ISACA BUDAPEST CHAPTER

MÁSODIK SZERDAI ELŐADÁS

TARJÁN GÁBOR: AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN – EGY KUTATÁS ELŐZETES EREDMÉNYEI

2019.11.13.

Felelősség kizárása

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

A kutatás célja, háttere

- Szervezeti vagyon védelme: az információ (mint vagyonelem) védelme
- A védelem kulcseleme: **az ember** (és az ő tudatossága)
- Versenyképességi kérdés (hatásosság és hatékonyság)
- Megfelelőségi kritérium (SOX [2002], HIPAA [1996], GLBA [1999], FISMA [2002], PCI DSS [2016], ISO 27001 [2013], TISAX [2016],…stb.)
- Komplex mérési probléma (skálaelméleti problémák, objektivitás, megismételhetőség, összemérhetőség)
- Több évtizedes auditori gyakorlat

- ***Cél: egy gyakorlatias modell létrehozása iránymutatással (mely kontrollok hatnak az információbiztonsági tudatosságra), hogy a szervezetek tudják fejleszteni a tudatosság érettségi szintjét!***

Kutatás kérdések

- 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?

Kontroll / Control

- „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)
- „The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature. Also used as a synonym for safeguard or countermeasure.” (COBIT 5.0)
- COBIT 2019…

- *… és ebből a kontrollhalmazból azok, melyek hatással vannak a szervezet információbiztonsági tudatossági szintjére!*

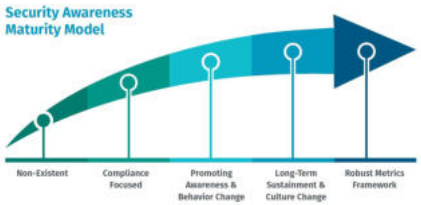
Audit bizonyíték / Audit evidence

- „Basis on which an auditor expresses audit opinion on the accounts and financial operations of the firm being audited. Auditors obtain such evidence from tests that determine how well accounting controls work (called 'compliance tests') and tests of accounting details such as completeness and disclosure of information.” (BD Business Dictionary)
- „Audit evidence supports the conclusions of an auditor during the audit process. It attests that management follows the right procedures to account for the internal controls within the IT environment.” (ISACA)

- *… és ebből a bizonyítékhalmazból azok, melyek utalnak a szervezet információbiztonsági tudatossági szintjére!*

**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)*

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

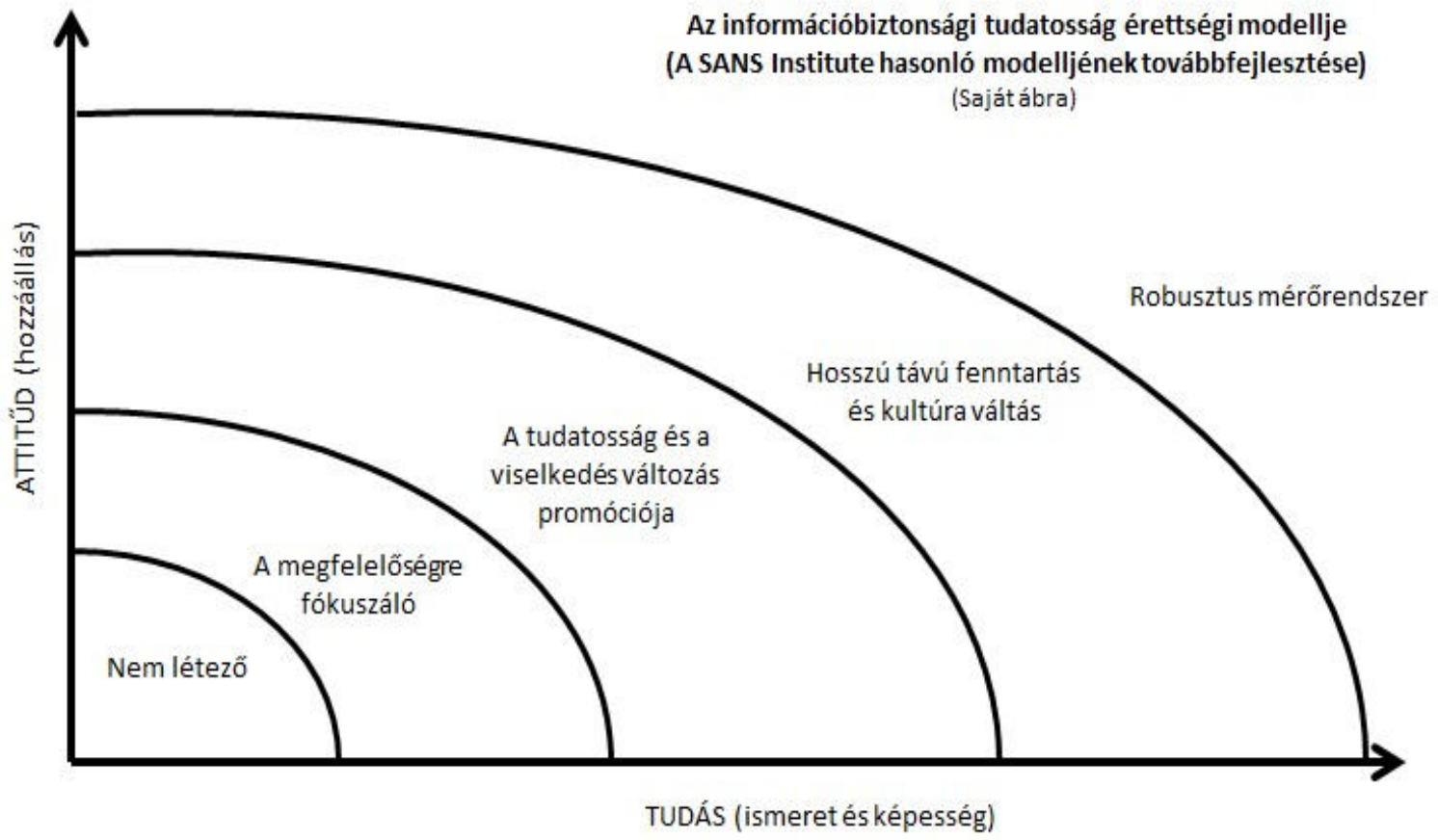


2012

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 bizonyítékok
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, szak-auditor, tanácsadó)
- Az ISACA Budapest Chapter tagsága (kb. 550 személy, gyakorló auditorok, tanácsadók, kockázatmenedzserek az IT területén)
- Az EIVOK tagsága (kb. 190 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 113 kitöltő és az elsődleges szűrés után egy 99 elemű minta maradt! *(2019.10.25.-ei állapot)*

A kérdőíves 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)!*

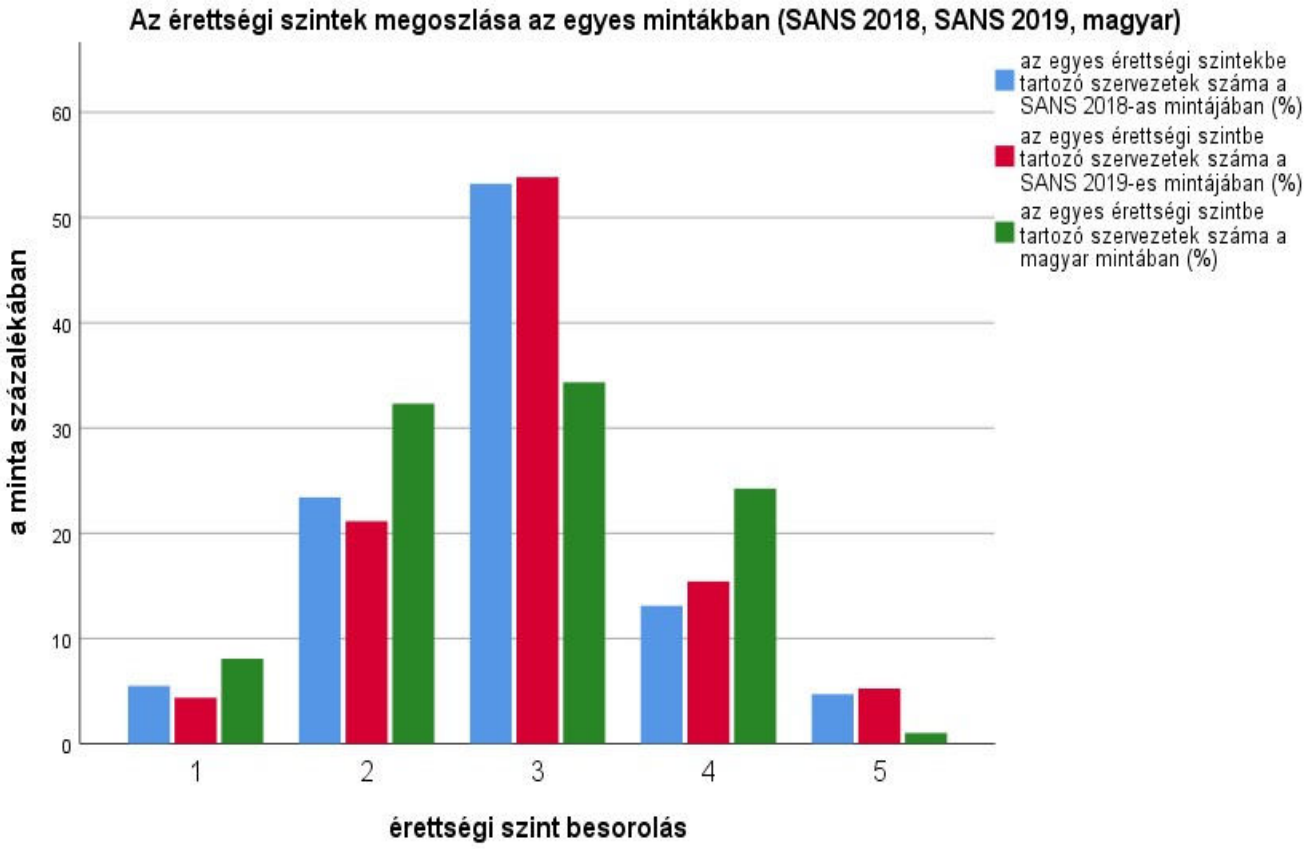
On-line kérdőívezés - Vizsgált attribútumok

(zöld színnel jelölve azok az attribútumok, melyekre értelmezhető és felhasználható adatmennyiséget kaptunk)

- A kérdőív kitöltői által az adott szervezet besorolása a kidolgozott érettségi modellben (1-5 fokozatú skála)
- A gazdálkodó szervezet jellege (non profit / for profit)
- A szervezet tevékenysége, szektora (állami szerv, önkormányzat, illetve iparági besorolás)
- A szervezet mérete (létszám alapján: mikro, kis, közép és nagyméretű)
- A kérdőív kitöltőjének szervezeti pozíciója (CEO, CIO, CISO, egyéb)
- A szervezetben meglévő és működő jellemző biztonságtudatosságot támogató és/vagy erősítő kontrollok
- A szervezetben fellelhető audit bizonyítékok *(melyek igazolják a fenti biztonságtudatosságot támogató kontrollok létét és működését)*

Három minta összevetése (SANS 2018 és 19, magyar)

- A két SANS minta (1700 és 1500 elemű) jó közelítéssel normális eloszlást mutat.
- A magyar minta (99 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	5	
A szervezet jellege	Non-profit szervezet	4	14	8	1	0	27
	Üzleti vállalkozás	4	18	26	23	1	72
Total		8	32	34	24	1	99

(99 elemű magyar minta)

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	13,539[a]	4	0,009
Likelihood Ratio	15,654	4	0,004
N of Valid Cases	99		

a. 3 cells (30,0%) have expected count less than 5. The minimum expected count is ,27.

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.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	0,370	0,009
	Cramer's V	0,370	0,009
N of Valid Cases		99	

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 0,370, tehát megállapíthatjuk, hogy a két változó között közepesnél kicsit gyengébb szignifikáns kapcsolat van.

A szervezet mérete és az érettségi szint besorolás (korreláció vizsgálat 99 elemű mintán)

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 rang-korrelációs együttható jelen esetben = 0,157, tehát gyenge kapcsolat vélelmezhető a két változó között, ráadásul viszonylag alacsony szignifikancia szinten (0,120).

A szervezet mérete rangsorba állítva (1-4) * szintbesorolás (1-5) Crosstabulation

		szintbesorolás (1-5)					
		1	2	3	4	5	Total
A szervezet mérete rangsorba állítva (1-4)	1	1	2	1	0	0	4
	2	2	3	5	4	0	14
	3	3	6	6	3	0	18
	4	2	21	22	17	1	63
Total		8	32	34	24	1	99

Symmetric Measures

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	0,173	0,098	1,734	,086[c]
Ordinal by Ordinal	Spearman Correlation	0,157	0,100	1,568	,120[c]
N of Valid Cases		99			

a. Not assuming the null hypothesis.

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

c. Based on normal approximation.

Az említett kontrollok száma és az érettségi szint besorolás (korreláció vizsgálat 99 elemű mintával)

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 rang-korrelációs együttható szignifikáns, hiszen p < 0,05-nél kisebb. Az együttható értéke: 0,624 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.

Symmetric Measures

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	0,632	0,061	8,038	,000[c]
Ordinal by Ordinal	Spearman Correlation	0,624	0,070	7,863	,000[c]
N of Valid Cases		99			

a. Not assuming the null hypothesis.

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

c. Based on normal approximation.

Az audit bizonyítékok* száma és az érettségi szint besorolás (korreláció vizsgálat 99 elemű mintával)

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 rang-korrelációs együttható szignifikáns, hiszen p < 0,05 alatti. Értéke: 0,464 pedig közepes pozitív irányú kapcsolatot jelez a két változó között, azaz minél több az audit bizonyíték, annál magasabb a szervezet érettségi szintje, és ez egy közepesen erős kapcsolatnak mondható.

Symmetric Measures

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Interval by Interval	Pearson's R	0,493	0,075	5,573	,000[c]
Ordinal by Ordinal	Spearman Correlation	0,464	0,091	5,164	,000[c]
N of Valid Cases		99			

a. Not assuming the null hypothesis.

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

c. Based on normal approximation.

**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)*

TARJÁN GÁBOR
GABOR.TARJAN@MAGICOM.COM

Köszönöm a figyelmet!