HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET INFORMÁCIÓBIZTONSÁGI SZAKOSZTÁLY

EIVOK-11. Információbiztonsági Szakmai Fórum
2019.10.03.

Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben – egy kutatás előzetes eredményei

Tarján Gábor
Ügyvezető partner
www.magicom.hu

Miért kell tudatossággal foglalkoznunk az EIVOK-ban? (1.)

- Törvényi előírás: *Az állami és az önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (1) bekezdésének g) pontja értelmében a szervezet vezetőjének gondoskodnia kell az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek (biztonságtudatosság) szinten tartásáról.*

Miért kell tudatossággal foglalkoznunk az EIVOK-ban? (2.)

- a 41/2015. (VII.15.) BM rendelet) meghatározza, hogy „*az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára*", mely képzésnek nem csak a belépéskor kell megtörténnie, hanem az ismeretek felfrissítése és aktualizálása érdekében rendszeresen (célszerűen évente) meg kell tartani.

Egy „tudományos” kutatás kérdései

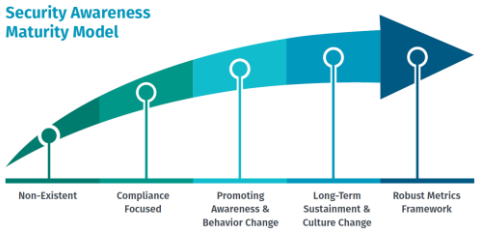
- Q1: Hogyan írható le, hogyan értékelhető a szervezetekben az információbiztonsági tudatosság szintje, minősége a szervezet szintjén?
- Q2: Mérhető-e a változás (javulás, romlás) egy szervezet életében a tudatosság érettségi szintje vonatkozásában?
- Q3: Összehasonlíthatók-e a szervezetek az információbiztonsági tudatosság érettsége szempontjából szervezeti szinten?
- Q4: Támogatható-e a tudatosság szintjének értékelése hagyományos audit eszközökkel (pl. ellenőrző listák)?
- Mely kontrollok megléte és működése jellemző az egyes érettségi szinteken?
- Milyen audit bizonyítékokat találhatunk egy szervezetben az egyes jellemző kontrollok működésére?

Információbiztonsági tudatosság / Information security awareness (ISA)

Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban. / *ISA is a knowledge and attitude of interested parties of an organization on the protection of information assets owned or managed by the organization.*

- Érdekelt felek?
- Tudás?
- Attitűd?
- Saját tulajdonú vagy kezelt információk?

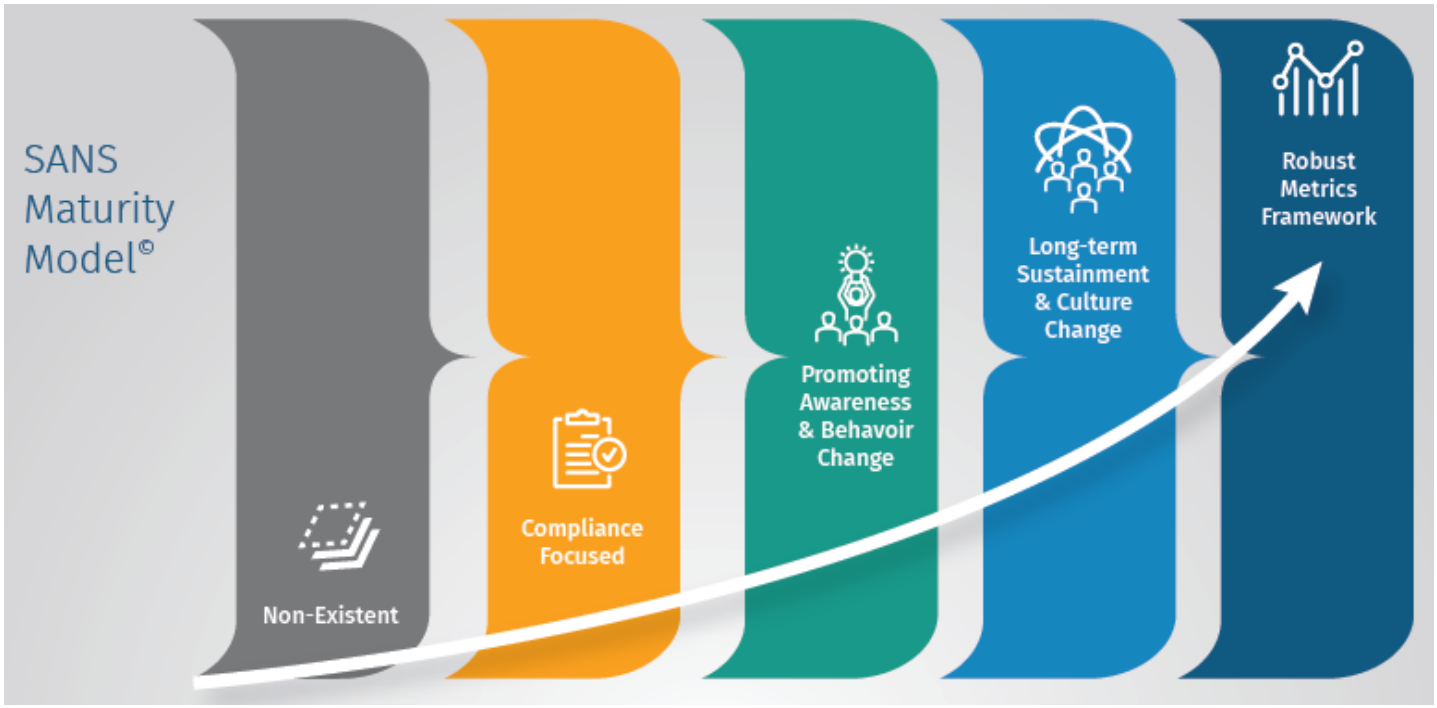
SANS Institute - Az Információbiztonsági Tudatossági Érettségi Modell
(2012.05.22. Lance Spitzner blogbejegyzése – 2017 – 2018 - 2019…)



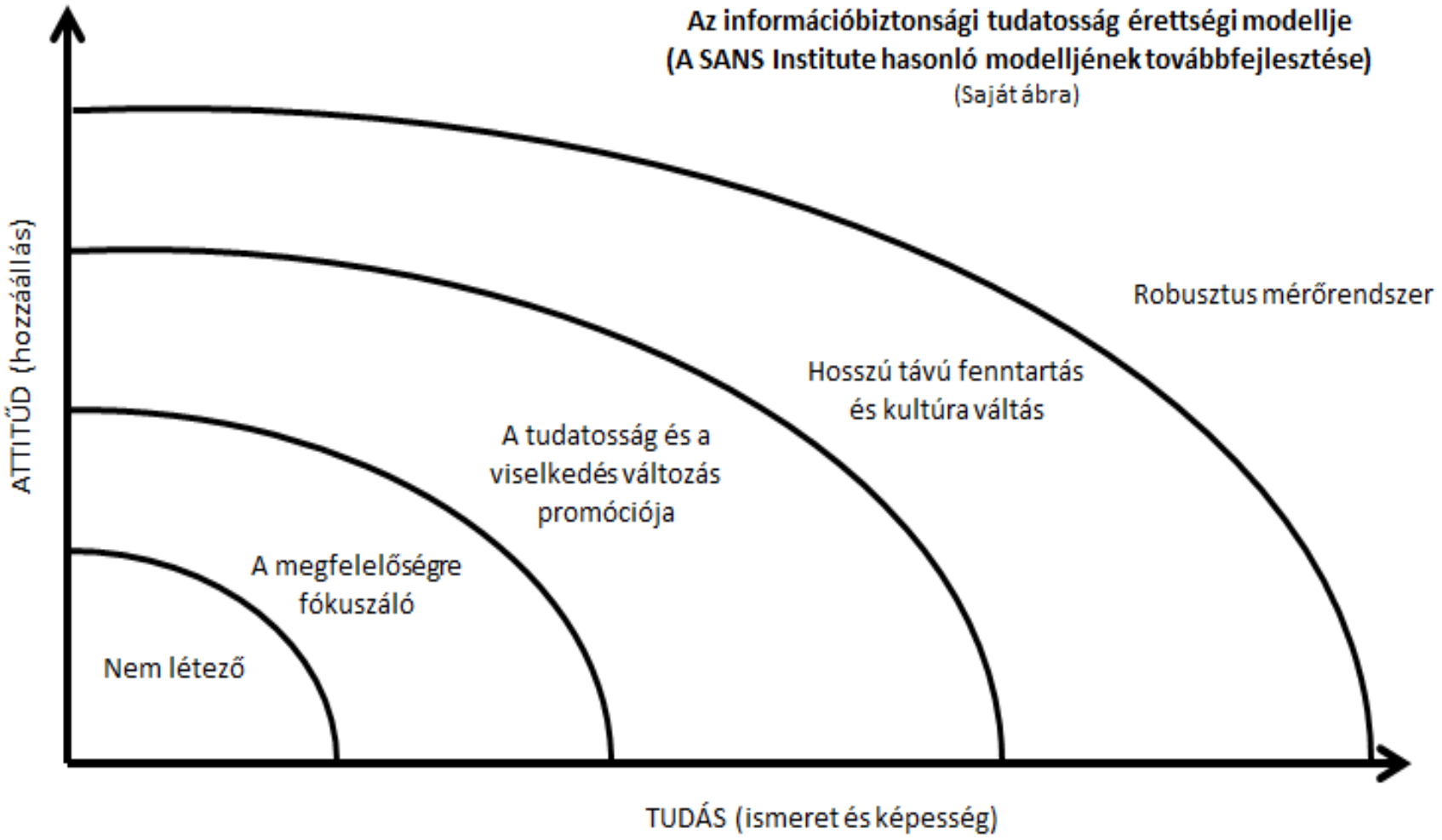
2012

A SANS Institute 5 fokozatú modellje 2012-19

2019



A SANS Institute modelljének továbbfejlesztése (TG - 2018)



Érettségi szint (a SANS model alapján)	A szint általános jellemzői	Tudást (ismeret és képesség) támogató kontrollok	Attitűdöt (hozzállást) támogató kontrollok	Audit bzonyítékok
Nem létező	Információbiztonsági tudatosság gyakorlatilag nem létezik.	Nincsenek.	Nincsenek.	Nincsenek a tudatosság létezésére vonatkozóan.
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
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.
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).
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.

Részletező saját modell

On-line kérdőívezés (kvantitatív kutatás)

- 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 feltételezés: 2000 egyedi célszemély, *30 %-os válaszadási ráta*!, 600 fős minta, 500 gazdálkodó szervezet
- A realitás: összesen 85 kitöltő és az elsődleges szűrés után egy 74 elemű minta maradt!

A vizsgálat (kutatás) logikája

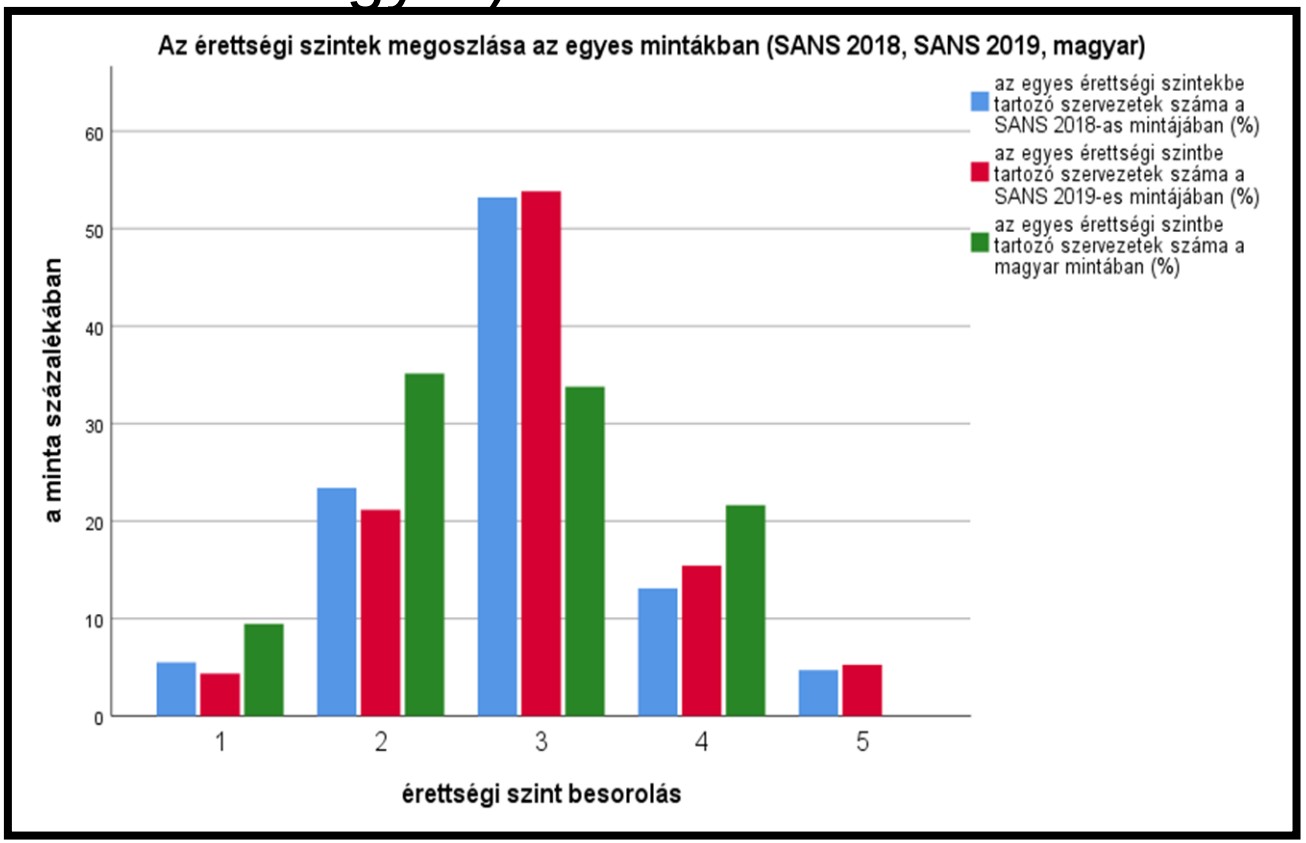
1. Válaszadói (demográfiai) jellemzők begyűjtése
2. A válaszadó besorolja szervezetét a modell alapján
3. A válaszadó egy előre megadott listában megjelöli azokat a kontrollokat, melyek léte jellemző a szervezetére…
4. A válaszadó egy előre megadott listában megadja azokat az audit bizonyítékokat, melyeket fel tud a szervezete mutatni egy audit során…
5. *A (remélhetően) statisztikai méretű mintán vizsgáljuk az érettségi szint besorolás és a jellemző kontrollok és az audit bizonyítékok kapcsolatát (kapcsolati erősségét)!*

Az előzetes kutatási eredmények

- Egy elméleti keretrendszer megalkotása: (Saját) definíció alkotás
- Megközelítések és modellek tanulmányozása (Dzazali-Zolait – SEM, SANS Institute – érettségi modell)
- Saját részletes érettségi modell alkotása
- Kérdőívezés eredményei – főbb megállapítások (a mintához kötötten):
  - A hazai és a nemzetközi (SANS) minta eltérő jellegű megoszlást mutat.
  - Az üzleti vállalkozások jellemzően magasabb szintbe sorolódnak mint a non-profit szervezetek.
  - A szervezeti méret nem befolyásolja jellemző módon a besorolási szintet.
  - Minél több az említett kontrollok száma a szervezetben, annál magasabb a szervezet érettségi szintje, és ez egy viszonylag erős kapcsolatnak mondható.
  - Egy szervezetben minél több az audit bizonyíték annál magasabb a szervezet érettségi szintje, de ez nem mondható egy erős kapcsolatnak.

Három minta összevetése (SANS 2018 és 19, magyar)

- A két SANS minta (1700 és 1500 elemű) jó közelítéssel normális eloszlást mutat.
- A magyar minta (74 elemű) markáns módon más képet mutat.



A szervezet jellege (for profit / non profit) vs érettségi szint besorolás

A szervezet jellege * szintbesorolás Crosstabulation

Count

		szintbesorolás				Total
		1	2	3	4	
A szervezet jellege	Non-profit szervezet	4	14	7	1	26
	Üzleti vállalkozás	3	12	18	15	48
Total		7	26	25	16	74

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	11,898[a]	3	0,008
Likelihood Ratio	13,366	3	0,004
N of Valid Cases	74		

a. 2 cells (25,0%) have expected count less than 5. The minimum

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	0,401	0,008
	Cramer's V	0,401	0,008
N of Valid Cases		74	

74 elemű magyar minta

Független változó: A szervezet jellege

Függő változó: a szervezet érettségi szint besorolása

A két változó között szignifikáns összefüggés van, mert $p < 0,05$. Vagyis az, hogy milyen a szervezet jellege, befolyásolja azt, hogy milyen érettségi szintbe sorolódott be. Az üzleti vállalkozások jellemzően magasabb szintbe sorolódtak, mint a non profit szervezetek.

A Cramer's V mutató egy asszociációs együttható, amely két nominális változó közötti kapcsolat szorosságát mutatja meg. Mivelhogy van egy ordinális (szintbesorolás) és egy nominális (szervezeti jelleg) változónk, amelyek közötti kapcsolat szignifikáns, ezért a Cramer's V értékét is értelmeznünk kell. A Cramer's V értéke 0,401, tehát megállapíthatjuk, hogy a két változó között közepesnél kicsit gyengébb szignifikáns kapcsolat van.

A szervezet mérete és az érettségi szint besorolás (korreláció vizsgálat)

74 elemű magyar minta

Kérdés: A szervezet mérete (1-10, 11-50, 51-250, 250 felett) befolyásolja-e az érettségi szintjét?

Feltételezés (H0): A nagyobb méretű szervezetek tudatosság-érettségi szintje magasabb.

Spearman korreláció két ordinális mérési szintű változó között vizsgálva:

- Szervezeti méret és érettségi szint besorolás (1-2-3-4-5)

A korrelációs együttható jelen esetben = 0,139, tehát gyenge kapcsolat vélelmezhető a két változó között, ráadásul nagyon alacsony szignifikancia szinten (0,238).

Correlations

			A szervezet mérete rangsorba állítva	szintbesorolás
Spearman's rho	A szervezet mérete rangsorba állítva	Correlation Coefficient	1,000	0,139
		Sig. (2-tailed)		0,238
		N	74	74
	szintbesorolás	Correlation Coefficient	0,139	1,000
		Sig. (2-tailed)	0,238	
		N	74	74

Az említett kontrollok száma és az érettségi szint besorolás (korreláció vizsgálat)

Kérdés: A magasabb érettségi szintbe tartozó szervezetek több kontrollt működtetnek?

Feltételezés (H0): Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több kontroll azonosítható a működésében.

A korrelációs együttható szignifikáns, hiszen p < 0,05-nél kisebb. Az együttható értéke: 0,648 pedig közepesnél erősebb pozitív irányú kapcsolatot jelez a két változó között, azaz minél több az említett kontrollok száma a szervezetben annál magasabb a szervezet érettségi szintje, és ez egy viszonylag erős kapcsolatnak mondható.

Correlations

		Említett kontrollok száma	besorolás
Említett kontrollok száma	Pearson Correlation	1	,648**
	Sig. (2-tailed)		0,000
	N	74	74
besorolás	Pearson Correlation	,648**	1
	Sig. (2-tailed)	0,000	
	N	74	74

**. Correlation is significant at the 0.01 level (2-tailed).

Az audit bizonyítékok* száma és az érettségi szint besorolás (korreláció vizsgálat)

Kérdés: A magasabb érettségi szinthez több audit bizonyíték tartozik?

Feltételezés (H0): Minél magasabb érettségi szintbe sorolnak be egy szervezetet, annál több audit bizonyítékot szolgáltat.

A korrelációs együttható majdnem szignifikánsnak mondható, hiszen p < 0,05-hez közeli. Értéke: 0,226 pedig közepesnél gyengébb pozitív irányú kapcsolatot jelez a két változó között, azaz minél több az audit bizonyíték annál magasabb a szervezet érettségi szintje, de ez nem mondható egy erős kapcsolatnak.

Correlations

		Említett audit bizonyítékok száma	besorolás
Említett audit bizonyítékok száma	Pearson Correlation	1	0,226
	Sig. (2-tailed)		0,053
	N	74	74
besorolás	Pearson Correlation	0,226	1
	Sig. (2-tailed)	0,053	
	N	74	74

**Audit bizonyíték: Minden olyan feljegyzés, személyes megfigyelés, állapotjellemző, tapasztalás, mely arra utal, hogy egy adott kontroll működik a szervezetben (pl. egy képzés megtörténtének egyik audit bizonyítéka az aláírt jelenléti ív)*

Köszönöm a figyelmet!

Tarján Gábor
(06-20-502-7775)
gabor.tarjan@magicom.com