LOGISZTIKAI

TRENDEK ÉS LEGJOBB GYAKORLATOK

VI. évfolyam 1. szám 2020. június

A fenntartható ellátási lánc kihívásai

Fókuszban a teljesítménymérés

Tartalom

LOGISZTIKAI
TRENDEK ÉS LEGJOBB GYAKORLATOK

Alapító:
Dr. Karmazin György †

BI-KA Logisztika Kft.
alapító tulajdonosa

A Logisztikai trendek és legjobb gyakorlatok kereskedelmi forgalomban nem kapható, zárt terjesztésű szaklap.
Megjelenik évente 2 alkalommal.
ISSN 2416-0555 (Nyomtatott) · ISSN 2560-0362 (Online)

Főszerkesztő: Dr. habil Oláh Judit· *Főszerkesztő helyettes:* Dr. habil Kozma Tímea.
A szerkesztőség címe és elérhetőségei:
5000 Szolnok Városmajor u. 23.
Telefon: +36 30 4224 117; +36 20 480 4177 · E-mail: logisztikaitrendek@gmail.com
Felelős kiadó: BI-KA Logisztika Kft.

Az aktuális lapszámban szereplő szakcikkek a kiadvány hivatalos online-felületén érhetők el.

Tanúsítványok értékelése ellátási láncok IT biztonsági megfelelésének vizsgálatára

Barta Gergő
IT Menedzser, PhD hallgató
Deloitte Üzletviteli és Vezetési Tanácsadó Zrt., Szent István Egyetem Gazdálkodás és Szervezéstudományok Doktori Iskola
e-mail: gbarta@deloittece.com

Absztrakt

A szervezetek és ellátási láncok a közös együttműködés hatékonyságának növelése érdekében operatív szinten is mindinkább integrálódnak, mely magába foglalja a közös adatkezelést és informatikai rendszerek megosztását, ezért jogosan merül fel az elektronikus erőforrások sértetlenségének, bizalmasságának és rendelkezésre állásának a kockázata, mely az egymásra utaltságból, a kellően nem ellenőrzött IT biztonsági kontrollok üzemeltetéséből és a kibervédelmi fenyegetettségekből ered. Egy szervezetnek nem elég a saját biztonsági környezetének magas színvonalon történő üzemeltetése, meg kell bizonyosodnia arról, hogy partnerei is betartják az általa megkövetelt IT biztonsági kontroll-előírásokat, mivel egy-egy hiányosság az ellátási láncban az egész lánc reputációjába kerülhet. A megfelelési kényszer jogi oldalon is megjelenik, a GDPR 2018. május 25-étől kötelező érvényű, ezért kiemelt figyelmet kell fordítani a személyes adatok védelmére. A cikk célkitűzése, hogy kielemezze azon tanúsítványokat, melyek bizonyosságot adhatnak egy szervezetnek, hogy beszállítói és partnerei is követik az IT biztonsági jógyakorlatokat, melyet akár szerződésben is kiköthet.

Kulcsszavak:
IT biztonság, Ellenőrzés, Tanúsítás, Kockázatkezelés, Harmadik fél tanúsítása

Abstract

Organizations and supply chains are increasingly getting integrated at operational level so as to enhance the effectiveness of joint cooperation, which includes joint data management and the utilization of shared IT services, therefore there is a risk of compromised integrity, confidentiality and availability of information resources that is arising from the interdependence of companies, the ineffectively operated IT security controls and cyber security threats. It is not enough for an organization to operate its own security environment in an effective manner, it must ensure that its partners also comply with the IT security control requirements. Even a single deficiency in the supply chain can lead to reputational loss for each of the organizations. The pressure to be compliant has also appeared from legal part, the GDPR has become mandatory to be implemented since 25 May 2018, and thus, special care must be paid to the protection of personal data. The purpose of this article is to analyze the certifications that may provide assurance to an organization that its suppliers and partners also follow IT security best practices, which they can even enforce in their contract.

Keywords:
IT security, Audit, Certification, Risk management, Third party assurance

DOI: 10.21405/logtrend.2020.6.1.27

1. Bevezetés

A globalizációnak, az egyre inkább növekvő piaci versenynek, az egyre komplexebb és egyre rövidebb életciklusú termékeknek, az egyre gyakrabban változó vevői igényeknek, valamint napjaink talán egyik legjelentősebb tényezőjének, vagyis a digitális transzformáció hatásának köszönhetően új gyártási technológiák, üzleti folyamatok, újszerű vállalati stratégiák, üzleti modellek, rugalmas szervezeti struktúrák és globális ellátási lánc hálózatok alkalmazása válik szükségessé (Tóth et.al,2017a, 2018, Kozma et.al, 2017). Az ellátási láncokba szerveződő vállalatoknál a fenntarthatóság kérdése beépült a vállalati politikák közé. A legismertebb környezetirányítási rendszer (IR) az EMAS, melynek előfeltétele az ISO 14001 szabvány megléte (Kovács et.al, 2018)

Ezért a szervezetek és ellátási láncok a közös együttműködés hatékonyságának növelése érdekében operatív szinten is mindinkább integrálódnak. Az üzleti folyamatok magas szintű automatizálása és a technológia trendek követése potenciális üzleti előnyhöz vezethet, azonban, a mai nap inkább már a lemaradás kockázatát próbálják meg a szervezetek mérsékelni komplex és intelligens rendszerek fejlesztésével és implementálásával, amely ugyanakkor számos sérülékenységet rejt magában (Görcsi et al., 2019). Ezen sérülékenységeket a támadók gyorsan kihasználhatják, és pillanatok alatt kezet emelhetnek a kiszemelt szervezet üzletileg kritikus adatvagyonára. A rosszindulatú kiberbűnözőkön kívül veszélyt jelenthetnek a szervezet saját munkatársai is, akik véletlen vagy szándékos módon is kijátszhatják az informatikai rendszerek sérülékenységeit, és akarva-akaratlanul is segítenek illetéktelenek kezébe juttatni értékes adatokat. A szervezetek számára kiemelten fontos, hogy magas színvonalú, hatékonyra tervezett, implementált és üzemeltetett IT biztonsági kontrollokkal rendelkezzenek, ha az adatszivárgásból és illetéktelen felhasználásból eredő kockázatokat mitigálni szeretnék (Barta – Görcsi, 2019). Az integrált együttműködés a partnerek, kiszervezést végrehajtó szolgáltatók és a teljes ellátási lánc szereplői között azonban további kockázatokat jelent az IT biztonság szemszögéből is. Az ellátási lánc szereplői nem képesek mindig a többi résztvevő informatikai környezetét kontrollálni, ezért egy gyenge IT biztonsági kontroll-környezet a teljes láncra nézve fenyegetettséget jelent, melyet komoly pénzügyi bírság követhet. Boyens (2016), a NIST program vezetőjének kutatása szerint az adatszivárgások 80%-a ered az ellátási láncokból, és a kutatás résztvevőinek 72%-a nyilatkozott arról, hogy nem rendelkeznek teljes rálátással az ellátási láncuk szereplőire. Továbbá, az incidensek 55% több, mint 25 millió dollár kárt okoz (Boyens, 2016). Kieras et al. (2020) külön kiemeli, hogy az IoT eszközök elterjedésével ezen kitettség

Tanúsítvány/riport	Alkalmazhatóság	Kiterjedés	Kiállító	Árazás (USD)[1]	Megbizonyosodás foka
ISO/IEC 27001	Akkor alkalmazható, ha a szolgáltató szervezet biztosítani szeretné a partnereit arról, hogy megfelelő Információbiztonsági Irányítási Rendszerrel (IBIR) rendelkezik.	A szabványban előre definiált követelmények	Akkreditációs szervezet	10.000 <	Tanúsítvány
ISO/IEC 27701	Akkor alkalmazható, ha a szolgáltató szervezet biztosítani szeretné a partnereit arról, hogy az IBIR-en felül megfelelő Adatvédelmi Irányítási Rendszerrel (AIR) rendelkezik.	A szabványban előre definiált követelmények	Akkreditációs szervezet	10.000 <	Tanúsítvány
ISO 22301	Akkor alkalmazható, ha a szolgáltató szervezet biztosítani szeretné a partnereit arról, hogy megfelelő Üzletmenet Folytonossági Irányítási Rendszerrel rendelkezik.	A szabványban előre definiált követelmények	Akkreditációs szervezet	6.000 <	Tanúsítvány
SOC1	Leginkább akkor alkalmazható, ha a szolgáltató tranzakció feldolgozó rendszerek kapcsán nyújt szolgáltatást, vagy tranzakció feldolgozási tevékenységet végez.	Kiemelt vizsgálati területek a pénzügyi beszámolóra gyakorolt kontrollok	Okleveles könyvvizsgáló	20.000 <	Bizonyosságot adó auditjelentés
SOC2	Akkor alkalmazható, ha a szolgáltató szervezet bizalmas adatokat tárol vagy feldolgoz, bizalmi szolgáltatást nyújt.	Bizalmasság, Rendelkezésre állás, Feldolgozási tevékenységek integritása, Adatvédelem, Biztonság	Okleveles könyvvizsgáló	20.000 <	Bizonyosságot adó auditjelentés
SOC3	Ugyanaz az alkalmazhatósága, mint a SOC2-nek, azonban sokkal általánosabb jellegű.	Bizalmasság, Rendelkezésre állás, Feldolgozási tevékenységek integritása, Adatvédelem, Biztonság	Okleveles könyvvizsgáló	n/a	Bizonyosságot adó auditjelentés kivonata

[1] Becsült érték

1. táblázat: Tanúsítványok és auditjelentések összefoglaló táblázata
Forrás: Saját szerkesztés

várhatóan tovább nő. Bár javasolt szerződésekben külön záradékot meghatározni kizárólag az IT biztonsági követelményeknek, a legnagyobb akadályt az jelenti, hogy számos esetben a partnerek nem képesek annak teljes mértékben megfelelni, ezért szükségessé válhat a megfelelőség kikényszerítése további eszközökkel. Egyrészt a biztonsági tudatosságot magas színvonalon biztosítani kívánó szervezet rendelkezhet úgy, hogy időszakoson auditot végez, tehát az általa alkalmazott biztonsági szakértőgárdát bízza meg, hogy ellenőrizze partnerei megfelelőségét. Ez a megoldás akkor működőképes, ha a szervezet rendelkezik belső szakértelemmel és kidolgozott audit stratégiával. Az is gyakori példa, hogy a partnerek által belsőleg elvégzett audit zárójelentését kéri be a szervezet és értékeli ki, azonban ebben az esetben felmerül a függetlenségi kérdés, azaz az auditált szervezet függetlenül a nem megfelelés következményétől, a vezetéstől és üzleti célkitűzésektől szuverén módon végezte-e el a vizsgálatot (Barta, 2018b). A harmadik lehetőség külső ellenőrök megbízása, akik valamilyen akkreditációs szervezettől vagy független könyvvizsgálótól érkeznek, és képesek tanúsítani vagy auditálni a partnereket a megbízó fél részére valamilyen keretrendszer alapján, ezzel bizonyosságot szerezve a megbízónak a megfelelés tényéről. A tanúsítványok és bizonyosságot adó auditjelentések köre sokszínű, a továbbiakban a legnépszerűbb és leggyakrabban alkalmazott lehetőségek kerülnek bemutatásra és értékelésre. A cikkben ismertetett tanúsítványok és auditjelentések összefoglaló táblázatát az 1. táblázat szemlélteti.

2. Módszertan

Az elemzés hatóköre a jelenleg piacon legelismertebb tanúsítványok és audit riportok köre a teljesség igénye nélkül. Az elemzés kiterjed a tanúsítványok célkitűzéseinek megértésére és alkalmazhatósági kérdéseire. Fókuszban az ellátási láncok általi felhasználhatóság, követelményrendszer, rugalmas testreszabhatóság és az árazás áll. Az elemzés nem teljeskörű, azaz a cél nem az, hogy átfogóan tárgyalásra kerüljenek az egyes tanúsítványok, hanem a fő kérdés az volt, hogy melyeket érdemes elvárni a partnerektől koncentrálva IT biztonsági kérdéskörökre.

3. Tanúsítványok és auditjelentések

3.1 ISO/IEC 27001 – Információbiztonsági IR

Az egyik legnépszerűbb szabvány, mely lehetőséget biztosít akkreditációra az IT biztonsági kontroll-környezet megfelelésének biztosítására az ISO/IEC 27001. 2018 év végén az ISO (International Organization for Standardization, azaz Nemzetközi Szabványügyi Szervezet) által végzett kutatás szerint a világon 31.910 szervezet rendelkezett érvényes tanúsítvánnyal 2018-ban, míg a Magyarországon működő cégek között ez a szám 484 (ISO, 2018). A szabvány alapvetően két részből áll; az első alkotórész az Információbiztonsági Irányítási Rendszer, mint a biztonsági szervezet és folyamatok összességének rendszere és hozzá kapcsolódó elvárások együttese, a második rész a konkrét IT biztonsági követelmények listája kategóriánként (ISO/IEC 27001, 2013). A szabvány hiányossága, hogy jelenlegi állapotban elévültnek tekinthető, számos új technológiai trenddel kapcsolatos követelmény nem szerepel benne. Ilyen pl. a felhőszolgáltatásokra vonatkozó megkötések, mely röviden és összefoglalóan az informatika egy részének, vagy egészének harmadik félhez történő kiszervezését, szolgáltatásként való igénybevételét jelenti általában előfizetéses rendszerben (MNB, 2019). Mindazonáltal az ISO/IEC 27001 rugalmas szabvány, mivel a követelményekhez a szervezet által meghatározott egyéb

kiegészítő kontrollok köre is beépíthető, ezért javasolt szerződéses formában nem kizárólag a szabvány meglétét előírni, hanem az extra elvárásokat is megkövetelni, mely az Alkalmazhatósági Nyilatkozatban kerül definiálásra (Heron, 2019). A szabvány rendelkezik egy külön kontroll kategóriával, amely a beszállítók menedzsmentjével foglalkozik, tehát harmadik felek IT biztonsági szabályozása is teret nyer benne, mely betartatása az ellátási lánc szereplői között megfelelőséget kényszeríthet ki. A tanúsítvány megszerzése lehetséges apróbb kontroll-hiányosságok együttes meglétével, mely azt jelenti, hogy a tanúsítvány szerződés szerinti bemutatásával nem derül fény az esetleges hibákra, mivel az nem része az oklevélnek. A tanúsítvány nem bizonyosságot adó auditjelentés. A PivotPoint Security (2020) adatai alapján a tanúsítás ára kb. 10.000 dollár, amely nem tartalmazza a szervezet további költségeit pl. a felkészülést a megfelelésre, vagy az éves fenntartási költségeket. Továbbá, az ár a tanúsítandó szervezet hatókörétől is függ, ami jelenti az akkreditációba bevont telephelyek számát, nagyságát, az üzleti környezet komplexitását stb. Összességében az ISO/IEC 27001 egy jól kidolgozott, széleskörben elfogadott szabvány, a tanúsítás független akkreditációs fél végzi, ezért indokoltnak tűnik az implementálását az ellátási láncon keresztül kikényszeríteni.

3.2 ISO/IEC 27701 – Adatvédelmi IR

Az ISO/IEC 27701 az ISO/IEC 27001 2019-ben megjelent szabvány kiegészítése, mely számba veszi a személyes adatokra vonatkozóan az adatvédelemmel kapcsolatos jogi követelményeket, és az informatikai kontroll-katalógust az ISO/IEC 27001-hez képest további 32 helyen egészíti ki (ISO/IEC 27701, 2019). A szabvány majdnem egészében a GDPR által támasztott követelményeket sorolja fel, ezért az implementálása nagyban segítheti a jogi megfelelést is. Az ISO/IEC 27701 önmagában nem tanúsítható, kizárólag az ISO/IEC 27001 szabvány részeként, ezért árazás tekintetében hasonló paraméterekkel rendelkezik. A szabvány két fontosabb terület mentén elkülöníthető; első része a személyes adatkezelőkre vonatkozik, a második, az adatfeldolgozókra. A GDPR megjelenése óta a személyes adatok védelme az érintett vállalatok egyik kiemelt prioritása, mely nem kizárólag reputációs kockázatot jelent, de a pénzügyi bírság is jelentős, melyet adott nemzetgazdaság adatvédelmi hatósága szab ki nem megfelelés esetén (Barta, 2018a). Amennyiben az ellátási láncban történik közös adatkezelés, adatfeldolgozás, mely ügyfelek, partnerek, munkavállalók személyes adatait érinti, akkor az ISO/IEC 27001 mellé javasolt az ISO/IEC 27701 implementálása is.

3.3 ISO 22301 – Üzletmenet Folytonossági IR

Az ISO szabvány család egy másik szabványa az ISO 22301, melynek fókuszterülete az üzletmenet folytonosság biztosítása. Az üzletmenet folytonosság fenntartása az ellátási láncok esetén kiemelten kritikus, mivel bármilyen válsághelyzet vagy katasztrófa esetén a stabil üzletműködésben bekövetkező zavarok a lánc összes szereplőjét negatívan érintheti, ezáltal fennakadást okozva az ellátásban és szállításban. A szabvány részletesen tárgyalja az üzletmenet folytonosság fenntartásához szükséges folyamatokat, teendőket és az irányítási rendszer üzemeltetéséhez szükséges követelményeket. Az ISO 22301 bevezetése szinte kikerülhetetlennek tűnik, azonban az ISO/IEC 27001 egy külön fejezetben szintén részleteiben tárgyalja a témakört, melyhez az ISO 22301 csak részben ad hozzá új elvárásokat, ezért javasoltnak bizonyul elsődlegesen az ISO/IEC 27001 megkövetelése, majd a kritikus beszállítók esetén az ISO 22301 kikényszerítése, amennyiben nem elégségesek az ISO/IEC 27001-ben közölt elvárások. Ez a gondolatmenet az akkreditált szervezetek számából is tetten érhető, míg világszerte 2018-ban 1.506 szervezet rendelkezett a tanúsítvánnyal, hazánkban csupán 6 volt az akkreditált szervezetek száma, mely töredéke az ISO/IEC 27001-el tanúsított szervezeteknek (ISO, 2018). Az árazás tekintetében nincs konkrét publikált adat, azonban, ha az ISO/IEC 27001 akkreditáció árából indulunk ki, az első tanúsítás, egyéb költségek nélkül, kb. 6.000 dollárra tehető.

3.4 SOC1/SOC2/SOC3 – Szolgáltató Szervezetek Tanúsítása

A SOC1/SOC2/SOC3 valójában audit riport típusok, keretrendszerek, tehát alapvetően a tanúsító szervezet (okleveles könyvvizsgáló) nem oklevelet, hanem egy auditjelentést bocsájt ki. Legnagyobb előnyük, hogy bizonyosságot nyújtó riportokról van szó, mely részleteiben tartalmazza a tesztelt kontrollok körét, audit eljárásokkal ellátva, beleértve a hiányosságok részletes leírását, ezért az ISO tanúsításokkal ellentétben sokkal részletesebbek, mely nagyobb és valósabb képet adhat az ellátási lánc szereplőinek IT biztonsági helyzetéről. Ezért is a megosztásuk korlátozott, mivel potenciális IT biztonsági sérülékenységet tartalmazhat, így csak egy szűk partneri körnek érdemes kiadni, azonban marketing célokból érdemes a riport meglétét feltüntetni pl. weblapon. A három különböző riport között lényegi különbségek vannak. A SOC1 egy olyan audit riport, mely a szolgáltató azon kontrolljaira vonatkozik, mely a partner/ügyfél pénzügyi beszámolójára hatással lehet, pl. ha az informatikai beszállító a szervezet vállalatirányítási rendszerét üzemelteti. A SOC2 és SOC3 esetén az auditor 5 bizalmi elv (trust principles) mentén végez vizsgálatot, amelyek a bizalmasság, feldolgozási tevékenység integritása, rendelkezésre állás, biztonság és adatvédelem kategóriák. A SOC1 és SOC2 a legrugalmasabb riportok, tehát a hatókörben lévő IT biztonsági kontrollok köre a kötelező kritériumokon kívül tovább bővíthetőek. A SOC3 annyiban különbözik a SOC2-től, hogy főleg marketing célokra lehet alkalmazni, mivel általánosabb jellegű és nem tartalmaz bizalmas információt az IT biztonsági működéssel kapcsolatban (AICPA, 2020). Két féle riport típus különíthető el; Type I., mely kizárólag a kontrollok megfelelését tervezés szinten tárgyalja, míg a Type II., mely implementáció és működési hatékonyság mentén is véleményezni az adott szervezet IT biztonsági működését. A SOC2 és SOC3 számára előírt kontroll-követelmények az AICPA (American Institute of Certified Public Accountants, azaz Könyvvizsgálók Amerikai Szakmai Szervezete) által kiadott „Trust Services Criteria"-ban találhatóak, amely az ISO/IEC 27001-hez hasonlóan ugyancsak több pontban részletezi az elvárásokat a beszállítók felé, mint pl. adatvédelmi követelményeket harmadik felek részéről, a beszállítók értékelését, oktatását illetve egyéb információbiztonsági elvárásokat (AICPA, 2017). A SOC1 és SOC2 riportok ára hasonló, az SSAE-16 oldal szerint alapvetően a Type I. riport 10.000 és 20.000 dollár között mozog, természetesen itt sem számolva a felkészülés költségével és egyéb megelőző felkészülési auditokkal

(SSAE-16, é.n.). A TrustNet (é. n.) ajánlatkérő oldalán a Type I. riportok ára 20.000 dollártól kezdődik, míg ez Type II. esetén 30.000 dollár, azonban itt is fontos kiemelni, hogy az árazást nagyban befolyásolja az audit hatóköre, ami a telephelyek és irodák számát, kontrollok mennyiségét és komplexitását és tesztelendő alkalmazásokat jelent. SOC3 esetén nem elérhető publikus árazás, azonban a SOC3 a SOC2 riportokból könnyedén elkészíthető, ezért, ha marketing célú anyagra van szükség, érdemes elsőre egy SOC2-t elvégezni, majd abból SOC3-at kivonatolni.

4. Konklúzió

A cikk célja az volt, hogy magas szinten összegezze az elérhető tanúsítványokat és megszerezhető auditjelentéseket, melyeket érdemes megkövetelni a beszállítóktól és partnerektől, sőt akár együttműködés feltételévé tenni. Az értékelés alapján legjobban javasolt az ISO/IEC 27001 és/vagy SOC2 elvégzése, mely látható módon nem kizárólag bizonyosságot ad az IT biztonsági helyzetről egy adott szervezet esetén, de segíthet azt megerősíteni ezzel csökkentve a potenciális adatszivárgások és a jövőben bekövetkező IT biztonsági incidensek számát. Az ellátási láncokban kiemelten fontos az együttműködések biztonságának fenntartása érdekében követelményrendszert támasztani a partnerek részére, ezért a folyamatos ellenőrzésnek és tanúsításnak komoly hatása van a kockázatkezelésben.

5. Felhasznált irodalom

- AICPA (2020): SOC for Service Organizations: Trust Services Criteria for General Use Report. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc3report.html
- AICPA (2017): Trust Services Criteria. American Institute of Certified Public Accountants, Inc. New York.
- Barta, G. (2018a): Challenges in the compliance with the General Data Protection Regulation: Anonymization of personal information and related information security concerns. Knowledge – Economy – Society. Business, Finance and Technology as protection and Support for Society. Publishing House: Foundation of the Cracow University of Economics, pp. 115-121.
- Barta, G. (2018b): The Increasing Role of IT Auditors in Financial Audit: Risks and Intelligent Answers. Business, Management and Education 16:1 pp. 81-93.
- Barta, G. – Görcsi, G. (2019): Assessing and managing business risks for artificial intelligence based business process automation. Proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering '2019. Vilnius, Litvánia: Vilnius Gediminas Technical University Press, pp. 823-832.
- Boyens, J. (2016): Integrating Cybersecurity Into Supply Chain Risk Management. RSA Conference 2016. https://www.slideshare.net/cisoplatform7/integrating-cybersecurity-into-supply-chain-risk-management
- Görcsi, G. – Barta, G. – Széles, Zs. (2019): Üzleti intelligencia megoldások alkalmazásának sikertényezői - A hazai szolgáltató szektor nagyvállalatainak körében végzett mélyinterjús kutatás. Információs Társadalom: Társadalomtudományi Folyóirat 19 : 2 pp. 23-34.
- Gyenge, B. - Kozma, T. (2013): The role of quality management in a company's organizational structure. In: Elena, Horska; Iveta, Ubreziova (szerk.) Business Management - Practice and theory in the 21st century - Proceedings Nitra, Szlovákia : Slovak Agricultural University, (2013) pp. 239-248.
- Heron, J. (2019): The ISO 27001:2013 Statement of Applicability (SoA): The Complete Guide. https://www.isms.online/iso-27001/iso27001-statement-applicability-simplified/
- ISO (2018): The ISO Survey of Management System Standard Certifications 2018. https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1
- ISO/IEC 27001. (2013): Information technology – Security techniques – Information security management systems – Requirements. International Standard.
- ISO/IEC 27701. (2019): Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. International Standard.
- Kovács L, Dr. Pónusz M., Dr. Kozma T. (2018): A zöld beszerzés stratégiai jelentősége. LOGISZTIKAI TRENDEK ÉS LEGJOBB GYAKORLATOK. Vol. 4. No. 1, pp. 28-32.
- Kozma, T. - Gyenge, B. - Tóth, R. - Mester, É. (2017): Hazai vállalkozások finanszírozási gyakorlata. In: Fenyvesi, Éva; Vágány, Judit (szerk.) KORKÉP: XXI. századi kihívások. Budapest, Magyarország : Budapesti Gazdasági Egyetem (BGE), (2016) pp. 114-145.
- Kieras, T. – Farooq, M. J. – Zhu, Q. (2020): Modeling and Assessment of IoT Supply Chain Security Risks: The Role of Structural and Parametric Uncertainties. https://arxiv.org/pdf/2003.12363.pdf
- MNB (2019): A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről. https://www.mnb.hu/letoltes/4-2019-felho.pdf
- PivotPoint Security (2020): How much does ISO 27001 Certification Cost? https://www.pivotpointsecurity.com/blog/iso-27001-cost-estimate-48000-information-security-confidence-priceless/
- SSAE-16 (é. n.): How much does a SOC1 Type 1 Cost? https://www.ssae-16.com/faq/how-much-is-a-soc-1-type-1/
- Tóth, R. – Pónusz, M. – Kozma, T. (2018): A vállalkozások stratégiájának és üzleti modelljének változása napjainkban: az e kereskedelem tendenciái és megjelenési formái az ellátási láncokban. LOGISZTIKAI TRENDEK ÉS LEGJOBB GYAKORLATOK 4 : 2 pp. 10-15.
- Tóth, R. – Túróczi, I. – Szijártó, B. – Mester, É. (2017a): Gazdaságélénkítő és versenyképességet erősítő megoldások a vidéki térségekben. A FALU 32: 3 pp. 57-66. , 10 p.
- Tóth, R. – Szijártó, B. – Mester, É. – Túróczi, I. (2017b): A vállalkozások belső és külső finanszírozási gyakorlata – A pénzügyi controlling finanszírozást megalapozó döntések. CONTROLLER INFO 5 : 2 pp. 28-33.
- TrustNet (é.n.): SOC Report Cost. https://www.trustnetinc.com/pricing/soc-ssae18-report-cost/