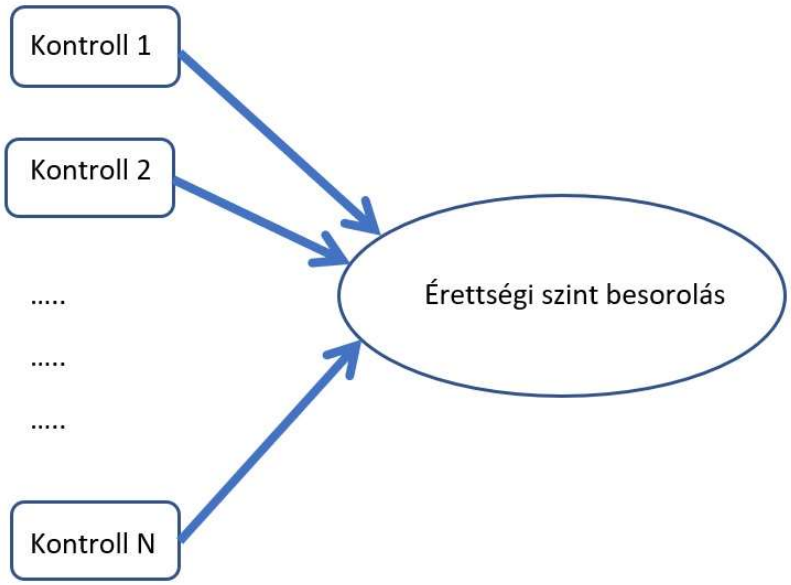
Dzazali és Zolait (2012) modelljét és módszertanát felhasználva és némileg meghaladva kísérletet tettem magyarországi szervezetek vizsgálatára annak érdekében, hogy meghatározzam azokat a tényezőket, melyek jellemző módon hatnak egy szervezet információbiztonsági kultúrájára, azaz az információbiztonság érettségi szintjére. A következő fejezet tárgyalja a modellalkotást, a vizsgálati eredményeket a 4. fejezet, a következtetéseket pedig az 5. fejezet mutatja be.

2.6.2 Magyarországi szervezetek információbiztonsági tudatosságának érettségi szintjének vizsgálata a SEM alkalmazásával

Az első kutatási kérdésem (RQ1) arra irányult, hogy hogyan értékelhető a gazdálkodó szervezetekben az információbiztonsági tudatosság szintje, minősége a szervezet szintjén. A már hivatkozott Spitzner (2012) féle Security Awareness Maturity Model egy ötfokozatú érettségi modellel operál.

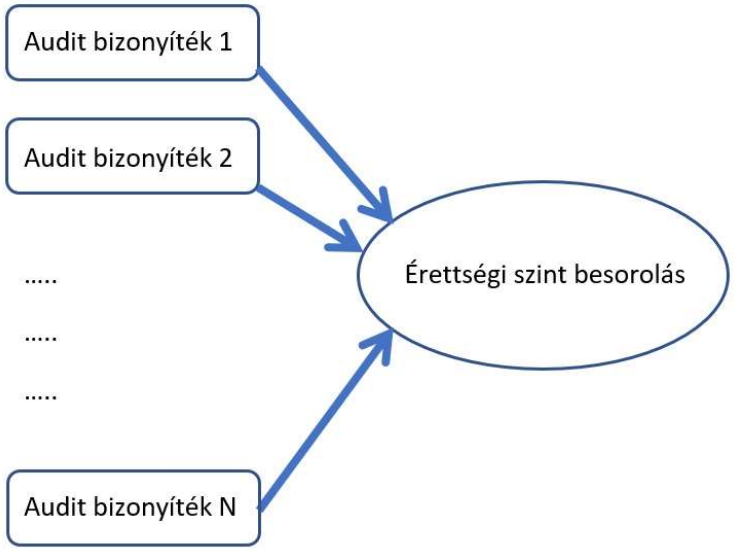
Ha szeretnénk az egyes szervezeteket ebben az ötfokozatú modellben elhelyezni, akkor azt érdemes vizsgálnunk, hogy a szervezetnél azonosított kontrollok mely érettségi szinthez köthetők, azaz egy olyan ún. formatív modellben érdemes gondolkodnunk, ahol az egyes kontrollok léte vagy nem léte meghatározza a szervezet besorolását a modellben.

Általánosabban szólva, formatív mérési modellem a kontrollok esetében a következőképpen néz ki:



13. *ábra: Az érettségi szint és az egyes kontrollok kapcsolata egy formatív mérési modellben (saját ábra)*

Hasonló modell alkalmazható az audit bizonyítékok esetében is. Itt a formatív modell így fest:



14. *ábra: Az érettségi szint és az egyes audit bizonyítékok kapcsolata egy formatív mérési modellben (saját ábra)*

A fenti két formatív modell működőképessége jól vizsgálható egy kérdőíves felméréssel, ahol az egyes szervezetek képviselői számára bemutatom a tudatosságot megteremtő vagy fokozó lehetséges kontrollokat és megkérem a válaszadókat, hogy a szervezetében azonosított kontrollok alapján sorolja be szervezetét a számára bemutatott érettségi modellben. Az egyes kontrollok említési gyakorisága és a szervezet besorolása összekapcsolható és vizsgálhatom a kapcsolati erősséget (korrelációt) az egyes kontrollok megléte és a szervezet érettségi szintje között.

Hasonló módon vizsgálhatók az audit-bizonyítékok is: A kérdőívben felsorolom a lehetséges audit-bizonyítékokat és megkérem a válaszadókat, hogy jelöljék a szervezetükben fellelhető audit-bizonyítékokat és ugyanakkor sorolják be szervezetüket az érettségi modell szerint. Az audit-bizonyítékok említési gyakorisága és a szervezet besorolása összekapcsolható és vizsgálhatóvá válik a kapcsolati erősség (korreláció) az egyes audit bizonyítékok fellelhetősége és a szervezett érettségi szintje között.

A disszertáció 3.4 és 4.1 fejezeteiben azt a kérdőíves felmérést és eredményeit mutatom be, melyben a fentebb ismertetett formatív mérési modelleket alkalmaztam.

2.7 A kutatási kérdéseim a szakirodalom tükrében

A kutatás kezdetén megfogalmazott kutatási kérdéseimre már a szakirodalmi áttekintés is érdekes válaszokat szolgáltatott. Az alábbiakban foglalom össze a szakirodalomból tanulmányozásból levonható következtetéseket az egyes kutatási kérdéseink mentén:

RQ1: HOGYAN ÍRHATÓ LE, HOGYAN ÉRTÉKELHETŐ A GAZDÁLKODÓ SZERVEZETEKBEN AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG SZINTJE, MINŐSÉGE A GAZDÁLKODÓ SZERVEZET SZINTJÉN?

MEGÁLLAPÍTÁS: A SZAKIRODALOM TANULMÁNYOZÁSA RÁVILÁGÍTOTT ARRA A MEGLEPŐ TÉNYRE, HOGY IGAZÁBÓL NINCS KOHERENS ÉS KONZISZTENS DEFINÍCIÓJA AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁGNAK. SZÁMOS SZERZŐ SZÁMOS MEGKÖZELÍTÉSBEN TÁRGYALJA A TÉMÁT, AZ ÉRTEKEZÉSBEN KITÉREK ERRE A DEFINÍCIÓS PROBLÉMÁRA, ÉS BEMUTATOK EGY LEHETSÉGES DEFINÍCIÓT, MELY A KÉSŐBBI KUTATÓ MUNKA ALAPJA IS LEHET.

RQ2: MÉRHETŐ-E A VÁLTOZÁS (JAVULÁS, ROMLÁS) EGY GAZDÁLKODÓ SZERVEZET ÉLETÉBEN A TUDATOSSÁG ÉRETTSÉGI SZINTJE VONATKOZÁSÁBAN?

MEGÁLLAPÍTÁS: EGY SZERVEZET VEZETŐJE SZÁMÁRA EZ ALAPVETŐ KÉRDÉS, ÉS EZT A KÉRDÉST MEGVÁLASZOLANDÓ A MÉRHETŐSÉG KÉRDÉSKÖRÉT JÁROM KÖRÜL KUTATÁSOM EGYIK ELEMEKÉNT. MEGVIZSGÁLTAM, HOGY MELY MÉRÉSI SKÁLÁK HASZNÁLATA LEHETSÉGES EGY ILYEN VIZSGÁLAT SORÁN.

RQ3: Q3: ÖSSZEHASONLÍTHATÓK-E A GAZDÁLKODÓ SZERVEZETEK AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGE SZEMPONTJÁBÓL SZERVEZETI SZINTEN?

MEGÁLLAPÍTÁS: SZERVEZETI SZINTEN AZ ÖSSZEHASONLÍTHATÓSÁGOT TÁMOGATJÁK AZ ÚN. ÉRETTSÉGI / KIVÁLÓSÁGI MODELLEK, MELYEK A SZERVEZETI MŰKÖDÉS SZÁMOS TERÜLETÉRE SZÜLETTEK MEG. A SZERVEZETI INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI MODELLJÉNEK EGY VÁZLATOS LEÍRÁSÁT ADJA A SANS INSTITUTE 2012-BEN PUBLIKÁLT MODELLJE. KUTATÁSOM SORÁN EZT A MODELLT FELHASZNÁLVA ÉS TOVÁBB FEJLESZTVE KÍVÁNOK EGY OBJEKTÍVNEK TEKINTHETŐ MÉRŐRENDSZERT LÉTREHOZNI, MELY ALKALMAS LEHET A MÉRÉSEKKEL KAPCSOLATOS TUDOMÁNYOS KRITÉRIUMOK (PL. MEGISMÉTELHETŐSÉG) TELJESÍTÉSÉRE.

RQ4: Q4: Támogatható-e a tudatosság értékelés hagyományos audit eszközökkel (pl. ellenőrző listák)?

Megállapítás: Auditorként is dolgozva azt tapasztalom, hogy bizonyos kontrollok megléte vagy hiánya utal a szervezet információbiztonsági tudatosságának érettségére, szintjére. Kutatásom eredményeképpen javaslatot teszek egy ilyen kontroll leltár létrehozására, mely segítségével egy adott gazdálkodó szervezet információbiztonsági tudatosságának érettségi szintje mérhetővé válhat.

A disszertáció 2. fejezetében a szakirodalmi kutatás eredményeit foglaltam össze. A 3. fejezet a gyakorlati kutatás módszertanát, a 4. fejezet pedig a konkrét kutatási eredményeket mutatja be.

3 A GYAKORLATI KUTATÁS MÓDSZERTANA

A disszertáció ezen fejezete az alkalmazott gyakorlati kutatási megközelítést és módszertant mutatja be.

A kutatás részletes terve mellett szólok azokról a módszertani választási lehetőségekről, melyekből építkeztem és megindokolom a ténylegesen választott utat.

3.1 Módszertani választások a gyakorlati kutatás kapcsán

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:

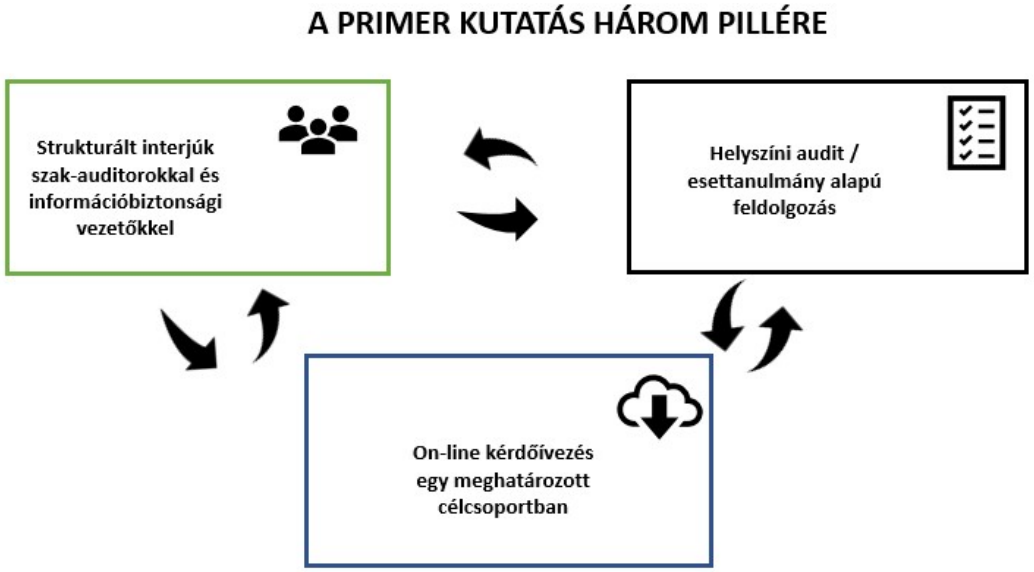
- Dzazali és Zolait (2012) már hivatkozott modelljét kívántam hazai környezetben részlegesen reprodukálni és tesztelni kérdőíves módszerrel. A 3.3-as fejezetben szólok részletesebben ennek a modellnek az alkalmazásáról.
- Spitzner (2012) érettségi modelljéhez minden évben kapcsolódik egy világszintű 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 3.3-as fejezetben bemutatom a kérdőívem kapcsolatát a hivatkozott érettségi modellel.

3.2 A gyakorlati kutatás pilléreinek kapcsolata

A gyakorlati kutatás három pillére:

- On-line kérdőívezés egy meghatározott célcsoportban
- Strukturált interjúk szakauditorokkal és információbiztonsági vezetőkkel
- Esettanulmány alapú feldolgozás / Információbiztonsági tudatosság érettségi szintjének megállapítása helyszíni audit alapján

A 15. ábra mutatja az egyes pillérek kapcsolatát:



15. ábra: A gyakorlati kutatás pilléreinek kapcsolata (saját ábra)

A három pillér kapcsolata:

- 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 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).

A három gyakorlati kutatási pillér részletesebben:

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

Statisztikai értelemben releváns méretű mintán kívántam értékelni a létrehozott érettségi modellt. Ennek érdekében az alábbi szakmai csoportokat akartam elérni egy on-line kérdőívvel:

- A Hétpecsét Információbiztonsági Egyesület levelező listájának tagjai (kb. 2200 személy, akik jelentős része gyakorló információbiztonsági szakember, szakauditor, tanácsadó)
- Az ISACA Budapest Chapter tagsága (kb. 550 személy, gyakorló auditorok, tanácsadók, kockázatmenedzserek az IT területén)
- Az EIVOK tagsága (kb. 150 személy, gyakorló információbiztonsági vezetők jellemzően a közigazgatási, államigazgatási szférából)

A három lista jelentős átfedéseket tartalmaz, de így is kb. 2000 egyedi célszemély volt azonosítható rajtuk, és egy kb. 30 %-os válaszadási hajlandósággal számolva ez egy 600 fős reprezentatív mintát szolgáltathatott volna, mely nagyjából 500 szervezetet fedhet le Magyarországon. Az átlagost lényegesen meghaladó válaszadási hajlandóságot azért tételeztem fel, mert az említett szakmai közösségekben olyan mértékű a szerepvállalásom, hogy jó eséllyel kaphattam volna a szokásost jóval felülmúló arányban értékelhető válaszokat ebből a körből.

Sajnos a gyakorlat nem igazolta ezt a feltételezésemet, és a kb. 2000 fős megcélzott körnek csak alacsony hányada válaszolt, így meg kellett elégednem egy 122 fős mintanagysággal. Ezt a megfigyelés számot csak úgy tudtam elérni, hogy megengedtem a kérdőív hagyományos kézi kitöltését is, és a válaszokat én rögzítettem az on-line felületen. Ráadásul a kérdőív igen hosszú ideig volt elérhető a kitöltők számára, mert ezzel is próbáltam a kitöltési gyakoriságot növelni. Az adatbázis időbélyegei szerint az első kitöltés 2018. december 23.-án valósult meg, és az utolsó bejegyzés 2019. november 24.-én történt, azaz 11 hónapnyi időablak állt rendelkezésre. Hivatalosan 2019. december 1.-én zártam le az on-line kérdőívet. Összesen négy különböző típusú rendezvényen, két-két alkalommal ismertettem a kutatási kezdeményezést és az előzetes kutatási eredményeket, hogy minél több releváns kitöltőhöz jusson el az információ:

- A Hétpecsét Egyesület Információbiztonsági Fórumai (2018.11.21. és 2019.11.20.)
- ISACA Budapest Chapter 2. szerdák (2018.10.10. és 2019.11.13.)
- EIVOK Klub Estek (2018.11.29. és 2019.10.03.)
- OGIK éves konferenciák (2018.11.09. és 2019.11.08.)

Ezeket az alkalmakat egészítették ki olyan egyetemi kurzusok (Metropolitan Egyetem, Budapest Corvinus Egyetem), ahol post graduális hallgatók csoportjai kapták kézhez a kérdőívet vagy annak on-line linkjét QR-kód formájában. Minden alkalommal mutatkozott némi kitöltői aktivitás, de messze nem a remélt mértékben. Utólag elemezve a kitöltési hajlandóság viszonylagos alacsony szintjét, arra a következtetésre jutottam, hogy a kérdőív a két modell (Dzazali és Zolait (2012) illetve Spitzner (2012)) egyidejű verifikálási szándéka miatt túl hosszúra sikeredett, és ezért csökkent a kitöltői hajlandóság. Valószínűleg, egy kétfelé vagy még több részre bontott, és emiatt lényegesen rövidebb kérdőív több kitöltőt vonzhatott volna.

A kérdőív kitöltői megőrizhették anonimitásukat, mert a név és e-mail cím megadása (1. – 2. kérdés) nem volt kötelező, és ezzel a személyes adatok kezelésével kapcsolatos kihívások egy része alól is mentesülhettem, mert nem szerettem volna valamilyen GDPR (2016) alapú adatkezelési problémát generálni a kutatással.

A kérdőívek feldolgozása során vizsgált szociológiai jellemzők (3. – 6. kérdés):

- A kitöltőnek a szervezetben elfoglalt helye, szerepe (a SANS Institute 2018-as Awareness Report-ja által használt osztályozás szerint) (2018)
- A szervezet mérete (létszám alapján: mikro, kis, közép és nagyméretű)
- A szervezet működési területe / iparága
- A szervezet jellege (non profit / for profit)

Ezek a szociológiai jellemzők tudatosan lettek kiválasztva, mert a kapott válaszokból reméltem, hogy fontos részhipotézisekre kaphatok választ:

- A szervezet mérete befolyásolja a szervezet érettségi szintjét. – Azt feltételeztem, hogy a nagyobb méretű szervezetek általában magasabb információbiztonsági tudatossági érettségi szintet képviselnek.
- A szervezet jellege befolyásolja a szervezet érettségi szintjét. – Azt gondoltam, hogy a „for profit" szféra szereplői magasabb érettségi szinten állnak.

A kutatás ezirányú eredményeit az értekezés 4. fejezete tárgyalja.

Szerettem volna azt is vizsgálni, hogy a kérdőívet kitöltők szervezetben elfoglalt helye befolyásolja-e az általuk vélelmezett érettségi szintet, de ez a vizsgálat meghiúsult, mert a kitöltők több mint 12 féle szervezeti pozíciót adtak meg, és ilyen mintanagyság (122 kitöltő) mellett érdemi statisztikai vizsgálat nem volt végezhető. Próbáltam a szervezeti pozíció kérdéskörét vizsgálhatóvá tenni olyan módon, hogy a szervezeti pozíciókat két alcsoportba (menedzseri pozíciók kontra szakértői pozíciók) rendeztem és így elemeztem az általuk végzett besorolás eredményeit. Itt egy újabb részhipotézist állítottam fel:

- A kitöltő menedzseri vagy szakértői pozíciója befolyásolja a besorolás eredményét. – Azt vélelmeztem, hogy a menedzserek jellemzően magasabb „osztályzatot" adnak szervezeteiknek, mint a mélyebb ismeretekkel rendelkező szakértők.

A kutatási eredményeknek ezt a dimenzióját is az értekezés 4. fejezete tárgyalja.

A kérdőív II. szekciója (7. – 20. kérdés) Dzazali és Zolait (2012) modelljének részleges reprodukciójára alapult, hogy ezen keresztül vizsgálható legyen modelljük alkalmazhatósága és helytállósága egy magyarországi mintán. A kérdőívem II. szekciójának 14 kérdésével próbáltam lefedni a három meghatározó és pozitív komponenst a hivatkozott tanulmány hat komponenséből:

3. *táblázat: Dzazali és Zolait hipotézisei és a kapcsolódó kérdőív kérdései (saját szerkesztés)*

A Dzazali-Zolait (2012) féle modell hat komponense (konstrukciója) és a hozzájuk kapcsolódó hipotéziseik (H1-H6)	Az adott komponenshez (és így az adott hipotézishez) kapcsolódó kérdés az on-line kérdőívemben (a válaszokat Likert-skálán értékelve kértem be)
DZ-H1: A kockázatkezelési mechanizmusnak (Risk Management Mechanism - RM) pozitív hatása van az információbiztonsági tudatosság érettségére.	Az információbiztonsági kockázatokat minden működési folyamat kapcsán azonosítják és figyelembe veszik.
	A szervezet számára kritikus információkat és informatikai infrastruktúra elemeket (pl. hálózati elemek, alkalmazások stb.) azonosították.
	Hatékony menedzsment eljárásokat / kontrollokat határoztak meg a veszélyekkel, fenyegetettségekkel szemben.
	Az információs rendszerek sérülékenységeit és a kapcsolódó folyamatokat rendszeresen azonosítják.
	A biztonsági eseményekre a felsővezetés azonnal reagál.
DZ-H2: A szervezeti struktúrának (Organisation Structure - OS) pozitív hatása van az információbiztonsági tudatosság érettségére.	Az információbiztonsági szervezeti egység képviselői fontos szerepet játszanak az információbiztonsággal kapcsolatos döntéshozatali folyamat irányításában.
	Az átfogó információbiztonsági szervezet működését értékelik és hozzáigazítják a változó feltételekhez.
	Az információbiztonsági szervezeti egység vagy annak képviselői találkoznak az üzleti / szolgáltató szervezeti egységek vezetőivel, hogy megértsék azok üzleti (működési) céljait és információbiztonsági igényeit.
	Az információbiztonsági tudatosságot a szervezet valamennyi tagja számára rendszeresen kommunikálják.
DZ-H3: Az információbiztonsági tudatosság fontosságnak személyes érzékelésének (Individual's Perceptions - IP) pozitív hatása van	*Kérdőívünkben ezt a komponenst nem vizsgáltuk, mert a hivatkozott szerzők*

az információbiztonsági tudatosság érettségére.	*regressziós modelljébe nem került be ez a komponens az elhanyagolható hatása miatt.*
DZ-H4: A szervezeti tudatossági és képzési kultúrának (Awareness and training culture – AT) pozitív hatása van az információbiztonsági tudatosság érettségére.	Az informatikai rendszerek felhasználóit oktatják arra, hogy a gyanús tevékenységeket azonosítsák és jelentsék.
	A munkatársak rendszeresen vesznek részt információbiztonsági tréningeken.
	Az informatikai rendszerek felhasználóit világos utasításokkal látták el az adatok osztályozásával kapcsolatban a digitális adatfeldolgozó műveletek kapcsán.
	A munkatársakat világos utasításokkal látták el az adatok osztályozásával kapcsolatban a manuális adatfeldolgozó műveletek kapcsán.
	Az információbiztonsági tudatosságról szóló tájékoztató anyagok tartalma és formája szabványosított.
DZ-H5: A társadalmi korlátok (Social barriers – SB) negatív hatással vannak az információbiztonsági tudatosság érettségére.	*Kérdőívünkben ezt a komponenst nem vizsgáltuk, mert a hivatkozott szerzők regressziós modelljébe nem került be ez a komponens az elhanyagolható hatása miatt.*
DZ-H6: A technikai (műszaki) korlátok (Technical barrier's – TB) negatív hatással vannak az információbiztonsági tudatosság érettségére.	*Kérdőívünkben ezt a komponenst nem vizsgáltuk, mert a hivatkozott szerzők regressziós modelljében ez egy negatív befolyásoló tényezőként került be.*

A hivatkozott tanulmány (Dzazali és Zolait (2012)) hat hipotéziséből a magyarországi mintán azt a hármat vizsgáltam, melyek a regressziós modelljük szerint erős és pozitív kapcsolatot mutatnak egy szervezet információbiztonsági tudatossági érettségével. Elhanyagolható hatásuk miatt a tanulmányban közölt regressziós modellben már nem jelenik meg a DZ-H3 és DZ-H5 hipotézisek által érintett két komponens („Személyes érzékelés" és „Szociális korlátok"). A DZ-H6 hipotézis („Technikai korlátok") által érintett komponens pedig negatív hatást fejt ki a tudatosság érettségi szintjére. Emlékeztető gyanánt a már korábban is említett regressziós modell:

$$ISM = 7.426 + 1.060\ (RM) + 0{,}807\ (OS) + 0{,}426\ (AT) - 1{,}015\ (TB)$$

Mivel a kérdőív hosszát is figyelembe kellett vennem a szerkesztéskor, hiszen minél hosszabb a kérdőív, annál alacsonyabb a kitöltési hajlandóság, ezért is indokolt volt egy jelentős kérdéscsokor (DZ-H3, DZ-H5, DZ- H6 hipotézisekhez kötődő kérdések) elhagyása.

A II. szekcióban kizárólag 7 fokozatú Likert-skálákkal dolgoztam, ahol a kódolás a következőképpen történt:

07 – Teljes mértékben egyetértek

06 – Nagyrészt egyetértek

05 – Csak kismértékben értek egyet

04 – Közömbös számomra

03 – Nem túlságosan értek egyet

02 – Nagyrészt nem értek egyet

01 – Egyáltalán nem értek egyet

Ugyanakkor megadtam a lehetőséget, hogy a válaszadónak ne kelljen nyilatkoznia olyan tényezőről, melyről beosztásánál, szakmai szerepénél fogva nincs kellő ismerete vagy az általa képviselt szervezetben nem értelmezhető az adott tényező:

00 – Nincs róla információm / Nem értelmezhető a szervezetben

Mivel általánosan elfogadott (Füstös, Tárnok, (2017) p. 18), hogy ha a hiányzó adatok száma meghaladja a 15 %-ot, akkor ezeket a megfigyeléseket törölni illik az adatbázisból, ezért a kérdőívekre adott válaszok feldolgozáskor kihagytam azokat a válaszadókat, akik a II. szekció 14 db kérdésből több mint 2 kérdésnél a „Nincs róla információm / Nem értelmezhető a szervezetben" választ adták.

Az extrém értékekkel bíró (outlier) megfigyeléseket hiányzó adatként kezeltem és az adott megfigyelést (egy adott válaszadó által kitöltött teljes kérdőívet) listaszerű törlésnek vetettem alá. Bár viszonylag alacsony megfigyelés számmal (122 darab kitöltött kérdőív) zárult a kérdőíves adatgyűjtés, mégis kizártam 48 megfigyelést a hiányos kitöltés, illetve a válaszokban tetten érhető inkonzisztencia miatt. A kizárás oka volt például az, ha a válaszadó a majdnem legmagasabb érettségi szintbe sorolta szervezetét úgy, hogy ugyanakkor alig 1-2 kontrolt és 1-2 audit bizonyítékot jelölt meg a kérdőív IV. és V. szekciójában, ami logikai ellentmondás, hiszen, ha a szervezetben nincs jelen semmilyen jó gyakorlat, akkor hogyan várható el az érett tudatos magatartás.

A törölt megfigyelések viszonylag magas aránya (39 %!) még azzal is magyarázható, hogy a Likert-skála kódolásakor módszertani hibát követtem el azzal, hogy „0-s" értéket rendeltem a „Nincs róla információm / Nem értelmezhető a szervezetben" típusú válaszokhoz, ugyanis ezzel az értékkel a válaszok konverziója során a létező legnagyobb különbséget (7 – 0 = 7) építettem be a használt korrelációs képletekbe, ami nyilvánvalóan meghamisítaná az eredményeket.

A kérdőívünk III. szekciójában kellett a kitöltőknek az általuk képviselt szervezetet egy ötfokozatú érettségi modellben besorolni. Ez az öt fokozat megfelel Spitzner 2012-ben publikált érettségi modelljének és megegyezik a 2.5 fejezetben ismertetett saját modell fokozataival is. Ez az egyezőség lehetőséget kínált a SANS Institute évente publikált Security Awareness Report 2018-as és 2019-es kiadásában megjelent adatokkal történő összevetésre (SANS Institute (2018), SANS Institute (2019)). A két nemzetközi és a magyar minta eloszlás-képeit és az abból levonható következtetéseket a 4.1.3 fejezetben mutatom be.

A IV. szekció tartalmazta a szervezeti tudatosság érettségére jellemzőnek vélt kontrollokat, melyekből a kitöltők szabadon válogathattak, illetve akár újabb kontrollt is megadhattak. Szándékos volt a kitöltési sorrend megfordítása, mert arra is kíváncsi voltam, hogy a kitöltők mennyire képesek az általuk választott érettségi szinttel összekapcsolni a szervezetükben létező, működő kontrollokkal. A kontrollok említési sorrendje szándékosan eltért a modellben leírt és az egyes érettségi szintekhez rendelt sorrendtől, hogy ne befolyásoljam a kitöltőt a modell elméleti struktúrájával, azaz maga a modell is validálható legyen a válaszok tükrében (mely érettségi szinthez mely kontrollok létét kapcsolja a kitöltő).

Az V. szekcióban helyeztem el az audit bizonyítékok listáját a IV. szekcióhoz hasonló logika mentén. A kitöltők itt is megadhattak olyan bizonyítékokat, melyek nem szerepeltek az előre elkészített listában, melyből tetszőleges számú elemet választhattak. Az audit bizonyítékok listája szándékosan kevert lista volt, azaz nem az egyes érettségi szintek sorrendjében lettek felsorolva a tételek, hogy ezzel is biztosítsam a befolyásolásmentes kitöltését.

Az egyes szociológiai jellemzők összefüggéseit (rang-korreláció) vizsgáltam a gazdálkodó szervezet által képviselt érettségi szintek függvényében, hogy az alábbi kérdésekre tudjak matematikailag megalapozott választ adni:

- A szervezet jellege befolyásolja-e az érettségi szintjét, azaz pl. a „for profit” szervezetek átlagos érettségi szintje magasabb-e?
- A szervezet mérete befolyással van-e az érettségi szintre, azaz pl. egy mikro-vállalat átlagosan alacsonyabb szintet képvisel-e?
- A szervezetek különböző pozíciójú tagjai másképp értékelik-e az érettségi szintet, azaz pl. egy elsőszámú vezető jellemzően magasabbra értékeli-e a szervezeti teljesítményt?
- A szervezet tevékenységének jellege (iparági besorolása) befolyásolja-e az érettségi szintjét, azaz pl. egy pénzügyi szolgáltató szervezet átlagos érettségi szintje magasabb-e a minta átlagáénál?

Ez utóbbi kérdés a kapott mintában megint csak nem volt vizsgálható, mert annyira sokszínű lett a kép a szervezetek által képviselt iparágak szempontjából (több mint 10 féle iparág reprezentánsai kerültek be a mintába!), hogy az egyes kitöltői csoportokba tartozó egyedszám statisztikai elemzésre elégtelen mennyiségű lett.

A kapott válaszok számossága és megoszlása a többi kérdés vonatkozásában a statisztikai elemzéshez elégséges minta nagyságot produkált. A következtetéseket a 4.1 fejezetben ismertetem.

A személyes adatokkal kapcsolatosan szigorodó törvényi szabályozás (GDPR (2016)) figyelembevételével igyekeztem minimalizálni a kérdőívezés során kezelt személyes adatok körét. Mivel a vizsgálat szempontjából amúgy sem volt releváns, hogy a kérdőív kitöltőjének mi a neme, illetve mekkora az életkora, emiatt ilyen demográfiai jellegű adatokat nem kérdeztem. Következésképpen a kitöltők sokaságának demográfiai típusú elemzését nem végeztem el ezen adatok hiányában.

A kérdőív III., IV. és V. szekciójához kapcsolható és vizsgált hipotézisek:

- KH1: Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több kontroll azonosítható a működésében.

- KH2: Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több audit bizonyítékot szolgáltat.
- KH3: Minél több tudatosító kontrollt működtet egy szervezet, annál több audit bizonyíték keletkezik a szervezetben.
- KH4: Az üzleti vállalkozások jellemzően magasabb információbiztonsági tudatosság érettségi szintet képviselnek, mint a non-profit szervezetek.
- KH5: A nagyobb szervezetek jellemzően magasabb érettségi szintet képviselnek.
- KH6: A menedzserek jellemzően magasabbra értékelik szervezetüket az érettség szempontjából, mint a szervezetben dolgozó szakértők.
- KH7: Az egyes érettségi szintekhez tartozó jellemző kontrollok a vizsgált mintában azonosíthatók és ezáltal maga a kidolgozott érettségi modell megfelelősége is igazolható.
- 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.

A kérdőívekre kapott és megtisztított válaszokat és a belőlük levont következtetéseket a 4.1 fejezet tárgyalja.

3.4 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.

Kvale (1996) az interjúkészítés folyamatának hét szakaszát különbözteti meg, és kutatásom során igyekeztem ezeket a szakaszokat betartani:

- Tematizálás: a célom egyértelműen az volt, hogy a kérdőíves megkérdezéssel szerzett információkat ellenőrizzem, és a modell validálásához szükséges háttérinformációkat megszerezzem,
- Tervezés: a kérdőív lezárása után egy nagyjából kéthetes periódusba szerveztem az interjúkat, hogy az „élmények” még viszonylag frissek legyenek az interjúalanyok számára,
- Interjúzás: az interjúk nagyjából egy-másfélórás időkeretekben zajlottak,
- Leírás: nem használtam diktafont, hogy ne feszélyezzem az interjúalanyokat, de kulcsszavakra fókuszáló feljegyzéseket készítettem,
- Elemzés: kerestem a visszatérő kulcsszavakat és megállapításokat az interjúvázlatokban,
- Verifikálás: igyekeztem ütköztetni az egyes interjúalanyok által elmondottakat saját kérdőíves válaszaival, illetve a kérdőívek összefoglaló eredményeivel,
- Tudósítás: az értekezés 4.2 fejezete tartalmazza megállapításaimat.

A mélyinterjúk előre rögzített interjúvázlat alapján zajlottak és a következő főbb pontokat tartalmazta:

- A kiválasztott szervezet működési jellemzőinek azonosítása (méret, iparág, jelleg stb.)
- A szervezet képviselője hogyan értelmezi az információbiztonsági tudatosságot
- A szervezetben működő információbiztonsági kontrollok leltára
- Fizikai kontrollok
- Adminisztratív kontrollok
- Műszaki (technikai) kontrollok
- A szervezetben a tudatosság (a tudás és az attitűd nyomai, bizonyítékai) jellemzői
- Létező információbiztonsági programok és azok eredményei
- Információbiztonsággal kapcsolatba hozható mérőszámok és mérések a szervezet gyakorlatában
- A szervezet önértékelésének eredményei (mely érettségi szintre sorolta be magát és milyen elvek mentén).

A szervezetek önértékelése kiváló lehetőséget biztosított a modell működőképességének értékelésére, hiszen a kutatói / szerzői szándéktól függetlenül értelmezték az érettségi modell egyes elemeit, és ha ez az értelmezés pl. nem működik az önértékelés során, akkor az egyértelmű bizonyítékot szolgáltat a modell gyenge pontjaira nézve.

A mélyinterjúk tartalmát és következtetéseit a 4.2 fejezetben tárgyalom.

3.5 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.

A cél az volt, hogy hagyományos audit technikákkal találjak minden érettségi szintre (1-5 fokozat) legalább egy minta szervezetet. Ezek a célzott auditok voltak hivatottak olyan további információk gyűjtésére, melyek alapján a modell működőképességének értékelése és „finomhangolása” még pontosabban megtörténhetett.

A helyszíni auditokra előzetes ellenőrző-lista készült, mely a vizsgálandó témaköröket határozta meg:

- A kiválasztott szervezet működési jellemzőinek azonosítása (méret, iparág, jelleg stb.)
- A szervezet hogyan értelmezi az információbiztonsági tudatosságot
- A szervezetben működő információbiztonsági kontrollok leltára
    - Fizikai kontrollok
    - Adminisztratív kontrollok
    - Műszaki (technikai) kontrollok
- A szervezetben a tudatosság (a tudás és az attitűd nyomai, bizonyítékai) jellemzői
- Létező információbiztonsági programok és azok eredményei
- Információbiztonsággal kapcsolatba hozható mérőszámok és mérések a szervezet gyakorlatában

- Az audit összefoglaló eredménye (az auditor mely érettségi szintre sorolja be a szervezetet és milyen elvek mentén).

A gyakorlati kutatás fentiekben ismertetett három pillére remélhetően kellő alapot biztosított a kutatási kérdések megválaszolásához.

3.6 A kutatási kérdéseim a gyakorlati kutatás tükrében

Ahogy azt a 1.3.2 fejezetben is megemlítettem, a gyakorlati kutatás a következő kutatási kérdésekre fókuszál:

RQ1:	HOGYAN ÍRHATÓ LE, HOGYAN ÉRTÉKELHETŐ A GAZDÁLKODÓ SZERVEZETEKBEN AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG SZINTJE, MINŐSÉGE A GAZDÁLKODÓ SZERVEZET SZINTJÉN?
RQ2:	MÉRHETŐ-E A VÁLTOZÁS (JAVULÁS, ROMLÁS) EGY GAZDÁLKODÓ 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)?

4 A GYAKORLATI KUTATÁS EREDMÉNYEI

Ebben a fejezetben a gyakorlati kutatás három pillére mentén megszerzett tapasztalataimat és a kutatási eredményeimet foglaltam össze.

4.1 A kérdőív alkalmazásával megszerzett tapasztalatok

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 IIII. 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 modell egyes érettségi fokaihoz kapcsoltan.

A három kutatási irány eredményeit részleteiben a következő fejezetekben tárgyalom.

4.1.1 A MAGYAR KÉRDŐÍVES MINTA ÁLTALÁNOS JELLEMZŐI

A minta egyes általános jellemzőinek összefüggéseit (rang-korreláció) vizsgáltam a szervezet által képviselt érettségi szintek függvényében, hogy az alábbi kérdésekre megalapozott választ tudjak adni:

- A szervezet jellege befolyásolja-e az érettségi szintjét, azaz pl. a „for profit" szervezetek átlagos érettségi szintje magasabb-e?
- A szervezet tevékenységének jellege befolyásolja-e az érettségi szintjét, azaz pl. egy pénzügyi szolgáltató szervezet átlagos érettségi szintje magasabb-e a minta átlagáénál?
- A szervezet mérete befolyással van-e az érettségi szintre, azaz pl. egy mikro-vállalat átlagosan alacsonyabb szintet képvisel-e?
- A szervezetek különböző pozíciójú tagjai másképp értékelik-e az érettségi szintet, azaz pl. egy elsőszámú vezető jellemzően magasabbra értékeli-e a szervezeti teljesítményt?

A válaszadási hajlandóság alacsony szintje miatt ez utóbbi kérdés a kapott mintában végül nem volt közvetlenül vizsgálható, mert annyira sokszínű lett a kép a kitöltők szervezeti szerepe, funkciója szempontjából (több mint 12 lehetséges szerep és funkció köszönt vissza a kitöltőktől kapott válaszok alapján!), hogy az egyes kitöltői csoportokba tartozó egyedszám statisztikai elemzésre elégtelen mennyiségű lett. Nem szerettem volna a vizsgálatnak ezt az aspektusát teljesen kihagyni az elemzésből, ezért egy kicsit más megközelítésben próbáltam választ keresni az utolsó kérdésre is. A 4.1.3 fejezet mutatja be ennek a vizsgálatnak az eredményét.

4.1.2 A DZAZALI ÉS ZOLAIT MODELL VIZSGÁLATA A MAGYAR MINTÁN

Dzazali és Zolait (2012) már hivatkozott modelljét kívántam a hazai környezetben reprodukálni és tesztelni a kérdőíves módszerrel. A 3.3-as fejezetben már részletesebben kifejtettem ennek a modellnek az alkalmazását, de fontos megjegyeznünk, hogy míg ők kovariancia-alapú strukturális egyenletek módszerét alkalmazták, addig az általam választott modell variancia-alapú volt. Ennek oka, hogy ők az elméletük tesztelését és megerősítését tekintették elsődleges prioritásnak, én pedig az előrejelzésre és a modell fejlesztésére helyeztem a hangsúlyt.

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).

Ahogy azt már a 3.3-as fejezetben is jeleztem, a hivatkozott tanulmány (Dzazali és Zolait (2012)) hat hipotéziséből a magyarországi mintán csak azt a hármat vizsgáltam, melyek az ő regressziós modelljük szerint erős és pozitív kapcsolatot mutatnak egy szervezet információbiztonsági tudatossági érettségi szintjével.

Az eredeti modellel összhangban, mind a három hipotézishez tartoztak állítások (RM1-RM5, OS1-OS4, AT1-AT5), melyeket a magyar válaszadóknak is egy Likert skálán kellett értékelniük. A három hipotézist és a hipotézisekhez kapcsolódó állításokat foglalja össze a 4. táblázat:

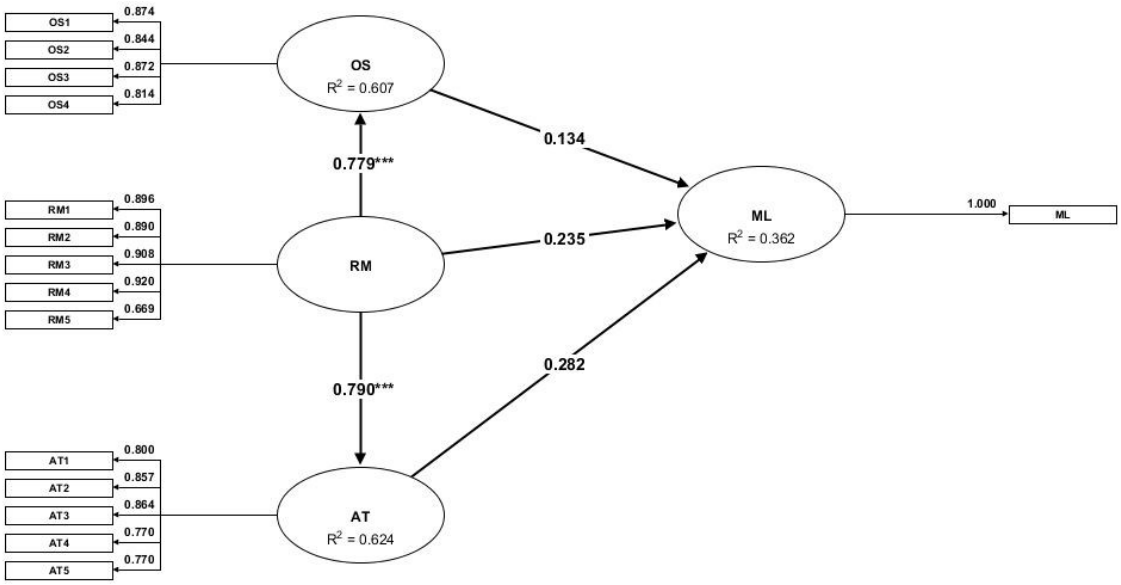
4. táblázat: Az általam vizsgált három hipotézis Dzazali és Zolait (2012) hat hipotézise közül (saját szerkesztés)

A Dzazali-Zolait (2012) féle modell hat komponenséből az a három, melyet a kérőívemmel vizsgáltam és a hozzájuk kapcsolódó hipotézisek (H1, H2, H4)	Az adott hipotézishez kapcsolódó kérdések az on-line kérdőívemben (a válaszokat Likert-skálán értékelve kértem be)
DZ-H1: A kockázatkezelési mechanizmusnak (Risk Management Mechanism - RM) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (Maturity Level – ML).	RM-1: Az információbiztonsági kockázatokat minden működési folyamat kapcsán azonosítják és figyelembe veszik.
	RM-2: A szervezet számára kritikus információkat és informatikai infrastruktúra elemeket (pl. hálózati elemek, alkalmazások stb.) azonosították.
	RM-3: Hatékony menedzsment eljárásokat / kontrollokat határoztak meg a veszélyekkel, fenyegetettségekkel szemben.
	RM-4: Az információs rendszerek sérülékenységeit és a kapcsolódó folyamatokat rendszeresen azonosítják.
	RM-5: A biztonsági eseményekre a felsővezetés azonnal reagál.
DZ-H2: A szervezeti struktúrának (Organisation Structure - OS) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (Maturity Level – ML).	OS-1: Az információbiztonsági szervezeti egység képviselői fontos szerepet játszanak az információbiztonsággal kapcsolatos döntéshozatali folyamat irányításában.
	OS-2: Az átfogó információbiztonsági szervezet működését értékelik és hozzáigazítják a változó feltételekhez.
	OS-3: Az információbiztonsági szervezeti egység vagy annak képviselői találkoznak az üzleti / szolgáltató szervezeti egységek vezetőivel, hogy megértsék azok üzleti (működési) céljait és információbiztonsági igényeit.
	OS-4: Az információbiztonsági tudatosságot a szervezet valamennyi tagja számára rendszeresen kommunikálják.
DZ-H4: A szervezeti tudatossági és képzési kultúrának (Awareness and training culture – AT) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (Maturity Level – ML).	AT-1: Az informatikai rendszerek felhasználóit oktatják arra, hogy a gyanús tevékenységeket azonosítsák és jelentsék.
	AT-2: A munkatársak rendszeresen vesznek részt információbiztonsági tréningeken.
	AT-3: Az informatikai rendszerek felhasználóit világos utasításokkal látták el az adatok osztályozásával kapcsolatban a digitális adatfeldolgozó műveletek kapcsán.
	AT-4: A munkatársakat világos utasításokkal látták el az adatok osztályozásával kapcsolatban a manuális adatfeldolgozó műveletek kapcsán.
	AT-5: Az információbiztonsági tudatosságról szóló tájékoztató anyagok tartalma és formája szabványosított.

A kérdőívezés során nyert válaszokat erős szűrésnek kellett alávetnem a hiányos és emiatt sokszor nyilvánvalóan inkonzisztens kitöltés miatt, és így a 122 kitöltésből 74 elemezhető maradt.

A modell 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.

Az első és így minden konstrukciót és minden az egyes konstrukciókhoz kapcsolódó állítást tartalmazó modell futtatási eredményei az alábbi ábrában foglalhatók össze:



16. ábra: Az első strukturális modell és az eredmények (saját ábra az ADANCO modell alapján)

Az ábrából az látható, hogy az igazolni szándékozott három hipotézis egyike sem tűnik szignifikánsnak a magyar mintában (DZ-H1: RM → ML; DZ-H2: OS → ML; DZ-H4: AT → ML), ellenben az OS, RM és AT konstrukciók közötti kapcsolat szignifikáns és erős.

Az első futtatáskor az is kiderült, hogy a mérési modell minőségi kritériumai közül az egyik legfontosabb, a diszkriminációs érvényesség (discriminant validity – Heterotrait - Monotrait Ratio of Correlations – HTMT legyen 0,85-nél kisebb), nem teljesül a konstrukciók vonatkozásában:

5. táblázat: A HTMT értékei az egyes konstrukciók között az első strukturális modellben (saját szerkesztés az ADANCO futási eredményei alapján)

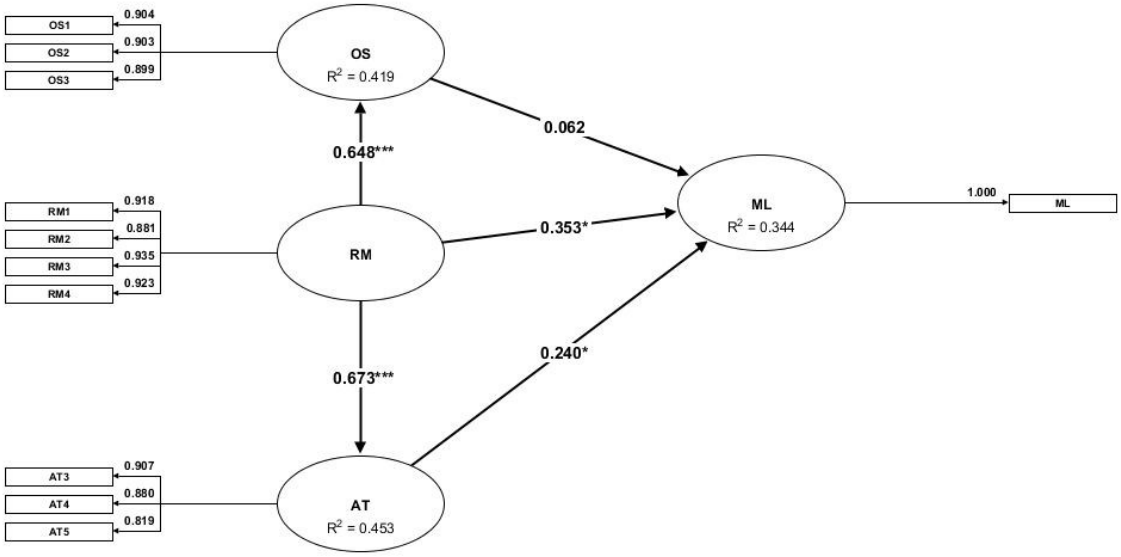
Konstrukció	RM	OS	AT	ML
RM				
OS	0,8578			
AT	0,8807	0,8225		
ML	0,5891	0,5424	0,6059	

A konstrukciók ebben az első modellben nem válnak el egymástól elég élesen a magyar mintán. Érződik, hogy az eredeti Dzazali-Zolait (2012) féle modell a magyar mintán „nem működik jól”, az egyes konstrukciókban lévő állítások túlságosan átfedésben vannak egymással.

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:



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

A modell négy összefüggő konstrukciója:

- OS (Organisational Structure) = szervezeti struktúra
- RM (Risk Management Mechanism) = kockázatmenedzselési mechanizmus
- AT (Awareness and training culture) = szervezeti tudatossági és képzési kultúra
- ML (Maturity Level) = érettségi szint

A kérdőívre kapott válaszok értékelése nélkül, csak a szakmai tapasztalataimra alapozva helytállónak vélelmeztem Dzazali-Zolait (2012) kiinduló feltételezéseit:

- ***DZ-H1:*** *A kockázatelemzési mechanizmusnak (**Risk Management Mechanism - RM**) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (**Maturity Level – ML**).* Minden információbiztonsági irányítási rendszernek alapelme, kiinduló pontja a kockázatelemzés és annak eredménye, hiszen ehhez rendelnek hozzá kockázatokat kezelő (mérséklő) intézkedéseket, melyek közvetlen módon hatnak a munkatársak napi információbiztonsági tevékenységére. Például, ha a menedzsment a kockázatelemzés eredménye nyomán az adathalászati tevékenységtől fél, akkor olyan tudatosító kontrollt fog bevezetni (rendszeres imitált adathalász levelek kiküldése a munkatársaknak), mely a tudatosság egy magasabb szintje felé „löki” a szervezetet, és máris adódik a kapcsolat a két konstrukció között.

- *DZ-H2: A szervezeti struktúrának (**Organisation Structure - OS**) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (**Maturity Level – ML**).* A szervezeti felépítés a cégkultúrát alapjaiban befolyásoló elem. Elég csak a jelentési láncok hosszára és tagoltságára gondolnunk. Ha van egy incidens, akkor annak jelentése vagy eltitkolása szervezeti struktúrától függő kulturális elem. Egy hosszú jelentési lánc egy hierarchikus szervezetben leszoktatja a munkatársakat arról, hogy aktívan jelentsék az észlelt incidenseket és egyre inkább abban válnak érdekeltté, hogy az eseteket elfedjék, elfelejtsék. Máris látszik, hogy egy laposabb szervezeti struktúra előnyösebb az információbiztonsági tudatosság kultúrájának egy magasabb szintjének elérése szempontjából.
- *DZ-H4: A szervezeti tudatossági és képzési kultúrának (**Awareness and training culture – AT**) pozitív hatása van az információbiztonsági tudatosság érettségi szintjére (**Maturity Level – ML**).* A szervezeti működés minden dimenziójában lényegi elemként szoktunk tekinteni a képzésre, tudatosításra. Ha ezt magas szinten végezzük a szervezetben, akkor annak közvetlen hatása van az emberi viselkedésre: Ha tudom, hogy mit és miért kell csinálnom (például miért kell komplex jelszavakat használnom), akkor az visszahat arra, hogy lesz-e belső motivációm a helyes és elvárt magatartás megvalósítására. Ez általában annyira sikeres nevelő tevékenység, hogy az emberek a jó gyakorlatokat átviszik a privát életükbe is (pl. a jelszókomplexitási szabályokat a privát hozzáféréseik esetében is betartják, mert érzik a hasznosságukat).

Amennyiben a 16. ábrán bemutatott végső strukturális modell minőségi (jósági) kritériumai teljesülnek, akkor a kiválasztott három hipotézis (DZ-H1, DZ-H2, DZ-H4) a magyar mintán is igazolhatóvá válik, mert a pozitív és enyhén szignifikáns kapcsolatok mindhárom esetben számszerűsítettek.

Ennek kimondásához vizsgáljuk meg a főbb minőségi (jósági) kritériumokat a felrajzolt modell esetében:

A konvergencia érvényesség (Convergent Validity) teljesülésére használt mutató az AVE (Average Variance Extracted / átlagos kivonatolt variancia), ahol a 0,5-ös értéket kell meghaladni minden egyes konstrukció esetében (HAIR et al. (2012)). Ez bőven teljesül a modellem esetében, ahogy ez az alábbi táblázat is mutatja:

6. táblázat: A négy konstrukció AVE értékei (saját szerkesztés az ADANCO futási eredményei alapján)

Konstrukció / Construct	Average variance extracted (AVE)
RM	0,8361
OS	0,8137
AT	0,7561
ML	1,0000

A diszkriminancia érvényességét a Fornell-Larcker (1981) teszt alapján mértük, mely szerint az AVE mutatónak minden esetben nagyobbnak kell lennie, mint a konstrukciók közötti korreláció négyzete. A 7. táblázatból látható, hogy ez a kritérium is teljesül:

7. táblázat: Fornell-Larcker kritérium teljesülését bemutató táblázat (saját szerkesztés az ADANCO futási eredményei alapján)

Konstrukció	RM	OS	AT	ML
RM	0,8361			
OS	0,4193	0,8137		
AT	0,4526	0,2943	0,7561	
ML	0,3072	0,1769	0,2610	1,0000

Az AVE értékek a táblázat diagonálisában láthatók. A diagonális alatt a négyzetes korreláció (squared correlation) értékei olvashatók.

Összegezve megállapítható, hogy van statisztikai bizonyíték a négy konstrukció létezésére, és arra, hogy a mért változók megfelelő indikátorai a hozzájuk kapcsolódó faktoroknak.

A PLS (Partial Least Squares – parciális legkisebb négyzetek módszere) modellezésben jelenleg jellemzően egyetlen modell-illeszkedési mutatót használnak, az SRMR-t, amelynek küszöbértéke 0,08 (Hu – Bentler, (1999)). Az általam felrajzolt modell illeszkedése megfelelő, mivel az SRMR (Standardized Root Mean Square Residual – standard reziduális négyzetes középérték) kisebb a küszöbértéknél:

Goodness of model fit (estimated model) SRMR = 0,0637

A konstrukciók megbízhatóságát (Construct reliability) igazoló kritériumok értékeit egy táblázatban foglaltam össze:

8. táblázat: A konstrukciók megbízhatóságát igazoló kritériumok és értékeik (saját szerkesztés az ADANCO futási eredményei alapján)

Konstrukció	Dijkstra-Henseler's rho (ρ_A)	Jöreskog's rho (ρ_c)	Cronbach's alpha(α)
RM	0,9351	0,9533	0,9345
OS	0,8863	0,9291	0,8856
AT	0,8396	0,9027	0,8376
ML	1,0000	1,0000	

A végső strukturális modell és a kapcsolódó eredmények alapján az látható, hogy a hipotézisek ekkor elfogadhatók a magyar mintán is:

- **DZ-H1:** A kockázatkezelési 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**).

A konstrukciók egymásra gyakorolt hatását foglalja össze a következő táblázat:

9. táblázat: A konstrukciók egymásra gyakorolt hatása (saját szerkesztés az ADANCO futási eredményei alapján)

Hatás	Eredeti koefficiens (Béta)	Standard bootstrap results				
		Mean value	Standard error	t-value	p-value (2-sided)	p-value (1-sided)
RM -> OS	0,6475	0,6515	0,1214	5,3321	0,0000	0,0000
RM -> AT	0,6727	0,6726	0,0943	7,1369	0,0000	0,0000
RM -> ML	0,3526	0,3164	0,1688	2,0888	0,0370	0,0185
OS -> ML	0,0622	0,1200	0,1944	0,3198	0,7492	0,3746
AT -> ML	0,2399	0,2151	0,1169	2,0528	0,0403	0,0202

A hipotéziseim szempontjából lényeges hatásokat a táblázat utolsó három sora tartalmazza, melyből látszik, hogy a kockázatértékelési mechanizmus (RM) van leginkább hatással az érettségi szintre (ML).

Mindez a gyakorlat számára azt üzeni, hogy amennyiben szeretnénk a szervezetekben a tudatosság érettségi szintjét növelni, akkor van értelme olyan kontrollok bevezetésének, melyek támogatják a kockázatkezelési mechanizmusokat (pl. kockázatmenedzsment eljárás bevezetése és működtetése), érdemes a szervezeti struktúrában erősíteni az információbiztonsági szervezet szerepét, és van tényleges hatása annak, ha a munkatársakat rendszeresen és célzottan képezzük.

Csak emlékeztető gyanánt az értekezés 62. oldalán már bemutattam Dzazali-Zolait (2012) eredményeit egy általuk konstruált regressziós modellben kifejezve (ISM – Information Security Maturity – Információbiztonsági érettség):

$$ISM = 7.426 + 1.060\ (RM) + 0{,}807\ (OS) + 0{,}426\ (AT) - 1{,}015\ (TB)$$

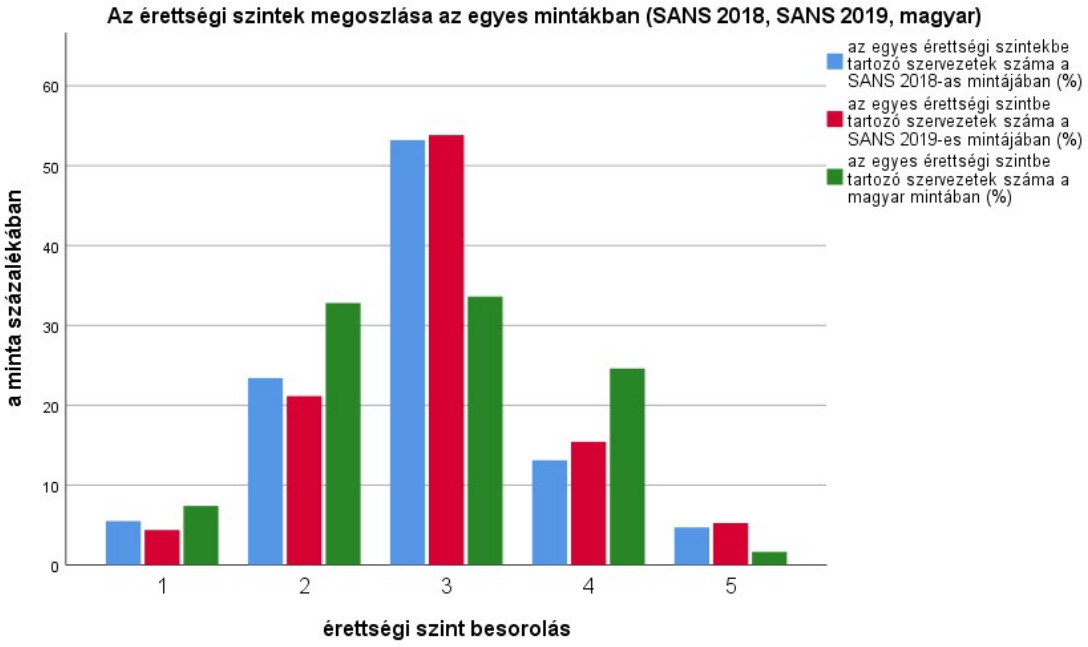
Tulajdonképpen ezzel részben egybe cseng a magyar minta eredménye, mert nálam is az RM konstrukcióhoz tartozik a legerősebb koefficiens (0,3526), de ugyanakkor a mi mintánkban az OS konstrukció koefficiense (0,0622) lényegesen alulmúlja az AT konstrukció koefficiensét (0,2399). Erre a különbségre egy magyarázatot tudok elképzelni: Dzazali és Zolait cikkében malajziai közszolgálati szervezetek képviselői körében töltötték ki a kérdőívüket, és a közszolgálat jóval hierarchizáltabb („félkatonai") működésű, tehát a kitöltők automatikusan nagyobb szerepet tulajdoníthattak a szervezeti struktúrának, hierarchiának, mint a jóval vegyesebb magyar minta, így a maláj közszolgák ösztönszerűen erősebben pontozták ezt a szervezeti hatást. Az értekezés kereteit meghaladja ennek a vélelmezett hatásnak a vizsgálata, de egy jövőbeni kutatási irányként érdemes megemlékeznünk róla.

Dzazali és Zolait (2012) modellje után vizsgáljuk meg a kérdőívek tükrében Spitzner (2012) modelljét, és elemezzük a magyar és nemzetközi minta közötti hasonlóságokat és különbözőségeket.

4.1.3 Spitzner modelljének értékelése a magyar mintán

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.



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

A három mintán végeztem normalitás vizsgálatot, melynek eredményeit az alábbi táblázat foglalja össze:

10. *táblázat: Normalitás vizsgálat a három mintán (saját szerkesztés)*

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
az egyes érettségi szintekbe tartozó szervezetek száma a SANS 2018-as mintájában (%)	0,234	5	,200*	0,832	5	0,144
az egyes érettségi szintbe tartozó szervezetek száma a SANS 2019-es mintájában (%)	0,277	5	,200*	0,827	5	0,133
az egyes érettségi szintbe tartozó szervezetek száma a magyar mintában (%)	0,222	5	,200*	0,865	5	0,249

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

4.1.4 A MAGYAR MINTA STATISZTIKAI JELLEMZŐINEK VIZSGÁLATA A MEGALKOTOTT ÉRETTSÉGI MODELL TÜKRÉBEN

A két nemzetközi és a magyar minta összevetése után a magyar mintán vizsgáltam néhány hipotézist, hogy a kidogozott modellt részleteiben tesztelhessem.

4.1.4.1 Az érettségi szintbe sorolás és a szervezet által bevezetett kontrollok közötti összefüggés elemzése

Az első vizsgált hipotézis:

- KH1: Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több kontroll azonosítható a működésében.

A 122 kérdőíves választ az IBM SPSS Statistics (version 25) statisztikai elemző szoftverével dolgoztam fel:

11. *táblázat: Az említett kontrollok száma és az érettségi szint besorolás táblázatos formában összefoglalva (saját szerkesztés az SPPS eredményei alapján)*

Említett kontrollok száma * Besorolás Crosstabulation

		Besorolás					
		1	2	3	4	5	Total
Említett kontrollok száma	0	1	1	4	0	0	6
	1	5	8	2	4	0	19
	2	1	6	8	3	1	19
	3	0	11	6	3	0	20
	4	2	6	3	3	0	14
	5	0	5	7	1	1	14
	6	0	1	5	4	0	10
	7	0	1	2	4	0	7
	8	0	1	2	3	0	6
	9	0	0	2	2	0	4
	10	0	0	0	2	0	2
	11	0	0	0	1	0	1
Total		9	40	41	30	2	122

Elvégeztem egy Spearman-féle rang-korreláció vizsgálatot, melynek eredményeit az alábbi táblázat mutatja be:

12. *táblázat: Spearman féle rangkorreláció vizsgálat eredményei a kontrollok száma és az érettségi szint kapcsolatában (saját szerkesztés az SPPS eredményei alapján)*

Symmetric Measures

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	0,387	0,074	4,594	,000[c]
Ordinal by Ordinal	Spearman Correlation	0,362	0,082	4,261	,000[c]
N of Valid Cases		122			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

Az eredmény gyenge-közepes kapcsolatot mutat igen alacsony elsőfajú hiba elkövetési valószínűség mellett.

4.1.4.2 Az érettségi szintbe sorolás és a szervezet által szolgáltatott audit bizonyítékok közötti összefüggés elemzése

Hasonló vizsgálatot végeztem el az audit bizonyítékok vonatkozásában, ahol az alábbi nullhipotézissel éltem:

- KH2: Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több audit bizonyítékot szolgáltat.

A vizsgálat eredményeit az alábbi táblázat foglalja össze:

13. *táblázat: Az említett audit bizonyítékok száma és az érettségi szint besorolás táblázatos formában összefoglalva (saját szerkesztés az SPPS eredményei alapján)*

Említett audit bizonyítékok száma * Besorolás Crosstabulation							
		Besorolás					Total
		1	2	3	4	5	
Említett audit bizonyítékok száma	1	1	1	4	1	0	7
	2	3	6	7	7	0	23
	3	1	6	2	0	0	9
	4	1	10	4	2	1	18
	5	3	5	4	4	0	16
	6	0	3	8	1	0	12
	7	0	3	4	2	0	9
	8	0	2	2	4	1	9
	9	0	3	3	0	0	6
	10	0	1	1	3	0	5
	11	0	0	1	1	0	2
	12	0	0	0	2	0	2
	13	0	0	1	1	0	2
	16	0	0	0	2	0	2
Total		9	40	41	30	2	122

Itt is elvégeztem egy Spearman-féle rang-korreláció vizsgálatot, melynek eredményeit szintén egy táblázatban foglaltam össze:

14. *táblázat: Spearman féle rangkorreláció vizsgálat eredményei az audit bizonyítékok száma és az érettségi szint kapcsolatában (saját szerkesztés az SPPS eredményei alapján)*

Symmetric Measures					
		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	0,298	0,077	3,422	,001[c]
Ordinal by Ordinal	Spearman Correlation	0,244	0,088	2,761	,007[c]
N of Valid Cases		122			
a. Not assuming the null hypothesis.					
b. Using the asymptotic standard error assuming the null hypothesis.					
c. Based on normal approximation.					

Az eredmény gyenge-közepes kapcsolatot sejtet alacsony elsőfajú hiba elkövetési valószínűség mellett.

4.1.4.3 A szervezet által bevezetett kontrollok és a szervezet által szolgáltatott audit bizonyítékok közötti összefüggés vizsgálata

Az érettségi modell alkalmazhatóságának egyik legfontosabb kérdése az, hogy vajon a szervezetben működő kontrollok „kitermelik-e" a szükséges audit bizonyítékokat, azaz a több kontroll több bizonyítékot termel a szervezeti érettség kapcsán.

Ezt a feltételezést is formába öntöttem:

- KH3: Minél több tudatosító kontrollt működtet egy szervezet, annál több audit bizonyíték keletkezik a szervezetben.

15. *táblázat: Az említett audit bizonyítékok száma és az említett kontrollok száma táblázatos formában összefoglalva (saját szerkesztés az SPPS eredményei alapján)*

Említett audit bizonyítékok száma * Említett kontrollok száma Crosstabulation														
		Említett kontrollok száma												Total
		0	1	2	3	4	5	6	7	8	9	10	11	
Említett audit bizonyítékok száma	1	5	0	0	1	1	0	0	0	0	0	0	0	7
	2	1	13	7	2	0	0	0	0	0	0	0	0	23
	3	0	3	2	2	1	1	0	0	0	0	0	0	9
	4	0	1	7	7	1	1	0	1	0	0	0	0	18
	5	0	2	2	5	5	0	0	0	2	0	0	0	16
	6	0	0	1	3	3	2	3	0	0	0	0	0	12
	7	0	0	0	0	2	4	2	1	0	0	0	0	9
	8	0	0	0	0	0	3	3	2	1	0	0	0	9
	9	0	0	0	0	0	3	1	1	1	0	0	0	6
	10	0	0	0	0	1	0	1	1	2	0	0	0	5
	11	0	0	0	0	0	0	0	1	0	1	0	0	2
	12	0	0	0	0	0	0	0	0	0	2	0	0	2
	13	0	0	0	0	0	0	0	0	0	1	1	0	2
	16	0	0	0	0	0	0	0	0	0	0	1	1	2
Total		6	19	19	20	14	14	10	7	6	4	2	1	122

Elvégezve a Spearman-féle rang-korreláció vizsgálatot, az alábbi eredményeket kaptam:

16. *táblázat: Spearman féle rangkorreláció vizsgálat eredményei az audit bizonyítékok száma és az említett kontrollok száma viszonylatában (saját szerkesztés az SPPS eredményei alapján)*

Symmetric Measures					
		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Ordinal by Ordinal	Spearman	0,840	0,032	16,944	,000[c]
N of Valid Cases		122			
a. Not assuming the null hypothesis.					
b. Using the asymptotic standard error assuming the null hypothesis.					
c. Based on normal approximation.					

Ez a vizsgálat szolgáltatta a legmeggyőzőbb eredményt: Kifejezetten erős kapcsolat mutatkozik igen alacsony elsőfajú hiba elkövetési valószínűség mellett.

4.1.4.4 A szervezet jellege és a szervezeti tudatosság érettségi szintje közötti összefüggés vizsgálata

A következő vizsgált hipotézis:

- KH4: Az üzleti vállalkozások jellemzően magasabb információbiztonsági tudatosság érettségi szintet képviselnek, mint a non-profit szervezetek.

Mivel ebben az esetben van egy nominális változónk (szervezeti jelleg) és egy ordinális változónk (szintbesorolás), ezért első lépésként megpróbáltam egy khi négyzet próbát végezni a két minőségi változó közötti kapcsolat elemzésére. Az SPSS-ben először a szokásos összefoglaló táblázatot készítettem el:

17. *táblázat: A szervezet jellege (for profit és non-profit) és szintbesorolása egy táblázatban összefoglalva (saját szerkesztés az SPPS eredményei alapján)*

A szervezet jellege * szintbesorolás							
		szintbesorolás					Total
		1	2	3	4	5	
A szervezet jellege	Non-profit szervezet	5	15	9	1	0	30
	Üzleti vállalkozás	4	24	33	29	2	92
Total		9	39	42	30	2	122

A táblázatot megvizsgálva az alacsony összes megfigyelésszámból (122 elemű minta!) eredő problémába ütköztem: A khi négyzet próba elvégezhetőségi feltétele, hogy az összes cella maximum 20 %-ában lehet az elvárt gyakoriság száma kevesebb, mint 5. Ez ennél a 10 (2 x 5) vizsgált cellánál láthatóan nem teljesül, tehát a khi négyzet próba eredménye nem lenne valid.

A khi négyzet próba alternatívája ilyen esetekben a Cohran-Armitage teszt, melyet az SPSS nem számol. Emiatt egy újabb szoftvert az XLSTAT (2019.4.2.64053) kellett alkalmaznom, mellyel elvégezhető volt a Cohran-Armitage teszt. Az XLSTAT összefoglaló statisztikáját mutatja a következő táblázat:

18. *táblázat: A szervezet jellege (for profit és non-profit) és szintbesorolása kapcsán számolt arányosságok egy táblázatban összefoglalva*
(saját szerkesztés az XLSTAT eredményei alapján)

Érettségi szintek	Non-profit szervezetek száma	For profit szervezetek száma	Összes	Számolt arányosságok
1	5	4	9	0,556
2	15	24	39	0,385
3	9	33	42	0,214
4	1	29	30	0,033
5	0	2	2	0,000
Összes	30	92	122	1,000

A teszt eredményei egy összefoglaló táblázatban:

19. *táblázat: A Cohran-Armitage teszt eredményei (saját szerkesztés az XLSTAT eredményei alapján)*

Cochran-Armitage trend test (Asymptotic p-value) / Two-tailed test:	
|z| (Observed value)	4,087
|z| (Critical value)	1,960
p-value (Two-tailed)	< 0,0001
alpha	0,05

A nullhipotézis (H_0) ebben az esetben az, hogy nincs kapcsolat a megfigyelt arányosságok (observed proportions) és a szintbesorolás között. Az alternatív hipotézis (H_a) pedig az, hogy van kapcsolat a megfigyelt arányosságok és a szintbesorolás között. Mivel a számolt p-érték alacsonyabb, mint alpha = 0,05 szignifikancia szint, ezért a nullhipotézis elutasítandó és az alternatív hipotézis pedig elfogadható.

Az SPSS-sel számolt Cramer's V asszociációs együttható ennek a kapcsolati erősségét is megmutatja:

20. *táblázat: A kapcsolati erősség jellemző mutatói a 122 elemű mintában*
(saját szerkesztés az SPPS eredményei alapján)

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	0,372	0,002
	Cramer's V	0,372	0,002
	Contingency Coefficient	0,349	0,002
N of Valid Cases		122	

A számolt mutatók alacsony elsőfajú hiba elkövetési valószínűség mellett gyenge-közepes kapcsolati erősséget jeleznek.

4.1.4.5 A szervezet méret és a szervezeti tudatosság érettségi szintje közötti összefüggés elemzése

A vizsgálat egy újabb dimenziója annak megállapítása, hogy a szervezeti méret befolyásolja-e a szervezet információbiztonsági tudatosságnak érettségi szintjét. Ehhez a kérdéshez a következő nullhipotézist társítottam:

- KH5: A nagyobb szervezetek jellemzően magasabb érettségi szintet képviselnek.

A szervezeti méret és az érettségi szint táblázat formájában a 122 elemű mintán így néz ki:

21. *táblázat: A szervezeti méret és szervezet szintbesorolása egy táblázatban összefoglalva (saját szerkesztés az SPPS eredményei alapján)*

A szervezet mérete rangsorba állítva (1-4) * szintbesorolás (1-5)							
		szintbesorolás (1-5)					
		1	2	3	4	5	Total
A szervezet mérete rangsorba állítva (1-4)	1	1	2	4	0	0	7
	2	1	6	6	5	0	18
	3	4	6	11	2	1	24
	4	3	26	20	23	1	73
Total		9	40	41	30	2	122

A szervezeti méret kódolása a vizsgálat során:

- 1 = 10 fő alatt
- 2 = 11-50 fő
- 3 = 51-250 fő
- 4 = 250 fő felett

A két sorrendi skálán mért tényező (szervezeti méret és érettségi szint) ismét a Spearman korrelációs együttható számolásával vizsgálható:

22. *táblázat: A szervezeti méret és az érettségi szint kapcsolati erősség jellemző mutatói a 122 elemű mintában (saját szerkesztés az SPPS eredményei alapján)*

Symmetric Measures					
		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	0,113	0,082	1,240	,217[c]
Ordinal by Ordinal	Spearman Correlation	0,111	0,087	1,221	,224[c]
N of Valid Cases		122			
a. Not assuming the null hypothesis.					
b. Using the asymptotic standard error assuming the null hypothesis.					
c. Based on normal approximation.					

A kapott eredmények mentén csak nagyon gyenge kapcsolatot tudunk felmutatni a két tényező között a mintában, ráadásul az elsőfajú hiba elkövetésének viszonylag magas valószínűsége mellett.

4.1.4.6 A válaszadó betöltött szervezeti pozíciója és a szervezeti tudatosság érettségi szintjének értékelése közötti összefüggés vizsgálata

Ahogy azt már a 4.1.1 fejezetben jeleztem, a végső mintanagyság és a válaszok szórása miatt nem tudtam közvetlenül vizsgálni azt, hogy a szervezetek különböző pozíciójú tagjai másképp értékelik-e az érettségi szintet, ezért megpróbáltam a válaszadókat két csoportba sorolni:

- Menedzser jellegű beosztásban dolgozó kérdőívkitöltők: pl. kockázat menedzser, informatikai vezető, technológiai vezető stb.
- Szakértő jellegű beosztásban dolgozó kérdőívkitöltők: pl. tanácsadó, mérnök, informatikai munkatárs, információbiztonsági munkatárs stb.

Ezzel a csoportosítással a válaszadók közül 27-en kerültek a menedzseri csoportba és 94-en pedig a szakértői csapatba (és egy fő pedig nem adott meg beosztást).

A mintában vizsgált hipotézis:

- KH6: A menedzserek jellemzően magasabbra értékelik szervezetüket az érettség szempontjából, mint a szervezetben dolgozó szakértők.

Mivel most is van egy nominális változónk (szervezeti beosztás) és egy ordinális változónk (szintbesorolás), ezért első lépésként megpróbáltam egy khi négyzet próbát végezni a két minőségi változó közötti kapcsolat elemzésére. Az SPSS-ben először a szokásos összefoglaló táblázatot készítettem el:

23. *táblázat: A szervezeti pozíció és a szervezet szintbesorolása egy táblázatban összefoglalva (saját szerkesztés az SPPS eredményei alapján)*

A szervezeti pozíció		1 = menedzser / 2= szakértő * szintbesorolás					
		szintbesorolás					
		1	2	3	4	5	Total
A szervezeti pozíció 1 = menedzser 2= szakértő	1	3	6	8	9	1	27
	2	6	33	33	21	1	94
Total		9	39	41	30	2	121

A táblázatra ránézve, megint az alacsony összes megfigyelésszámból (121 elemű minta!) eredő probléma mutatkozik: A khi négyzet próba elvégezhetőségi feltétele, hogy az összes cella maximum 20 %-ában lehet az elvárt gyakoriság száma kevesebb, mint 5. Ez ennél a 10 (2 x 5) vizsgált cellánál jól láthatóan nem teljesül, tehát a khi négyzet próba eredménye megint nem lenne valid.

A khi négyzet próba alternatívája most is az a Cohran-Armitage teszt, melyet az SPSS nem számol. Ilyen módon megint az XLSTAT (2019.4.2.64053) segítségét kellett igénybe vennem, mellyel elvégezhető volt a Cohran-Armitage teszt. Az XLSTAT összefoglaló statisztikáját mutatja a következő táblázat:

24. *táblázat: A szervezeti pozíció és szintbesorolása kapcsán számolt arányosságok egy táblázatban összefoglalva (saját szerkesztés az XLSTAT eredményei alapján)*

Érettségi szintek	Menedzseri pozíciójú válaszadók	Szakértői pozíciójú válaszadók	Összesen	Számolt arányosságok
1	3	6	9	0,333
2	6	33	39	0,154
3	8	33	41	0,195
4	9	21	30	0,300
5	1	1	2	0,500
Összesen	27	94	121	1,000

A teszt eredményei egy összefoglaló táblázatban:

25. *táblázat: A Cohran-Armitage teszt eredményei (saját szerkesztés az XLSTAT eredményei alapján)*

Cochran-Armitage trend test (Asymptotic p-value) / Two-tailed test:	
|z| (Observed value)	0,952
|z| (Critical value)	1,960
p-value (Two-tailed)	0,341
alpha	0,05

A nullhipotézis (H_0) ebben az esetben is az, hogy nincs kapcsolat a megfigyelt (számolt) arányosságok (observed proportions) és a szintbesorolás között. Az alternatív hipotézis (H_a) pedig az, hogy van kapcsolat a megfigyelt arányosságok és a szintbesorolás között. Mivel a számolt p-érték lényegesen magasabb, mint alpha = 0,05 szignifikancia szint, ezért a nullhipotézis fogadható el és az alternatív hipotézis pedig elutasítandó.

Kimondható, hogy a KH6 jelű hipotézis ezen a mintán nem fogadható el, tehát nem bizonyítható, hogy a menedzserek jellemzően magasabbra értékelnék szervezetüket az érettség szempontjából, mint a szervezetben dolgozó szakértők.

Az érdekességképpen az SPSS-szel kontrollként számolt Cramer's V asszociációs együttható ugyanezt a matematikai problémát tükrözi:

26. *táblázat: A kapcsolati erősség jellemző mutatói a 121 elemű mintában (saját szerkesztés az SPPS eredményei alapján)*

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	0,177	0,433
	Cramer's V	0,177	0,433
N of Valid Cases		121	

Az eredmény igen gyenge kapcsolatot és az első fajú hiba elkövetésének extrém magas valószínűségét mutatja, tehát igazából a modell szempontjából értékelhető eredményt ezzel a vizsgálattal nem kaptunk.

Összegezve megállapíthatjuk, hogy a hat hipotézisből öt esetében viszonylag egyértelmű választ kaptunk (kapcsolati erősség és szignifikancia), ami bíztató a modellünk alkalmazhatósága szempontjából.

4.2 A mélyinterjúkból szerzett információk

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.

Elsődleges célom a modell és a kapcsolódó kérdőív validáltatása volt szakértői szemüvegen keresztül. A kiválasztott személyek tapasztalataik miatt alkalmasak voltak a kérdőív számára „láthatatlan" tényezők azonosítására. Az interjúkat előre összeállított kérdéslista mentén végzem, hogy a strukturáltság kritériumának meg tudjak felelni. Az interjúk fókuszpontjai:

- Iparági sajátosságok a tudatosság és annak érettsége szempontjából
- A tudatosság érettségi szintjei és azok elhatárolhatósága az egyes szervezetekben
- A szervezeteknél jellemzően létező és bevezetett kontrollok és keletkező audit bizonyítékok
- A tudatosság látható és rejtett elemei
- Tudatosító programok elemei és sajátosságai
- Látott és megtapasztalt jó gyakorlatok
- Jó és rossz vezetői minták a tudatosság területén
- A kérdőíves felmérés tapasztalatainak közös értékelése az interjúalanyokkal.

A kiválasztott személyek jellemzően érzékeny iparágakat, szolgáltatói területeket képviselnek (pl. pénzügyi szektor, IT szolgáltatás stb.). Meglátásaikat az alábbiakban foglaltam össze:

- Nemzetközi tanúsító testület sokéves gyakorlattal bíró szakauditora: Az auditor kollegina azt emelte ki az interjú során, hogy ő jellemzően 2-es szintű szervezetekkel találkozik, mert a tanúsító auditokat a cégek külső bizonyítékként kívánják felhasználni a megfelelőségre és elsősorban arra koncentrálnak, hogy a képzések megtörténtét tudják alátámasztani bizonyítékokkal és viszonylag kevés olyan cég van, mely ezen képzések megtörténtén túl a képzések hatékonyságát is mérné és megpróbálna túllépni a rutinszerű és jól dokumentált évenkénti tantermi oktatáson.
- Nemzetközi hírű magyar start-up cég információbiztonsági vezetője: A képviselt szervezet speciális biztonsági technológiát fejleszt és forgalmaz (fájltitkosítás felhőben) nemzetközi piacon. A kollegina elmondása szerint a szervezet emiatt rendkívül fogékony az információbiztonsági kérdésekre és maga a menedzsment kezdeményez tudatosító akciókat. Erre jó példa, hogy a menedzsment elvégzett egy átfogó kockázatelemzést és az adathalászatot azonosította, mint kiemelkedő kockázatot a szervezet életében. Elrendelték a rendszeres adathalászati teszteket a szervezeten belül, és egy visszajelzéses mérést is bevezettek a támadások eredményességének értékelésére. Ugyanitt egy eljárásban szabályozták az incidensek bejelentésével és kezelésével kapcsolatos

felhasználói aktivitás jutalmazását is. Egy időben és kellő dokumentáltsággal megtörtént bejelentés a bejelentő számára bónuszpontokat ér, amelyek egy időszak lezárásakor pénzügyi jutalommá válthatók. A bemutatott gyakorlataik alapján ez a szervezet bizonyult a legérettebbnek a vizsgált mintában és az értékelésben egyetértés mutatkozott az interjúvolt személlyel.

- Pénzügyi szektor felügyeleti szerve IT auditokat végző szervezeti egységének vezetője: A pénzügyi szektor szereplői általában magasabb érettségi szintet képviselnek, mert a törvényi és jogszabályi előírások évek óta abba az irányba terelik őket, hogy látható módon fokozzák a munkatársak tudatosságát. Emiatt az auditokon több bizonyítékot szolgáltatnak erről a tevékenységről és igyekeznek fenntartani a jó gyakorlatokat, tehát jellemzően a 3-as szintbe sorolná be a felügyelt szervezeteket. Erős lökést adott a felügyelt szervezeteknek az MNB ajánlás (2018) a PSD2 magyarországi alkalmazásával kapcsolatban, mely külön felhívja a figyelmet a biztonságtudatossági képzésekre.
- Multinacionális telekommunikációs szolgáltató cég magyarországi középvezetője: A cég nagyon sok jó gyakorlatot honosított meg az anyavállalati példák alapján. Színes oktatási tartalmak állnak rendelkezésre minden munkatársnak. Emlékezetes akciójuk volt a Mikulásnak beöltöztetett social engineer, aki megbízás alapján tesztelte a fizikai kontrollok munkatársi ismeretét és alkalmazását. December 6.-án az idegen „Mikulás" egy álcázott fejkamerával bejárta az irodákat és rögzítették a munkatársi reakciókat, hogy mennyire tud szabadon közlekedni az egyes zónák között, majd egy videó spot formájában megosztották a kollégákkal a tapasztalatokat. Az akció annyira emlékezetesre sikeredett, hogy a munkatársak még hónapokkal később is emlékeztek a videó üzenetére. Az említett példa arra hívja fel a figyelmet, hogy mennyire fontos a szokatlan „csatornák" használata a fontos üzenetek átvitelére.
- Hivatásos „social engineer": Szakmájából adódóan a tudatosságot fokozó kontrollok közül azt emelte ki, mely erős kapcsolatban áll a személyes tapasztalataival. Nagyon hasznosnak véli az ún. információbiztonsági szabaduló szoba alkalmazását (Oroszi és Bálint (2019)), mely élményszerű módon járul hozzá ahhoz, hogy az egyének megtapasztalják bizonyos információbiztonsági kontrollok működésének szükségességét a szervezetben. A pozitív tapasztalatok mellett elmondható, hogy ez a kontroll nem használható általánosan, mert rendkívül erőforrásigényes (szakértői óra és munkatársi időbefektetés) egy nagyobb szervezet esetében.
- Banki, pénzintézeti adatvédelmi felelős: A jogi végzettségű kolléga sokéves adatvédelmi felelősi múlttal arra hívta fel a figyelmet, hogy mennyire fontos a nem szokványos üzenetátviteli utak választása, mert így sokkal jobban rögzülnek a helyes magatartási minták az érintettekben. A hivatkozott szakértő egy korábbi munkahelyén rendszeresen ún. „adatvédelmi fecsegőket", azaz rövid, velős történeteket osztott meg kör-email formájában a munkatársakkal. Ezek a „fecsegők" általában valamilyen humoros történetbe ágyazva szóltak az információbiztonság ügyéről. A disszertációban felvázolt érettségi modellben ez a jó gyakorlat szintén elhelyezhető, de nem szükséges magának a modellnek a változtatása, mert csak egy további speciális kontroll fajtát jelent a fentiekben ismertetett eszköz.

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.

A már korábban több fórumon is megosztott kérdőíves eredményeket (lásd 4.1 fejezet) az interjúalanyok reálisnak értékelték, bár az alacsony válaszadási hajlandóságra ők sem találtak magyarázatot.

4.3 A helyszíni auditokból kapott eredmények

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.

A választásom elsődleges szempontja az volt, hogy olyan szervezetek kerüljenek be az audit mintába, melyek különösen szenzitív személyes adatokat kezelnek nagy tömegben (pl. pénzügyi szolgáltató, egészségügyi szolgáltató stb.), tehát vélelmezhetően az információbiztonsági tudatosság és annak érettsége a szervezeten belül egy kiemelten fontos területnek kell lennie. Ugyanakkor fontos a felülvizsgálói, tanúsítói oldal gyakorlata is, ezért meglátogattam a felügyeleti oldalt képviselő szervezeteket is. Minden kiválasztott szervezetnél vizsgáltam:

- az iparági sajátosságokat
- az adott iparágra jellemző megfelelőségi elvárásokat (milyen szabványoknak, előírásoknak kell eleget tenniük az információbiztonság területén)
- hogyan értékeli a szervezet saját információbiztonsági érettségét
- milyen létező és működő kontrollok támogatják a tudatosságot
- milyen audit bizonyítékok keletkeznek az érettségi szinttel kapcsolatban
- milyen tudatosító programok vannak folyamatban és milyen módon mérik azok hatását.

Az auditok hivatottak az értékelési séma mélyebb elemzésére és annak igazolására, hogy a szervezetek által folytatott gyakorlat ténylegesen és megismételhető módon kapcsolható az egyes érettségi szintekhez. A számos audit bizonyíték és megfigyelt jó vagy rossz gyakorlatból most azokat emelem ki szervezetenként, amelyek valamilyen módon hozzájárultak az érettségi modellem verifikálásához:

- IT outsourcing szolgáltató: Ezt a céget közel egy évtizede van szerencsém nyomon követni. Fontos jellemzője, hogy személyi állományának nagyjából kétharmada az ügyfelek telephelyein teljesít szolgálatot, és emiatt a munkatársak jelentős része az ügyfél információbiztonsági irányítási rendszerébe tagozódik be, és ott kell a megfelelőséget a tudatosság területén biztosítania és bizonyítania. Ez a jellemzően multinacionális

ügyfélkör jórészt anyavállalati támogatással robusztus e-learning rendszeren keresztül kommunikálja a szükséges tartalmakat. Minden, ügyfélhez kihelyezett és a vevő szempontjából külsős, munkatárs csak akkor kap hozzáférést az ügyfél rendszereihez, ha teljesít bizonyos e-learning kurzusokat az adott ügyfélnél. Ezek a kurzusok tartalom szempontjából az adott multi kultúráját közvetítik, de nem jellemző a szórakoztató tartalmak megjelenítése és nem foglalkoznak a kurzus résztvevőinek belső motivációjával. A cél, hogy bizonyíték keletkezzen arról, hogy az adott személy a kurzuson részt vett, és lehetőleg papírmentes környezetben. Az ügyfelek többségénél szokás az egyes munkahelyek (irodai asztalok és székek és fiókos szekrények együttese) rendszeres belső auditja, amikor is a belső auditorok végig járják munkaidő után az irodákat és zöld/piros jelző cédulákkal adnak visszajelzést az ottdolgozóknak a követett gyakorlat jóságáról. Ez a kontroll (rendszeres iroda audit) alkalmas a tudatosság érettségi szintjének harmadik fokozatát (a tudatosság és viselkedés-változás promóciója) előkészíteni a szervezetben az erős kettes szintre (megfelelőségre törekvés) alapozva. Ezt a gyakorlatot egészíti ki az általam vizsgált outsourcing szolgáltató azzal, hogy saját e-learning tartalmat is közvetít a munkatársai felé. Belépéskor és utána éves gyakorisággal kötelezően átesnek ezen a kurzuson is a munkatársak, de nyilvánvalóan ez a kurzus nem ügyfélspecifikus tartalmakat közvetít, hanem az IT szolgáltató általános biztonsági elvárásait.

- IT szolgáltató (felhő titkosítás): Az auditok során egyedül itt tapasztaltam a szokványostól eltérő gyakorlatot: Egy feltörekvő és zömében fiatalokból álló és fiatalos cégkultúrát mutató cégben a cégvezetők az adathalászatot tekintették a legnagyobb kockázatnak (valós alapokon elvégzett kockázatelemzés nyomán!), ezért havi-kéthavi gyakorisággal szerveztek belső adathalász támadást, ahol mérték és visszajelezték az érintetti körben a találati arányokat, azaz, hogy ki és hányszor dőlt be a nagy műgonddal előállított próba-levélnek. Nem véletlen, hogy az általam látogatott szervezetek közül ennek a szervezetnek az érettségi szintjét tekintettem a legmagasabbnak (4-es szint: hosszútávú fenntartás és kultúraváltás), ahol még a maximális érettségi szintet jellemző gyakorlat (robusztus mérőszámrendszer) elmei is fellelhetők voltak.
- Katasztrófavédelmi központi szakmai szervezet: A szervezet nyugodtan nevezhető félkatonai szervezetnek mind belső kultúráját (pl. egyenruha viselése a munkahelyen) mind belső szervezeti struktúráját illetően. A szervezet az ország védelmi képességét illetően is értékes adatvagyont kezel (pl. kritikus infrastruktúra elemek) és az információbiztonság kérdésköre létfontosságú számukra. Ennek ellenére a szervezet a megfelelőségre törekvés (2. szint) állapotában van. Számos és igen részletes szabályozással bírnak, de nincs formális, szabvány alapú, információbiztonsági irányítási rendszerük. Rendszeresen szerveznek a felügyelt szervezetek számára információbiztonsági tárgyú konferenciákat, tanfolyamokat, ahová az általam auditált szervezet saját személyi állományát is elvárja. Erősek a fizikai kontrollok (pl. bejutás az épületbe), melyek mindenki számára láthatók, érzékelhetők. Egyéb speciális kontrollokat – tudomásom szerint – nem alkalmaznak, de nem kizárhatók olyan titkosszolgálati módszerek (pl. munkatársak megfigyelése, átvilágítása), melyek jellemzők a nemzetbiztonsági szempontból kritikus szervezetekre. A szervezeti kultúrából adódóan a jogszabályi megfelelés a legfőbb mozgató rugó, és ennek megfelelően a szervezet a 2. szintre jellemző működési módot mutat.

- Nemzetközi Tanúsító Testület hazai fiókirodája: A Tanúsító Testület képviselői azt erősítették meg, hogy a szervezeteknél az információbiztonsági tudatosítás témakörével való foglalkozás legfőbb és szinte egyetlen motivációja a megfelelőségre való törekvés. Még az olyan szervezetek sem mutatnak nagyon fejlett gyakorlatot, ahol sok éve van létező és működő információbiztonsági irányítási rendszer: Szinte mindenhol az éves és sokszor sablonos tartalmú képzések bizonylatai kerülnek elő. Színes vagy a szokványostól eltérő oktatási tartalmak és metódusok nem jellemzők, általában az éves hagyományos előadásokon alapuló tudatosítást preferálják, illetve fejlettebb szervezeti környezetben e-learning tartalmak is fellelhetők, de szigorúan a hagyományos köntösben, azaz egy megnyitható szövegfájl és hozzá kapcsolódó feleletválasztós kérdések egy tesztelő környezetben. Az auditált cégeknél a GDPR miatt megjelentek olyan honlapokhoz kötött adatkezelési tájékoztatók, melyek a szervezeten belüli adatkezelésről rendelkeznek, de ezek oktatása, tudatosítása többnyire hiányos vagy a hagyományos keretek (tantermi oktatás) folyik.
- Egyetem (egyetemi belső informatikai szolgáltató): Két egyetem gyakorlatát volt szerencsém közelebbről megfigyelni tanácsadói megbízások részeként. Mindkét esetben a megbízás tárgyát képező projekt a GDPR megfelelőséget célozta meg, ami rögtön világos jelzést ad arra nézve, hogy mi is volt a legfőbb hajtóerő mindkét projekt esetében: félelem a GDPR bírságoktól. A vizsgált intézmények jellemzően erőforráshiánnyal küzdenek, és az oktatás és kutatás mellett kevés figyelmet fordítanak a védelmi kérdésekre. Több szempontból nincsenek sincsenek tisztában a védendő értékekkel és a szabályozás nagyon megengedő. Az egyes tanszékek, intézetek sziget-szerűen működnek és az alkalmazott szabályrendszer és az elvárt magatartás az adott intézményvezető által egyedi módon meghatározott. Nincs egységes tudatosító program, de a központi adminisztráció – félve a következményektől – a törvényi, jogszabályi megfelelőségre törekszik, és erre áldoz tanácsadói projektek formájában. Ugyanakkor sem az adminisztratív állomány, sem az oktatói gárda nem tekinthető túlságosan biztonságtudatosnak. Az alapvetően kollaborációs kultúra és az erős karizma, illetve tudás és tekintély alapú hatalmi mechanizmusok sem támogatják túlságosan a szabályozás alapú működést. Az egyes szervezeti egységek saját belső renddel és kultúrával bírnak, melybe külső beavatkozást nem, vagy csak igen nehezen engednek. A klasszikus adminisztrációs területek (pl. központi és kari tanulmányi osztályok) még erősebben szabálykövetőnek tekinthetők, mint az egyes intéztek, tanszékek, mert a központi funkciók jobban ki vannak téve hatósági, felügyeleti ellenőrzéseknek. Az olyan tanszékek, intézetek, melyek külső ipari kutatásokban vesznek részt, jobban kezelik szervezeti szinten a tudatosítás kérdését, mert a külső partnerek határozottabban megfogalmazzák információbiztonsági elvárásaikat velük szemben. Mindkét látott és vizsgált egyetem az érettségi szintek közül a 2. szintet teljesíti.
- Multinacionális egészségügyi diagnosztikai szolgáltató szervezet: Európa közel húsz országában szolgáltató ún. „kis multi” cég információbiztonsági tudatosító gyakorlata volt vizsgálható az audit során. Ez a cég a használt diagnosztikai berendezései (pl. MR és CT berendezések) révén erősen kapcsolódik egy másik igen nagy és több kontinensen jelenlévő multinacionális nagyvállalathoz. Gyakorlata sok szempontból hasonlít a nagy multiéhoz, mert több menedzsere is onnan került át ebbe a szervezetbe. Egészségügyi szolgáltatóként nagyon sok és nagyon érzékeny betegadatot kezel és a szigorú

nemzetközi szabályozások miatt rendszeres külső auditoknak is ki van téve a cég, de adatai nem hagyják el az Európai Uniót. Emiatt a szervezet erősen megfelelőség központú és keresi azokat a kontrollokat, melyek révén meg tud felelni a külső elvárásoknak. Ugyanakkor a szervezet egy agresszív növekedési pályán mozog, Magyarországon is több kisebb céget és ellátó centrumot vásároltak fel, ami miatt nem beszélhetünk egységes gyakorlatról. A cég informatikai infrastruktúrájának számos eleme Magyarországról működik, ami növeli az itt dolgozók felelősségét az esetleges informatikai incidensek kapcsán. A szervezet az által a működtetett kontrollok alapján a 2. szintre (megfelelőségre törekvő) sorolható be, speciális, máshol nem tapasztalt kontrollokat nem alkalmaz.

- Sérült személyeket támogató szakmai egyesület: A civil szférát képviselő szervezet életébe egy szoftverfejlesztési projekt kapcsán láthattam bele. A szervezet nagytömegű személyes adatot kezel (fogyatékkal élők személyes adatai), de az információbiztonsági szempontok figyelembevétele nélkül. Jellemző módon az első részleges adatkezelési szabályzat annak a szoftverfejlesztési projektnek az egyik „melléktermékeként" jött létre, melyben érintve voltam. Nincsenek az információbiztonságot támogató formális kontrollok, az egyének belátásán múlik, hogy ki, milyen védelmi intézkedéseket alkalmaz. Az erőforráshiány miatt a szervezet informatikai infrastruktúrája nem túl fejlett és kevés betartandó szabállyal működik. Az egyesület tipikus 1. szintű szervezet (nem létező információbiztonsági kultúra és érettség) a megalkotott érettségi modell szempontjából, ugyanakkor már felfedezhetők a 2. szintre utaló jelek is, mert pl. a GDPR-nak való megfelelőség jegyében a szervezet honlapján megjelenítenek adatkezeléssel kapcsolatosan vállalt kötelezettségeket, és ezekkel a vállalásokkal a központi iroda munkatársai tisztában vannak.

A vizsgált szervezeteknél megfigyelt speciális, csak az adott szervezetre jellemző, kontrollokat és audit bizonyítékokat foglalja össze a következő táblázat:

27. *táblázat: A vizsgált szervezetek és a szervezetek életében megfigyelt speciális kontrollok és audit bizonyítékok (saját szerkesztés)*

A vizsgált (auditált) szervezet	A szervezet besorolása az ötfokozatú érettségi skálán	Megfigyelt speciális kontroll	Megfigyelt speciális audit bizonyíték
IT outsourcing szolgáltató	3	Saját on-line (e-learning) tartalom szervezet-specifikus elemekkel	Rendszer által generált részvételi és aktivitás adatok
IT szolgáltató (felhő titkosítás)	4 (5)	Adathalászati kampány évi 5-6 alkalommal	Vezetői irányítópult (dashboard) eredménymutatókkal
Katasztrófavédelmi központi szakmai szervezet	2	Tudatosító konferenciák szervezése társszervezeteknek, ügyfeleknek	Saját beiskolázott állomány ezeken a rendezvényeken

Nemzetközi Tanúsító Testület hazai fiókirodája	2 (3)	Nincsen	Nincsen
Egyetem (egyetemi belső informatikai szolgáltató)	2	Nincsen	Nincsen
Multinacionális egészségügyi diagnosztikai szolgáltató szervezet	2	Nincsen	Nincsen
Sérült személyeket támogató szakmai egyesület	1 (2)	Nincsen	Nincsen

A 27. számú táblázat is mutatja, hogy az alacsonyabb érettségi szintek (1-es és 2-es szint) esetében nem találkozhatunk szembe speciális kontrollokkal és audit bizonyítékokkal, de ahogy feljebb lépünk a modellben (3-as vagy 4-es szint), máris megjelennek olyan kontrollok és audit bizonyítékok, melyek túlmutatnak a sablonos megoldásokon.

Összességben megállapítható, hogy az ötfokozatú modell és annak elemei jól vizsgálhatók voltak 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.

5 KÖVETKEZTETÉSEK ÉS ÖSSZEFOGLALÁS

Az értekezés az információbiztonsági tudatosság szintjének mérési lehetőségeivel foglalkozik olyan módon, hogy kísérletet teszek egy saját érettségi modell kidolgozására és annak használhatósági vizsgálatára.

Megfogalmaztam kutatási kérdéseimet és a kutatástól várható eredményeket, majd vizsgáltam más kutatásokban (lásd pl. Dzazali és Zolait modelljét és hipotéziseit, (2012)) megfogalmazott hipotéziseket, illetve megalkottam saját kutatási hipotéziseimet is.

A gyakorlati kutatás során kérdőíves felméréssel vizsgáltam Dzazali és Zolait (2012) modelljét és annak részleges alkalmazhatóságát. Ugyanez a kérdőív vizsgálta Spitzner (2012) érettségi modelljének tükrében a magyar minta szervezeti tudatosság érettségi szint megoszlását, a jellemző kontrollokat és audit bizonyítékokat.

A kérdőívezést kiegészítették mélyinterjúk és helyszíni auditok, hogy a modell „finomhangolása" is megtörténhessen. Az eredmények feldolgozása és értékelése a kérdőív lezárása, és az interjúk, valamint a helyszíni auditok lebonyolítása után történt meg.

5.1 Célok és várt eredmények

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 kutatástól előzetesen várt eredmények:

- 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.

Az alábbi kutatási részcélok pedig az alapcélt bontják le kisebb és logikailag jól összekapcsolható és könnyebben vizsgálható gondolati egységekre:

- 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?

A kutatástól várt eredmények és a kapcsolódó kutatási célok tükrében a következő kutatási kérdésekre fókuszáltam:

- 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)?

Az elérni vágyott eredmények a következők voltak:

- Legyen egy pontos és részletes leíró érettségi modell minden egyes érettségi szintre (a szintre jellemző kontrollok és audit bizonyítékok megadásával),
- Legyen alkalmas a modell világos különbségtételre szervezet és szervezet között a szervezeti tudatosság érettségi szintjében,
- Feltárhatók legyenek és matematikailag igazolhatók legyenek összefüggések a kitöltők által megjelölt érettségi szintek és az adott szintre a kitöltők által megadott kontrollok között,
- Feltárhatók legyenek és matematikailag igazolhatók legyenek összefüggések a kitöltők által megjelölt érettségi szintek és az adott szinthez a kitöltők által megadott audit bizonyítékok között,
- Szülessen egy nemzetközi mintával összevethető méretű és minőségű magyar minta, mely alkalmas a jelen kutatás nemzetközi szintű kutatással történő összekapcsolására.

A kutatási célokat sikerült megvalósítani, ugyanakkor a kutatásnak vannak feltárt és felismert korlátai.

5.2 A kutatás feltárt és felismert korlátai

Az értekezés koncepciója és módszertani megközelítése egyértelmű korlátok mentén alakult ki:

- Nem végeztem primer kutatást nemzetközi szinten, de két nemzetközi kutatás eredményeit összevetettem a magyarországi helyzettel:
    - Dzazali és Zolait (2012) modelljét részlegesen teszteltem a kérdőíves megkérdezés során,
    - Spitzner (2012) modelljét a maga teljességében vizsgáltam a magyar mintán.

- Dzazali és Zolait (2012) modelljének azon komponenseit (konstrukcióit) nem vettem figyelembe, melyeket az általuk bemutatott kutatás is jelentéktelennek vagy alacsony hatásúnak mért.
- Spitzner (2012) modelljét sem változtatás nélkül használtam: Két dimenzióval (tudás és attitűd) kiegészítettem a saját modellemben (lásd 2.5 fejezet).

Az értekezés és a kutatás további korlátai:

- A szakterület önmagában annyira rétegzett (lásd pl. alapfogalmak szintjén az informatikai biztonság, információbiztonság, adatbiztonság, adatvédelem, kiberbiztonság, kibervédelem fogalmi keveredését!), hogy a teljeskörűségnek még csak a kísérlete sem merülhet fel.
- Az alkalmazhatónak vélt érettségi modellek méréselméleti (skálaelméleti) korlátokat hordoznak: Jellemzően egy sorrendi skálán kell olyan műveleteket végzeni (pl. átlagszámítás), melyek az adott skálához nem, vagy csak erős korlátozó feltételekkel illeszkednek.
- A kidolgozott modell validálására első lépésben csak magyar vagy Magyarországon működő gazdálkodó szervezetek körében került sor. Mivel a modell beváltotta a hozzáfűzött reményeket, ezért a jövőben sor kerülhet nemzetközi kipróbálására is. Itt elsősorban közép-európai összevetésekre érdemes gondolni.
- A kutatás során nem végeztem ún. „action research" jellegű tevékenységet, azaz nem állapítottam meg egy vagy több konkrét szervezet induló érettségi szintjét pl. tanácsadási projekten keresztül, és nem próbáltam javítani információbiztonsági tudatossági teljesítményét, és aztán értelemszerűen nem végeztem visszamérést egy hosszabb időtávon.
- A kutatás során gyűjtött minták (megfigyelések) száma nem sokkal haladja meg a 100-as nagyságrendet (122 megfigyelés a kérdőíves megkérdezés eredménye). Ez egyrészt következik a kérdőívvel megszólíthatók korlátos számából, másrészt a relatíve alacsony válaszadási hajlandóságból.

Mindezeket a korlátokat felismerve és vállalva, igyekeztem a kutatás megközelítési módját és módszertani elemeit úgy összehangolni, hogy az eredmények hitelessége és bemutathatósága ne szenvedjen csorbát.

5.3 Következtetések és a hipotézisek értékelése

Ebben a fejezetben értékelem a kutatási kérdés alapján megfogalmazott hipotéziseimet.

Az 5. táblázat foglalja össze, hogy az egyes kutatási célok hogyan teljesültek, azaz a disszertáció, mely fejezete mutatja be az adott témakörben elért eredményeket:

28. *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. (lásd „B" jelű melléklet!) 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. (lásd „B" jelű melléklet!) 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 következő táblázatban a kutatási célok mentén megfogalmazott hipotézisek sorsát mutatja be:

29. *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!*

Ahogy a fenti táblázatból is kitűnik, a kutatás során többnyire sikerült a megfogalmazott hipotéziseket igazolni, de a KH5 és KH6 esetében ugyanez nem állítható, és a KH7-KH8 esetében pedig csak közvetett bizonyítékok állnak rendelkezésre az elvégzett mélyinterjúk és auditok nyomán.

5.4 A kutatás jelentősége és logikája

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.

5.5 A kutatás hozzájárulása a kérdéskör vizsgálatához

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 magyar szervezetek körében
- Egy második dimenzióként egy másik nemzetközi modell (Dzazali és Zolait (2012)) részleges vizsgálatát és elemzését végzem 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 teremt kapcsolatot.

A három említett dimenzió szervesen kiegészíti egymást és megbízható alapot szolgáltat további kutatások elvégzéséhez, illetve az eredmények gyakorlati felhasználhatóságát is támogatja.

5.6 Az előzetesen várt eredmények és a kutatás tényleges kimenete

A kutatás megkezdésekor megfogalmazott és várt eredmények nem minden vonatkozásban találkoztak a kutatás tényleges kimenetével. Az alábbi táblázat összegzi az előzetesen várt és a tényleges eredményeket.

30. 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.

5.7 A jövőbeni kutatás irányai

A rendelkezésemre álló 122 elemű minta erősen korlátos abból a szempontból, hogy ilyen megfigyelésszám mellett két fontos hipotézis igazából nem, vagy nagyon elnagyoltan vizsgálható:

- KH7: Az egyes érettségi szintekhez tartozó jellemző kontrollok a vizsgált mintában azonosíthatók és ezáltal maga a kidolgozott érettségi modell megfelelősége is igazolható.
- 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

Ha ezt a megfigyelésszámot lehetne látványos módon növelni, akkor adná magát egy fontos jövőbeni kutatás iránya: a KH7 és KH8 hipotézisek vizsgálata.

Egy másik ugyancsak izgalmas kérdés vizsgálatát tenné lehetővé egy nagyobb minta:

- Bizonyos adatvédelmi szempontból érzékeny iparágak (pl. pénzügyi és egészségügyi szolgáltatók) magasabb érettségi szintet produkálnak-e az erőteljesebb külső kényszerek miatt?

A megfigyelések korlátozott száma most nem teszi lehetővé „erős" statisztikai alapú következtetések levonását, hiszen pl. bizonyos iparágak, szektorok jelenléte pár megfigyelésre korlátozódik a mintában. Megalapozottabb következtetések levonásához lényegesen nagyobb minta (megfigyelésszám) szükséges, és ez lehet a jövőbeni kutatások egyik jellemző iránya.

Érdekes dimenziója lehet a vizsgálódásnak, ha ugyanezt a mintavételt pl. éves gyakorisággal megismételnénk nagyjából ugyanabban a vállalati körben, és így azt vizsgálhatnánk, hogy van-e elmozdulás az egyes iparágak, szektorok átlagos érettségi szintjében, illetve ugyanez a kérdés felvethető egyes konkrét szervezetek esetében is:

- A bemutatott modellünk alkalmas-e bizonyítékok szolgáltatására arra nézve, hogy időben hogyan változik (nő vagy csökken) egy gazdálkodó szervezet információbiztonsági tudatosságának érettségi szintje?

A most vizsgált minta elég erősnek bizonyult abból a szempontból, hogy kezdenek kirajzolódni a jellemző kontrollok és audit bizonyítékok az egyes érettségi szintekhez kötötten, és akkor innen már csak egy lépés egy viszonylag egyszerű szervezetdiagnosztikai eszköz készítése, melynek alkalmazásával gyors és valid válaszadható arra a kérdésre, hogy a vizsgált szervezet milyen érettségi szinten áll, és milyen lépések (mely kontrollok bevezetése) képesek ezt az érettséget a leghatékonyabb módon növelni, ami a szervezet menedzsment szempontjából egy nagyon értékes információ lehet. Ennek a diagnosztikai eszköznek a vázát mutatja be az „E" jelű melléklet.

Ahhoz, hogy a kitöltési hajlandóság drasztikusan növelhető legyen, arra van szükség, hogy látványosan lerövidítsük a kérdőívet. Mivel a továbbiakban Dzazali és Zolait (2012) modelljének verifikálása már nem kutatási cél, így a vonatkozó kérdések elhagyhatók, és jelentős mértékben kurtább lesz a kérdőív. Érdemes lehet ezzel megpróbálkoznom 2020 második felében.

Természetesen izgalmas kutatási kérdés lehetne az is, hogy a közép-kelet-európai régióban hasonló kérdésfelvetés milyen eredményeket hozna a régió egyes országaira vetítve.

A kutatás egy egészen más dimenziója lehetne, ha megvizsgálnánk az egyes szervezetek generációs összetételét és ennek kapcsolatát az adott szervezet információbiztonsági tudatossági érettségének szintjével. Azt tudjuk Lancaster és Stillman (2010) nyomán, hogy jelen pillanatban öt jellegzetes generáció van jelen párhuzamosan az egyes munkahelyeken:

– az „építők": akik 1946. előtt születtek,

– az ún. „baby boom"-osok: az 1946 és 1965 között születettek,

– az „X" generáció: az 1965-1980 között jöttek a világra,

– az „Y" generáció: akik 1980 után születtek,

– és a „Z" generáció: az 1995 után születettek.

Az egyes generációk információbiztonsági tudatossághoz való viszonyát jól jellemzi Tari (2010), aki szerint az „építők" generációja az informatikával már csak idős korában találkozott, ezért számukra az információs és kommunikációs technológiák használata önmagában is kihívást jelent.

A „baby-boom”-osok a demográfiai robbanás részeseiként, nem az internettel együtt nevelkedtek, tehát kevésbé tudnak alkalmazkodni a technológia fejlődéséhez, ezért esetükben technikai és tudásbéli hiányosságok figyelhetők meg. Lényegében felnőtt korukban kezdték el használni az infokommunikációs eszközöket, telefonálni például már szeretnek is, azonban az okoseszközök néha kihívást jelentenek számukra.

Az „X” generáció tagjai a jelenlegi munkaerőpiac domináns tagjainak tekinthetők (a „negyvenesek”). Munkavégzésüket már alapvetően befolyásolja az Internet-használat, komoly eszközhasználók, azonban a hatékonyabb munkavégzésre hivatkozva a biztonsági előírásokat gyakran figyelmen kívül hagyják. Amikor elkezdték használni a technológia nyújtotta lehetőségeket, még nem volt ekkora biztonsági kockázatokkal terhelt az IT világa. Náluk még nem volt jellemző az adatszivárgás, identitáslopás, kibertér és egyéb, ma már napi szinten használt fogalmak.

Az „Y” generáció tagjai – akik már az információs kor „gyermekei” (IT bennszülöttek) a mai húszasok-harmincasok – általában jóindulatúak és fogékonyak az információtechnológia iránt, de eredménytelenség (pl. lassúság vagy rossz minőségű felhasználói felület) esetén türelmetlenné válhatnak. Ez megmutatkozik abban is, hogy ha a biztonságra fordított erőfeszítés kényelmetlen, akkor inkább megkerülik a védelmi mechanizmusokat.

Nyilvánvalóan nagyon más alapvető információbiztonsági érettséget hordoz egy olyan szervezet, ahol sok a fiatal munkavállaló („Y” generáció), mint egy olyan szervezet, ahol a „baby boom” és az „X” generáció adja a munkavállalók zömét.

Érdekes kutatási kérdés lehet az, hogy a korösszetétel egy szervezet esetében mennyire meghatározó az induló információbiztonsági érettségi szint meghatározása szempontjából és mennyire lehet gyorsabb vagy lassabb az információbiztonsági kultúraváltás egy szervezet életében attól függően, hogy milyen „korfa” jellemzi az adott szervezetet.

Mellékletek

A melléklet jele	Tartalma
A	Rövidítések jegyzéke
B	A kutatás kérdőíve
C	A kutatás mélyinterjúinak kérdésjegyzéke
D	A kutatás során végrehajtandó helyszíni auditok ellenőrző listája
E	Gyorsteszt a vizsgált szervezet információbiztonsági tudatossága érettségi szintjének megállapítására

"A" Melléklet: Rövidítések jegyzéke

Az "A" mellékletben bemutatott szótár azoknak a fogalmaknak a rövidítéseit tartalmazza, mely fogalmakat az értekezés használja.

A1. Rövidítések jegyzéke

RÖVIDÍTÉS	A TELJES FOGALOM
BCP	Business Continuity Plan
CMM	Capability Maturity Model
CMMS	Capability Maturity Model for Software
COBIT	Control Objectives for Information and Related Technologies
CSF	Critical Success Factor
DRP	Disaster Recovery Plan
EO	Expected Output – Várt eredmény (kimenet)
FISMA	Federal Information Security Management Act
GDT	General Deterrence Theory – Az általános elrettentés elmélete
GLBA	Gramm–Leach–Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISA	Information Security Awareness – információbiztonsági érettség
ISACA	Information Systems Audit and Control Association
ISACM	Information Security Awareness Capability Model
ISO	International Organisation for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KGI	Key Governance Indicator
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
PCI DSS	Payment Card Industry Data Security Standard
PCMM	People Capability Maturity Model
PMT	Protection Motivation Theory – A védelmi motivációs elmélet
PRISMA	Program Review for Information Security Management Assistance
RACI	Responsible, Accountable, Consulted, Informed
RO	Research Objective – kutatási cél
RQ	Research Question – kutatási kérdés
SEM	Strukturális Egyenletek Modelljei
SOX	Sarbanes-Oxley Act
TAM	Technology Acceptance Model – A technológia elfogadási modell
TPB	Theory of Planned Behaviour – A tervezett viselkedés elmélete
UAMM	User Awareness Maturity Model

"B" Melléklet: A kutatás kérdőíve

Ez a melléklet azt az on-line kérdőívet mutatja be, melyet a kutatás során használtam:

Az információbiztonsági tudatosság érettségének mérése szervezeti szinten (kutatás)

Tisztelt Kitöltő!

Kérem, hogy a kitöltéssel kapcsolatos általános tudnivalókat figyelmesen olvassa el!

A kutatás céljai: A szervezetek információbiztonsági tudatosságát szeretnénk vizsgálni egy érettségimodell segítségével és azonosítani azokat a kontrollokat és audit bizonyítékokat, melyek az egyes szinteket jellemzik.

A kutatásnak nem célja kitöltői adatbázis építése személyes adatokból. Csak akkor adja meg nevét és elérhetőségét (email cím), ha kifejezetten szeretné beazonosítását abból a célból, hogy a kutatás eredményeiből közvetlen visszajelzést kapjon egy összefoglaló formájában. Személyes adatokat egyéb célból nem gyűjtünk, nem kezelünk és nem tárolunk. A kapott válaszokat kizárólag statisztikai feldolgozás céljából használjuk fel, és az adott válaszok nem lesznek egyetlen személyre vagy szervezetre sem visszavezethető módon kezelve.

A kutatás során a SANS Institute ötfokozatú Information Security Awareness Maturity modelljét használjuk fel némi átdolgozás és továbbfejlesztés nyomán.

A modellről bővebben itt:
https://www.sans.org/security-awareness-training/blog/security-awarenessmaturity-model
A kérdőív áttekintő szerkezete:

I. Általános (kutatás demográfiai) adatok: Név és email cím (melynek megadása nem kötelező!), kitöltő beosztása / funkciója a szervezetben, szervezeti méret, szervezet működési területe, a szervezet jellege

II. Néhány általános kérdés a szervezet információbiztonsági gyakorlatával kapcsolatban három kulcsterületen:
II.1 A kockázatkezelés mechanizmusa a szervezetben
II.2. A szervezeti struktúra sajátosságai az információbiztonság szempontjából
II.3 A tudatosság és tréning tevékenység kultúrája a szervezetben

III. Az ötfokozatú modell egyes érettségi fokozatainak rövid leírása alapján itt adja majd meg szervezetének vélelmezett érettségi szintjét.

IV. Támogató kontrollok: A kérdőívnek ebben a fejezetében kap egy listát egy szervezetben elképzelhető kontrollokról, melyek a tudatosságot hivatottak támogatni. Ön válasszon ezen kontrollok közül aszerint, hogy melyek létezése, működése jellemző a szervezetére. A listát ki is egészítheti személyes tapasztalatai alapján olyan kontrollokkal, melyekről azt gondolja, hogy azok támogatják szervezetében a tudatosságot.

V. Audit bizonyítékok: A kérdőív utolsó fejezetében olyan audit bizonyítékokat sorolunk, melyeket egy külső fél (pl. vevő vagy tanúsító) az Ön szervezeténél találhatna egy tudatossági audit során. Itt arra kérjük, hogy jelölje meg azokat a bizonyítékokat, melyek valóban hozzáférhetők az Ön szervezeténél! Természetesen ebben a pontban is van lehetőség olyan audit bizonyítékok megadására, melyre a kérdőív készítői nem gondoltak, és véleménye szerint bizonyítékul szolgálhatnak a szervezeti tudatosság érettségére.

A remélhetően statisztikai méretű minta alapján azt vizsgáljuk matematikai módszerekkel, hogy milyen kapcsolat mutatható ki az egyes kontrollok / audit bizonyítékok és a szervezetek információbiztonsági tudatosságnak érettségi szintje között.

A kérdőív kitöltése nagyjából 15-20 percet igényel és a beállítások miatt egyszer tölthető ki, tehát akkor fogjon hozzá, ha rá tudja szánni a szükséges időt.

Számos kérdésnél találja a "Kötelező" jelzést, ami csak azt kívánja hangsúlyozni, hogy a feldolgozhatóság miatt mindenképpen szükséges kitölteni (a kérdőív az ilyen kérdéseknél nem engedi a kitöltés nélküli továbblépést), emiatt megértését kérjük!

Ha a vizsgálattal kapcsolatban bármilyen kérdése, kérése merülne, fel, kérjük, keressen meg minket az alábbi elérhetőségen keresztül!

Üdvözlettel

Tarján Gábor
Gabor.Tarjan@magicom.com

I. Szekció: Általános (kutatás-demográfiai) adatok

Ezeknek az adatoknak a begyűjtése azt a célt szolgálja, hogy a kérdőív II.-III-IV.-V. fejezetében kapott válaszokat össze tudjuk kapcsolni szervezeti sajátosságokkal (pl. szervezeti méret, jelleg, iparág stb.)

1. Név (nem kötelező kitölteni, és csak akkor adja meg, ha szeretne személyes visszajelzést kapni a kutatási eredményekről): ……

2. E-mail cím (nem kötelező kitölteni, és csak akkor adja meg, ha szeretne személyes visszajelzést kapni a kutatási eredményekről): ……

3. Beosztás (funkció) - a SANS Institute Awareness Report által használt terminológia és felosztás szerint: *

Csak egyet jelöljön meg!

- Tudatosítás & Tréning (képzési) - Vezető
- Tudatosítás & Tréning (képzési) - Munkatárs
- Informatikai vezető (CIO) / technológiai vezető (CTO)
- Információbiztonsági vezető (CISO)
- Tanácsadó
- Mérnök
- Információbiztonsági Menedzser / igazgató
- Információbiztonsági munkatárs
- Informatikai menedzser / igazgató
- Informatikai munkatárs
- Jogi / Audit / Megfelelőségi vezető (pl. Adatvédelmi vezető - DPO)
- Kockázat menedzser / igazgató
- Egyéb: ……

4. A szervezet mérete (munkatársi létszám) - alkalmazottak és hozzáférésekkel bíró külsős munkatársak összesen: *

Csak egyet jelöljön meg!

- 1-10
- 11-50
- 50-250
- 250 felett

5. A szervezet működési területe / iparága: *

Csak egyet jelöljön meg!

- Állami szervezet
- Autóipar
- Egészségügy
- Elektronika
- Energia
- Építőipar
- Gyógyszeriipar
- Informatika
- Kereskedelem
- Közlekedés
- Közmű, közműszolgáltatás
- Kultúra
- Kutatás-fejlesztés
- Mezőgazdaság
- Oktatás
- Önkormányzat
- Pénzügy (bank, biztosítás)
- Szállítmányozás, logisztika
- Szolgáltatás, egyéb szolgáltatás
- Telekommunikáció
- Termelés
- Vendéglátás, idegenforgalom, szálloda
- Egyéb: ……..

6. A szervezet jellege: *

Csak egyet jelöljön meg!

- Üzleti vállalkozás
- Non-profit szervezet

II. Szekció: Néhány általános kérdés a szervezet információbiztonsági gyakorlatával kapcsolatban három kulcsterületen (kockázatmenedzsment, szervezeti kérdések, tudatosság)

Kérdőívünknek arányaiban ez a leghosszabb fejezete, de a kérdések viszonylag gyorsan megválaszolhatók! Értékelje az alábbi állításokat a szervezete kapcsán. Minden állításhoz nyolc válaszlehetőség tartozik (Egy lehetséges opció, ha a kérdés nem értelmezhető a kitöltő számára, illetve egy hétfokozatú ún. Likert-skála adja ki a további hét opciót). Minden egyes kérdésnél értelemszerűen egy opciót választhat!

7. A szervezetben az információbiztonsági kockázatokat minden működési folyamat kapcsán azonosítják és figyelembe veszik. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

8. A szervezet számára kritikus információkat és informatikai infrastruktúra elemeket (pl. hálózati elemek, alkalmazások stb.) azonosították. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

9. Hatékony menedzsment eljárásokat / kontrollokat határoztak meg a veszélyekkel, fenyegetésekkel szemben. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

10. Az információs rendszerek sérülékenységeit és a kapcsolódó folyamatokat rendszeresen azonosítják. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

11. A biztonsági eseményekre a felsővezetés azonnal reagál. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

12. Az információbiztonsági szervezeti egység képviselői fontos szerepet játszanak az információbiztonsággal kapcsolatos döntéshozatali folyamat irányításában. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

13. Az átfogó információbiztonsági szervezet működését értékelik és hozzáigazítják a változó feltételekhez. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

14. Az információbiztonsági szervezeti egység képviselői találkoznak az üzleti / szolgáltató szervezeti egységek vezetőivel, hogy megértsék azok üzleti (működési) céljait és információbiztonsági igényeit. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

15. Az információbiztonsági tudatosságot a szervezet valamennyi tagja számára rendszeresen kommunikálják. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

16. Az informatikai rendszerek felhasználóit oktatják arra, hogy a gyanús tevékenységeket azonosítsák és jelentsék. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

17. A munkatársak rendszeresen vesznek részt információbiztonsági tréningeken. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

18. Az informatikai rendszerek felhasználóit világos utasításokkal látták el az adatok osztályozásával kapcsolatban a digitális adatfeldolgozó műveletek kapcsán. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

19. A munkatársakat világos utasításokkal látták el az adatok osztályozásával kapcsolatban a manuális adatfeldolgozó műveletek kapcsán. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

20. Az információbiztonsági tudatosságról szóló tájékoztató anyagok tartalma és formája szabványosított. *

Csak egyet jelöljön meg!

- Nincs róla információm / Nem értelmezhető a szervezetben
- Teljes mértékben egyetértek
- Nagyrészt egyetértek
- Csak kismértékben értek egyet
- Közömbös számomra
- Nem túlságosan értek egyet
- Nagyrészt nem értek egyet
- Egyáltalán nem értek egyet

III. Szekció: Az ötfokozatú modell egyes érettségi fokozatainak rövid leírása alapján adja meg szervezetének vélelmezett érettségi szintjét!

Kérdőívünknek ez az egyik kulcseleme, kérjük figyelmesen olvassa el az egyes érettségi szintek tömör leírását!

21. Sorolja be szervezetét az alábbi információbiztonsági tudatossági érettségi szintek valamelyikébe az egyes szintekhez tartozó rövid leírások alapján! *

Csak egyet jelöljön meg!

- 1. szint: NEM LÉTEZŐ (Információbiztonsági tudatosság gyakorlatilag nem létezik.)
- 2. szint: A MEGFELELŐSÉGRE FÓKUSZÁLÓ (Információbiztonsági tudatosító program már létezik, de kifejezetten a megfelelőségre vagy külső audit követelmények teljesítésére készült.)
- 3. szint: A TUDATOSÍTÁS ÉS A 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.)
- 4. szint: A HOSSZÚTÁVÚ FENNTARTHATÓSÁG ÉS SZERVEZETI 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.)
- 5. szint: ROBUSZTUS MÉRŐSZÁM RENDSZER (Az információbiztonsági tudatosító programnak van egy robusztus mérőszám rendszerre, 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.)

IV. Szekció: Támogató kontrollok

A kérdőívnek ebben a fejezetében kap egy listát egy szervezetben elképzelhető kontrollokról, melyek a tudatosságot hivatottak támogatni. Ön válasszon ezen kontrollok közül aszerint, hogy melyek létezése, működése jellemző a szervezetére. A listát ki is egészítheti személyes tapasztalatai alapján olyan kontrollokkal, melyekről azt gondolja, hogy azok támogatják szervezetében a tudatosságot.

Természetesen itt van lehetőség több kontroll megjelölésére, illetve a lista kiegészítésére.

22. Az alábbi információbiztonsági tudatosságot támogató kontrollok közül azokat jelölje meg, melyek létezéséről (működéséről) van tudomása a szervezetében! *

Jelölje meg mindazokat, melyek a szervezetében léteznek, működnek!

- o Rendszeres (éves) tudatosító tréningek kerülnek lebonyolításra
- o Dokumentált fegyelmi eljárás létezik
- o Általános célú tudatosító tananyagok (tartalmak) rendelkezése állnak
- o A belépési folyamat részeként kapnak bevezető tudatosító tréninget az új belépők
- o Rendszeres belső auditokon értékeljük a tudatosságot
- o Kockázatelemzés alapján szervezetspecifikus tanagyagok (tartalmak) rendelkezésre állnak
- o Szabályozott ösztönző rendszer (pl. jutalmak, díjak) létezik az információbiztonság területén
- o Célcsoportokra bontott tananyagok (tartalmak) léteznek
- o Rendszeres információbiztonsági tudásfelmérő teszteket végzünk a szervezetben
- o Dokumentált és bevezetett eljárás a szervezeti információbiztonsági tudatosság mérésére (mérőszámok, a mérés végrehajtása, és a mérési eredmények felhasználására)
- o Személyre, szervezeti egységre szabott "SMART" célok. (SMART - specific, measurable, attainable, realistic, timely - specifikus, mérhető, elérhető, realisztikus, jól időzített)
- o Egyéb: ……

V. Szekció: Audit bizonyítékok

A kérdőív utolsó fejezetében olyan audit bizonyítékokat sorolunk, melyeket egy külső fél (pl. vevő vagy tanúsító) az Ön szervezeténél találhatna egy tudatossági audit során. Itt arra kérjük, hogy jelölje meg azokat a bizonyítékokat, melyek valóban hozzáférhetők az Ön szervezeténél! Természetesen ebben a pontban is van lehetőség olyan további audit bizonyítékok megadására, melyre a kérdőív készítői nem gondoltak, és véleménye szerint bizonyítékul szolgálhatnak a szervezeti tudatosság érettségére. Természetesen itt van lehetőség több audit bizonyíték megjelölésére, illetve a lista kiegészítésére.

23. Kérem, jelölje meg azokat az audit bizonyítékokat, melyek valóban hozzáférhetők az Ön szervezeténél! *

Jelölje meg mindazokat, melyek a szervezetében hozzáférhetők!

- o Általános célú információbiztonsági tudatosító tananyagok (tartalmak)
- o Képzési feljegyzések (pl. jelenléti ívek tudatosító képzésről)
- o Beléptetési folyamat "sétáló papírja" tudatosító képzéssel kapcsolatos bejegyzéssel
- o Dokumentált és bevezetett fegyelmi szabályzat
- o Belső audit jelentés információbiztonsági tudatosításról
- o Dokumentált és bevezetett belső audit eljárás
- o Ügyfél vagy harmadik fél által végzett információbiztonsági tudatossági audit jelentése
- o Azonosított célcsoportok tudatosító képzésekre
- o Célcsoport specifikus tudatosító tananyagok (tartalmak)
- o Dokumentált tudatosítási teszt eredmények
- o Incidensek kapcsán jutalmazott személyek
- o Tudatosító projektek projektdokumentációja (pl. Projekt Alapító Dokumentum - PAD)
- o Személyes teljesítményértékelő lapok tudatossággal kapcsolatos célokkal
- o Dokumentált és bevezetett eljárás a szervezeti információbiztonsági tudatosság mérésére
- o Személyre szabott és dokumentált SMART célok a tudatossággal kapcsolatban
- o Dokumentált, mért, jelentett és menedzselt tudatossági célok a szervezet szintjén
- o Egyéb: …….

Ez itt a kérdőív vége. Köszönjük érdeklődését, munkáját és értékes idejét, amelyet a kérdőív kitöltésére szánt!

*****

"C" Melléklet: A kutatás mélyinterjúinak kérdésjegyzéke

Ez a melléklet azt a kérdésjegyzéket mutatja be, melyet a kutatás mélyinterjúi során használtam:

- Az interjúalany által gondozott szervezetek általános szervezeti jellemzői (méret, iparág, for profit / non profit)
- Iparági sajátosságok a tudatosság és annak érettsége szempontjából (pl. milyen külső követelmények, standardok alkalmazandók a szervezetben, milyen külső auditoknak kitett a szervezet)
- A tudatosság érettségi szintbesorolása a vizsgált szintjei és azok elhatárolhatósága az egyes szervezetekben (a modell szakértői validálása)
- A szervezeteknél jellemzően létező és bevezetett kontrollok és keletkező audit bizonyítékok
- A tudatosság látható és rejtett elemei
- Tudatosító programok elemei és sajátosságai
- Látott és megtapasztalt jó gyakorlatok
- Jó és rossz vezetői minták a tudatosság területén
- A kérdőíves felmérés tapasztalatainak közös értékelése az interjúalannyal

******

"D" Melléklet: A kutatás során végrehajtott helyszíni auditok ellenőrző listája

Ez a melléklet azt az ellenőrző listát mutatja be, melyet a kutatás során végrehajtott helyszíni auditokon használtam:

Vizsgált jellemző	Jegyzetek (audit bizonyítékok)
Szervezet neve	
Iparág	
For profit / Non profit	
Méret (létszám)	
Egyéb működési jellemző (pl. több iroda, stb.)	
Szervezeti minősítések (pl. ISO 27001, stb.)	
A szervezet saját besorolása az ötfokozatú modellben	
Látott fizikai kontrollok és audit bizonyítékok a szervezetben	
Látott adminisztratív kontrollok és audit bizonyítékok a szervezetben	
Látott műszaki (technikai) kontrollok és audit bizonyítékok a szervezetben	
A szervezetben a tudatosság (a tudás és az attitűd nyomai, bizonyítékai) jellemzői	
Létező információbiztonsági programok és azok eredményei	
Információbiztonsággal kapcsolatba hozható mérőszámok és mérések a szervezet gyakorlatában	
Szakértői besorolás az ötfokozatú modellben (az esetleges különbség a szakértői és az önbesorolás között és ennek magyarázata)	

"E" Melléklet: Gyorsteszt a vizsgált szervezet információbiztonsági tudatossága érettségi szintjének megállapítására

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.

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)

Bowen, P., Kissel, R. (2007): NISTIR 7358 – Program Review for Information Security Management Assistance (PRISMA), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, 2007

Bulgurcu, B., Cavusoglu, H., Benbasat, I., (2010): „Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", MIS Quarterly. Vol. 34. Issue 3. pp. 523-548

Curtis, B., Hefley, W.E., and Miller, S. (2002): „The People Capability Maturity Model: Guidelines for Improving the Workforce." (ISBN 0-201-60445-0). Reading, MA: Addison Wesley Longman 2002

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"

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010): Multivariate data analysis. Englewood Cliffs, NJ: Prentice Hall, 2010

Hair, J. F., Sarstedt, M, Ringle, C. M., Mena, J. A. (2012): „An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research". Journal of the Academy of Marketing Science, 40.3. pp. 414-433.

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

Hu, L. T., Bentler, P. M., (1999): „Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives". Structural Equation Modeling. 6.1. pp. 1-55.

Humphrey, S., W., (1989): „Managing the Software Process", Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA 1989

IBM (2014): Big Data & Analytics Maturity Model, Blogs, Chris Nott, 15.08.2014 https://www.ibmbigdatahub.com/blog/big-data-analytics-maturity-model (2019.05.20.)

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

Kehl, D., (2011): Skálák és statisztikák: a méréselméletről és történetéről. Statisztikai Szemle, 89. évfolyam 10-11. Szám

Klimkó, G., (2001): „Knowledge Management and Maturity Models: Building Common Understanding", En: The Second European Conference on Knowledge Management. MCIL, Reading, UK, Bled, Slovenia

Kruse, S., Pankey, B., (2010): „Assessing the Effectiveness of Security Awareness Training", RSA and Tunitas Group, 2010

Kruse, S., Pankey, B., (2018): User Awareness Maturity Model (UAMM)
http://securitymetrics.org/attachments/Metricon-6.5-Kruse.pdf (2018.03.05)

Kvale, S., (1996): "Interviews: An Introduction to Qualitative Research Interviewing.", Thousand Oaks, CA, Sage, 1996.

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

Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, H., M., (2014): "Information security awareness and behavior: a theory-based literature review", Management Research Review, Vol. 37 Iss: 12, pp. 1049 – 1092

Longbottom, C., (2018): The ITIL 2018 update better catch up to modern IT
https://searchitoperations.techtarget.com/opinion/The-ITIL-2018-update-better-catch-up-to-modern-IT (2018.07.30)

Magyar Nemzeti Bank 26/2018. (VIII.16.) számú ajánlása a pénzforgalmi szolgáltatások működési és biztonsági kockázataival kapcsolatos biztonsági intézkedésekről (PSD2), Budapest, 2018

Maqousi, A., Balikhina, T., Mackay, M., (2013): „An effective method for information security awareness raising initiatives", IJCSIT Vol 5, No. 2, pp. 63-72

Merkow, S.M., Breithaupt, J. (2014): Information Security: Principles and Practices, 2nd Edition, Pearson IT Certifications Part of the Certification/training series, ISBN 978-0-7897-5325-0

Molnár, B., Kő, A., (2009): Információrendszerek auditálása; az informatika és az információrendszerek ellenőrzési és irányítási módszerei, Corvinno Kiadó, Budapest, ISBN 978-963-06-7254-2

Muha, L., (2008): Az informatikai biztonság egy lehetséges rendszertana, 2008 (In.: Bolyai Szemle, XVII. évf. 4. szám, p.137-156., Budapest: ZMNE BJKMK, ISSN: 1416-1443)

Nemeslaki, A., Sasvári, P., (2015): „Empirical Analysis of Information Security Awareness in the Business and Public Sectors in Hungary" Central and Eastern European e|Dem E|Gov Days 2015, Conference Proceedings, pp. 405-418

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

Nott, C., (2015): „A maturity model for big data and analytics", IBM, www.ibmbigdatahub.com, http://www.ibmbigdatahub.com/blog/maturity-model-big-data-and-analytics (22.12.2017)

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

Oroszi, E. D., Bálint B., (2019): Biztonságtudatossági szabaduló szoba, avagy a felhasználók biztonságtudatosságnak új fejlesztési eszköze, 2019, WITSEC Konferencia 2019.10.10. (prezentáció)

Osterman Research (2013): Security Awareness Training Effectiveness Report - Results of a Survey of KnowBe4 Customers and Non–Customers - An Osterman Research Survey Report (July 2013)

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., (2013): "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", Computers & Security, Vol. 42 pp. 165-176

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

Paulk, M., C., Curtis, B., Chrissis, M., B., Weber, C., V. (1993): Capability Maturity Model for Software, Version 1.1, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, 1993

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

Poepjes, R., Lane, M., (2012): „An Information Security Awareness Capability Model (ISACM)", Proceedings of the 10th Australian Information Security Management Conference

Project Management Institute (2008): Organizational Project Management Maturity Model (OPM3): Knowledge foundation: An American National Standard, ANSI/PMI 08-004-2008 / published by Project Management Institute

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

Sasvári, P., Nemeslaki, A., Rauch, W. (2015): „Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises", AARMS Vol. 14, No. 1, pp. 63-78

Siponen, T., M. (2000): “A conceptual foundation for organizational information security awareness”, Information Management & Computer Security, Vol. 8 Iss 1 pp. 31-41

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)

Stevens, S. S. (1946): On the Theory of Scales of Measurement. American Association for the Advancement of Science. Vol. 103. No. 2684. pp. 677–680.

Tari, A., (2010): Y generáció. Jaffa Kiadó. (2010) ISBN: 9789639971202

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

Wieringa, J., R., (2014): Design Science Methodology for Information Systems and Software Engineering, Springer-Verlag Berlin Heidelberg, ISBN 978-3-662-43838-1

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

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)

SZAKMAI PUBLIKÁCIÓK KIVONATAINAK LISTÁJA

SEFBIS JOURNAL NO.11/2017

Some Conceptual Questions on Information Security Awareness

Abstract. This article is focused on the concept of Information Security Awareness (ISA). ISA is referred very often in numerous articles related security but the concept itself is weakly defined. Some misinterpretations also experienced in the rich literature of the topic. This study completes a limited review and assessment on some existing approaches, definitions and provides a comprehensive discussion on the concept. The article also focuses on risks related to ISA and its control environment. The aim of this conceptual work to provide a solid basis for further research on measuring ISA maturity in various type of organizations.

SEFBIS JOURNAL NO.12/2018

Measuring Organizational Information Security Awareness Levels Supported by a Maturity Model

Abstract. With reference to a concept of Information Security Awareness (ISA) this article talks about the importance of measuring ISA as a focal point for an improved competitiveness of organizations. The measurement possibilities are limited by some ethical aspects and some measurement scale related challenges are also existing. Providing a balanced and selected picture of maturity models we describe a theoretical maturity model (MM) for measuring ISA in organizations. The presented model in this paper is waiting for tests and validations but as an initial step for further studies can be considered. Based on this study we have a solid basis for modelling ISA strengths in various organizations. The value of the elaborated ISA MM will be tested and validated in the next phase of the research, but it is important to initiate a discussion about the limitations of the ISA MM in an early phase of research.

Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben – egy érettségi modell alkalmazása

Absztrakt. A szervezetek információ vagyona és annak védelme a profit és a non-profit széférában is egyre nagyobb jelentőséggel bír. Egyrészt versenyképességi kérdés, másrészt pedig olyan megfelelőségi kritérium, melyet számos nemzetközi standard és előírás vár el a szervezetektől (lásd pl. a SOX, HIPAA, GLBA, FISMA, PCI DSS, ISO 27001 és egyéb standardokat). Az információbiztonsági incidensek, káresemények döntő hányada emberi hibára, gondatlanságra, szándékosságra vezethető vissza, ami ellen leginkább az információbiztonsági tudatossággal tudunk védekezni. Az információbiztonsági tudatosság alatt a szervezet tagjainak tudását és attitűdjét értjük a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban.

Az egyes szervezetek vezetői számára elemi érdek ennek a tudatosságnak a növelése az egyén és a szervezet szintjén. Doktorandusz-hallgatóként ennek kapcsán megfogalmaztam néhány kutatási kérdést és az egyes kérdések kapcsán megpróbáltam szakmai válaszokat alkotni szakirodalmi kutatás, modellalkotás és elemzés útján. A kérdések és a kapcsolódó kutatási eredmények:

Hogyan írható le, hogyan értékelhető a szervezetekben az információbiztonsági tudatosság szintje, minősége? A szakirodalom tanulmányozása rávilágított arra, hogy igazából nincs koherens és konzisztens definíciója az információbiztonsági tudatosságnak. Számos szerző számos megközelítésben tárgyalja a témát, és a cikkben kitérek erre a definíciós problémára, és bemutatok egy lehetséges definíciót, melyet egy érettségi modell megalkotásához is felhasználtam.

Összehasonlíthatók-e a szervezetek? Szervezeti szinten az összehasonlíthatóságot támogatják az ún. érettségi / kiválósági modellek, melyek a szervezeti működés számos területére születtek meg. A szervezeti információbiztonsági tudatosság érettségi modelljének egy vázlatos leírását adja a SANS Institute 2012-ben publikált majd 2017-ben tovább finomított modellje. Kutatásom során ezt a modellt felhasználva készítettem egy referencia (érettségi) modellt, mely alkalmas lehet a mérésekkel kapcsolatos tudományos kritériumok (pl. megismételhetőség) teljesítésére.

Támogatható-e a tudatosság értékelés hagyományos audit eszközökkel (pl. ellenőrző listák)? Auditorként is dolgozva azt tapasztalom, hogy bizonyos kontrollok megléte vagy hiánya utal a szervezet információbiztonsági tudatosságának érettségére, szintjére. Az ismertetésre kerülő érettségi modell ezeket az audit bizonyítékokat is igyekszik számba venni, támogatandó az információbiztonsági tudatosság értékelésére irányuló törekvéseket.

A cikk a fenti kutatási kérdésekben való előre haladásról kíván számot adni annak érdekében, hogy bemutasson egy részletesebb érettségi modellt, melynek validálása megkezdődött egy értékelhető méretű mintán magyarországi szervezetek (elsősorban pénzügyi szektor) körében.

Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben – egy kérdőíves felmérés eredményei

Absztrakt. A szervezetek információ vagyona és annak védelme a profit és a non-profit széférában is egyre nagyobb jelentőséggel bír. Ez egyrészt egy versenyképességi kérdés, másrészt pedig olyan megfelelőségi kritérium, melyet számos nemzetközi standard és előírás vár el a szervezetektől (lásd pl. a SOX, HIPAA, GLBA, FISMA, PCI DSS, ISO 27001, TISAX és egyéb standardokat). Az információbiztonsági incidensek, káresemények döntő hányada emberi hibára, gondatlanságra, szándékosságra vezethető vissza, ami ellen leginkább az információbiztonsági tudatossággal tudunk védekezni. Az információbiztonsági tudatosság alatt a szervezet tagjainak tudását és attitűdjét értjük a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban.

Az egyes szervezetek vezetői számára elemi érdek ennek a tudatosságnak a növelése az egyén és a szervezet szintjén. Doktorandusz-hallgatóként ennek kapcsán megfogalmaztam néhány kutatási kérdést és az egyes kérdések kapcsán megpróbáltam szakmai válaszokat alkotni szakirodalmi kutatás, modellalkotás, elemzés és egy kérdőíves felmérés útján. A kérdések és a kapcsolódó kutatási eredmények:

Hogyan írható le, hogyan értékelhető a gazdálkodó szervezetekben az információbiztonsági tudatosság szintje, minősége? A szakirodalom tanulmányozása rávilágított arra, hogy igazából nincs koherens és konzisztens definíciója az információbiztonsági tudatosságnak. Számos szerző számos megközelítésben tárgyalja a témát, előadásomban kitérek erre a definíciós problémára, és bemutatok egy lehetséges definíciót, melyet egy érettségi modell megalkotásához is felhasználtam.

Összehasonlíthatók-e a gazdálkodó szervezetek? Szervezeti szinten az összehasonlíthatóságot támogatják az ún. érettségi / kiválósági modellek, melyek a szervezeti működés számos területére születtek meg. A szervezeti információbiztonsági tudatosság érettségi modelljének egy vázlatos leírását adja a SANS Institute 2012-ben publikált majd 2018-ban tovább finomított modellje. Kutatásom során ezt a modellt felhasználva készítettem egy referencia (érettségi) modellt, mely alkalmas lehet a mérésekkel kapcsolatos tudományos kritériumok (pl. megismételhetőség) teljesítésére.

Milyen kontrollok támogatják egy szervezeten belül az információbiztonsági tudatosságot? Az elkészült érettségi modellt tesztelendő, végeztem egy *on-line felmérést* magyarországi szervezetek körében. Előadásomban ennek a felmérésnek az eredményeit és a belőlük levonható következtetéseket szándékozom bemutatni olyan módon, hogy két nemzetközi mintával (SANS Institute 2018 és 2019) is összevetettem a kapott eredményeket.