ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

DOMBORA SÁNDOR

Eredményes információbiztonsági rendszerek kialakítása és bevezetése

Témavezető: Prof. Dr. Michelberger Pál PhD

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2022. hónap nap

Tartalomjegyzék

1 Summary

In my thesis I analysed the operation of ISMS of various organizations. I assessed compliance with the requirements of the relevant local and international laws, standards, and frameworks. Practical experience gained in action research shows that the intensifying legislative environment and more sophisticated standards do not guarantee the necessary information security level for organisations. I examined, explored, standardized and grouped the factors influencing information security, looking for the reasons of occurrence and possibilities of elimination. I searched ISMS (Information Security Management System) models, implementation methods and techniques in the local and international literature that help to improve the materialized information security level.

The shortcomings identified include the structure, clarity and interpretability, applicability (compliance, enforceability and feasibility of requirement implementation), redundancies (inside and with the organisation processes) of the ISMS. Compliance issues are less common, typically because organizations build their information security systems according to the relevant standards or laws.

The results of research projects have confirmed that the relevant standards and legislation provide a good framework for information security implementation. It is the structure, language, design and operation of ISMS that mainly affect the effectiveness of information security.

I developed an ISMS model based on the integration of the requirements of information security legislation and standards, aligned with IT service management processes. I included a generic information security development and maintenance process model. Implementation of which eliminates the shortcomings, facilitates implementation of an effective ISMS, leads to consistent structure, effective collaboration with organization workflows and continuous improvement of information security.

I have developed an integrated incident management model to manage the overlaps and communication gaps of information security incident management with IT service, data protection and security incidents, which integrates and harmonizes the management of these incident types.

2 A kutatás előzményei

Az információbiztonság fogalmával a 2000-es évek elején találkoztam először, amikor az ország legnagyobb hirdetési napilapjánál részt vettem az internetes hirdetési rendszer infrastruktúrájának megépítésében és irányítottam annak üzemeltetését. A legfontosabb szempont az információ rendelkezésre állásának biztosítása és az alkalmazás technológiai védelme volt. Később IT szolgáltatásmenedzsment – köztük incidens, változás és konfigurációkezelés – megoldások bevezetésével kezdtem el foglalkozni, amelyek keretében megismertem az ITIL-t, banki környezetben pedig a COBIT-ot. Munkám során mindig nagy hangsúlyt fektettem a tervezett rendszerek információbiztonságára. 2013-ban volt az első olyan megbízásom, amikor egy szervezetcsoportra kellett ISO/IEC 27001 szabvány szerinti IBIR-t kialakítani. A megbízó kérése az volt, hogy az IBIR-t integráljuk az ITIL alapon kialakított informatikai munkafolyamatokkal, mert szeretné elkerülni azok végrehajtásának ellehetetlenítését. Ekkor derült ki számomra, hogy egy félresikerült IBIR bevezetés amellett, hogy akadályozza a munkát, nem képes eredményesen védeni a szervezet által kezelt információt. Visszaemlékezve a korábbi IT szolgáltatásmenedzsment projektekre rájöttem, hogy szinte minden esetben találkoztunk irracionális vagy munkát akadályozó információbiztonsági szabályzatokkal.

A hazai és nemzetközi felmérésk az ISO/IEC 27001 szabvány különböző követelményeinek meglétére kérdeznek rá, nem vizsgálják azok működőképesét a szervezetben. A tudományos szakirodalomban jellemzően az IBIR szabvány szerinti kialakítására vonatkozó tudományos publikációkat találtam. Kevés olyan írás jelent meg, amelyek az IBIR minőségével és az információbiztonság megvalósulásának szintjével foglalkozik.

3 Célkitűzések

Kutatásom legfőbb célja az volt, hogy megvizsgáljam a szervezetek információbiztonságának kialakítását, a bevezetett IBIR és védelmi intézkedések összhangjának szempontjából, továbbá megmutassam azt, hogy létezik olyan IBIR modell, amelynek megvalósítása eredményesen védi a szervezet által kezelt információt. Ennek keretén belül célul tűztem ki, hogy:

1. meghatározzam az információbiztonsági rendszerek problémáit és feltárjam azok forrását;
2. kidolgozzak egy olyan IBIR modellt, amelynek bevezetése biztosítja a szervezetek jogszabályi és szabvány követelményeknek megfelelő információbiztonságát;

3. meghatározzam az IBIR követelményeinek olyan minimális mennyiségű szabályzatra és eljárásrendre bontásának módját, amely biztosítja a szervezet struktúrájához való illeszkedést;
4. meghatározzam azt a bevezetési módot, amelynek alkalmazásával az általam kidolgozott IBIR modell megvalósítása elősegíti a munkafolyamatok zavartalan végrehajtását, a tervezett biztonsági szint elérése mellett;
5. kidolgozzak egy integrált incidenskezelési munkafolyamatot, amely hatékonyan kezeli az IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági események kezelését.

A kutatásnak nem célja a vonatkozó jogszabályok, szabványok és keretrendszerek teljes körű feltérképezése és bemutatása.

4 Vizsgálati módszerek

Az információbiztonság szervezetekben való működőképességének kutatása több szakterületre bontható. A szakterületek követelményeinek összehangolása meghatározza a kialakított rendszer hatékonyságát és hatásosságát. Az alkalmazott védelmi intézkedések által nyújtott biztonsági szint nyilvánosságra hozatala hatással lehet a szervezetek megítélésére, így a szervezetek igyekeznek bizonyítani a külvilág felé, hogy profi módon védik az általuk kezelt információt. Ahhoz, hogy közelebbről megismerhessem az információbiztonság megvalósításának eredményességét, csak olyan módszertan kiválasztása jöhetett szóba, amely részletes információt szolgáltat az egyes szervezetekben kialakított megoldásokról és azok hatékonyságáról. Az elvégzendő vizsgálatok részletessége miatt nincs lehetőség nagy elemszámú minták statisztikai elemzésére. Ez a megállapítás a kvalitatív módszertanok irányába terelte figyelmemet, mivel a kvalitatív kutatási módszertanok célja a probléma okainak és miértjeinek megértése, eredménye pedig a kiinduló probléma megértése.

Irodalomkutatás keretében feltártam az információbiztonságot és kapcsolatait tárgyaló tudományos szakirodalmat, kitértem az információbiztonság állapotát és fejlesztését befolyásoló tényezőkre. Szakirodalmi feldolgozást végeztem az információbiztonság és a szorosan kapcsolódó szakterületek: minőségirányítás és IT szolgáltatásmenedzsment kapcsolatról. Vizsgáltam az információbiztonság munkafolyamatokra és a szervezet versenyképességére gyakorolt hatását.

Mint a projektek aktív résztvevője adta magát, az akciókutatás módszertana, amelynek célja nemcsak elmélet létrehozása, hanem annak alkalmazása is a gyakorlatban. Az akciókutatás egy

keretet biztosít sokféle lehetősséggel a kutatóknak, amelyek között megtalálhatják a számukra megfelelőt kutatásaik elvégzéséhez.

Az információbiztonság hiányosságainak feltárásához mélyinterjúkat készítettem a szervezetek IT és információbiztonsági vezetőivel. Az így összegyűjtött információ alapján esettanulmányokat készítettem. Ezek alapján a tudásrendezés és megalapozott elmélet módszertanát alkalmazva határoztam meg az információbiztonsági rendszerek állapotát befolyásoló tényezőket.

Megalapozott elmélet módszertanát alkalmazva hoztam létre az IBIR alapmodellemet, amely szakterületek mentén csoportosítja az információbiztonsági követelményeket, ezáltal könnyen leképezhetővé és teszi a szervezet struktúrájára, lehetővé téve annak szervezeti egységek menti szabályzatokra bontását.

Az incidenskezelési siószerű folyamatok megszüntetésére irányuló integrált incidenskezelési modellemet, akciókutatás keretében hoztam létre. Az incidensek közötti összefüggéseket tudásrendezés módszertanával feleltettem meg egymásnak. Ez alapján az IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági incidenskezelés munkafolyamatokat egy modellbe építettem össze a az átfedések kiküszöbölésével.

5 Új tudományos eredmények

1. **Bizonyítottam, hogy a szervezetek információbiztonsági állapotát befolyásoló tényezők függetlenek a szervezet tevékenységétől és méretétől.**

Azonosítottam a szervezetek információbiztonsági állapotát befolyásoló tényezőket. Felfedtem az IBIR strukturális, érthetőségi és értelmezhetőségi, alkalmazhatósági és redundancia problémáit. Jellegük, előfordulásuk és azok okainak feltárása alapján megállapítottam, hogy ezek a tényezők függetlenek a szervezet tevékenységétől és méretétől.

Kapcsolódó publikációim: [110] [114]

2. **Az ITIL munkafolyamatainak, a jogszabályok és szabványok követelményeinek integrálásával megépítettem egy olyan IBIR modellt, amely a feltárt problémák kiküszöbölésével biztosítja a szervezetek számára a szükséges szintű információbiztonságot.**

Elméleti kutatás keretében vizsgáltam az információbiztonság, minőségirányítás és IT szolgáltatásmenedzsment összefügéseit, állapotának és fejlesztésének irányelveit, valamint

bevezetésének módjait. Ezek alapján létrehoztam az IBIR alapmodellt, amely a szabványok és jogszabályok követelményeit redundanciamentes fastruktúrába rendezi. Mivel a feltárt hiányosságok okait az IBIR kialakításának folyamatára vezettem vissza, ezek kiküszöbölésére egy Információbiztonság tervezési és fenntartási szabályzatot építettem be.

Kapcsolódó publikációim: [111] [107] [105] [113] [110].

3. **Az IBIR követelmények szakterületek mentén történő szabályzatokba és eljárásrendekbe csoportosítása, illeszkedik a szervezet struktúrájához megkönnyítve ezzel az IBIR bevezetését.**

Az információbiztonság kapcsolatainak, bevezetési módjainak és IT szolgáltatásmenedzsmentet támogató IBIR lehetőségeinek vizsgálata során megfigyeltem, hogy a szabványok közötti összerendelések jellemzően szakterületenként történtek. IBIR modellem megalkotása során a követelményeket szakterületenként csoportosítottam, ez lehetővé tette a projektek során a szabályzatok és eljárásrendek hozzárendelését a szervezetek szervezeti egységeiben működő szakterületekhez.

Kapcsolódó publikációim: [108] [113] [110].

4. **Létrehoztam az IBIR folyamatszemléletű bevezetési módját, amelynek alkalmazásával megvalósítható a munkafolyamatok zavartalan végrehajtása a szükséges biztonsági szint elérése mellett.**

Elméleti kutatásaim alapján megmutattam, hogy az információbiztonság folyamatlépésekbe építése biztosítja a folyamatok zavartalan működését és folyamatbiztonságot eredményez. Ennek mentén megalkottam a folyamatszemléletű IBIR bevezetési módot. Ez az IBIR integrált bevezetésére épül, tartalmazza az IT szolgáltatásmenedzsment munkafolyamatokat az IT szolgáltatások biztonságos működtetéséhez, a bevezetés legvégén pedig beépíti az információbiztonsági követelményeket a szervezet munkafolyamataiba. Ez a bevezetési mód kiküszöböli az IBIR és szervezeti folyamatok ellentmondásait, ugyanakkor végrehajtása információbiztonsági, folyamatmenedzsment és IT szolgáltatásmenedzsment szaktudást igényel. A bevezetéséhez szükséges erőforrások mértéke függ a szervezet munkafolyamatainak számától és méretétől.

Kapcsolódó publikációim: [115] [111] [107] [108] [112] [118]

5. **Definiáltam egy olyan integrált incidenskezelési munkafolyamat modellt, amely összehangoltan irányítja az IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági eseményeket.**

Létrehoztam egy integrált incidenskezelési munkafolyamat modellt, amely a különböző incidens típusok közötti átfedés esetén azonnali információáramlást biztosít, gyorsabb és hatékonyabb incidens kivizsgálást és reakciókészséget, ezáltal gyorsabb incidenselhárítást biztosít, mint az egymástól független IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági munkafolyamatok párhuzamos működtetése.

Kapcsolódó publikációim: [107] [109] [110]

6 Az eredmények hasznosítási lehetősége

Az azonosított IBIR hiányosságok és előfordulásuk okai felhasználhatók a szervezetek IBIR hiányosságainak feltárására.

A megalkotott eredményes IBIR modell alkalmazható újonnan létrehozandó információbiztonsági rendszer felléptéséhez és meglévő információbiztonsági rendszer megújításához. Az eredmény egy a szervezet struktúrájához igazodó IBIR, amelynek szabályzatai betarthatók és eredményesen védik a szervezet információit.

A folyamatszemléletű IBIR bevezetés segíti a szervezeteket olyan IBIR létrehozásában, amely nem csak eredményes és illeszkedik a szervezet struktúrájához, hanem beépül a munkafolyamatokba elősegítve a folyamatbiztonság megvalósulását is.

Az információbiztonsági követelmények szakterületenkénti csoportosítása, lehetőséget biztosít a szervezetek számára szakterületenként felépített optimális szabályzathierarchia kialakítására.

A megalkotott integrált incidenskezelési munkafolyamat minden szervezet számára hasznos az incidensek gyors észlelésének, kivizsgálásának és megszüntetésének érdekében.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] 187/2015. (VII. 13.) Kormányrendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

[2] 2011. évi CXII. törvény Az információs önrendelkezési jogról és az információszabadságról

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[4] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[5] 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

[6] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

[7] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[8] 42/2015. (VII. 15) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

[9] A Frost & Sullivan Market Study in Partnership with ISC2. (2013) The 2013 (ISC)2 Global Information Security Workforce Study. http://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (Letöltés ideje: 2015.02.27.)

[10] AAGEDAL, Ø. J. et al., „Model-based Risk Assessment to improve Enterprise Security," in *Proceeding of the 6th International Enterprise Distributed Object Computing Conference (EDOC'02)*, 2002., pp. 51-54. DOI:10.1109/EDOC.2002.1137696

[11] Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, Az Európai Unió Hivatalos Lapja, vol. C326, pp. 47-390, Oct. 2012.

[12] BAJAHZAR, A., BASLEM, A., ALQAHTANI, A., "A Survey Study of the Enterprise Resource Planning System," in *Advanced Computer Science Applications and Technologies (ACSAT)*, Kuala Lumpur, Malaysia, 2012., pp. 246-252. DOI:10.1109/ACSAT.2012.101

[13] BARACSKAI, Z., DÖRFLER, V., VELENCEI, J., „Concept Mapping and Expert Systems: Exploring Synergies," , vol. 3. 2008., pp. 70-74.

[14] Best Management Practice, *ITIL Continual Service Improvement*.: TSO, 2011., ISBN 9780113313082

[15] Best Management Practice, *ITIL Service Design*.: TSO, 2011., ISBN 9780113313051

[16] Best Management Practice, *ITIL Service Operation*.: TSO, 2011., ISBN 9780113313075

[17] Best Management Practice, *ITIL Service Strategy*.: TSO, 2011., ISBN 9780113313044

[18] Best Management Practice, *ITIL Service Transition*.: TSO, 2011., ISBN 9780113313068

[19] CALDER, A., *Implementing Information Security Based on ISO 27001/ISO 27002*, 2nd ed. Zaltbommer, Netherlands: Van Haren Publishing, 2009., ISBN 978 90 8753 540 7

[20] CANO, J,, J., "The Challenge of Transferring Failure in a Digital, Globalized World," *ISACA Journal*, vol. 5. 2015., pp. 37-42.

[21] CHIKÁN, A., CZAKÓ, E., ZOLTAYNÉ PAPRIKA, Z., *Vállalati versenyképesség a globalizálódó magyar gazdaságban*. Budapest, Magyarország: Akadémiai Kiadó, 2002., ISBN 9630579227

[22] COGHLAN, D., BARNNICK, T., *Doing Action Research in Your Own Organization*. London: Sage, 2001.

[23] COUGHLAN, P., COUGHLAN, D., "ActionResearch for Operations Management," *International Journal of Operations & Production Management*, vol. 22, no. 2. February 2002., pp. 220-240. DOI:10.1108/01443570210417515

[24] DANEZIS, G. et al., *Privacy and Data Protection by Design*.: ENISA, 2014. https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/@@download/fullReport (Letöltés ideje: 2016.02.10.)

[25] DEY, M., "Information Security Management – A Practical Approach," in *Proceedings of AFRICON*, 2007., p. 6. DOI:10.1109/AFRCON.2007.4401528

[26] DÖRFLER, V., VELENCEI, J., „Tudásrendezés," *Gazdaság vállalkozás, vezetés: A szervezési és vezetési tudományos társaság lapja*, vol. 3. no. 4., 1999., pp. 64-73.

[27] DRAKE, T., „Measuring software quality: a case study," *Computer*, vol. 29. no. 11. 1996., pp. 78-87. DOI:10.1109/2.544241

[28] EISENHARDT, K. M., „Building Theories from Case Study research," *Academy of Management Reviewer*, vol. 14. no. 4. 1989., pp. 532-550.

[29] Ernst&Young. (2014) Get ahead of cybercrime ez' Global Information Security Survey 2014. http://www.ey.com/Publication/vwLUAssetezEY-global-information-security-survey-2014/$FezE/EY-global-information-security-survey-2014.pdf (Letöltés ideje: 2015.02.27.)

[30] Fedeeral Trade Comission, Children's Online Privacy Protection Act of 1998

[31] Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347

[32] GLASER, G. B., STRAUSS, L. A., *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine, 1967.

[33] GODÁNYI, G., "Katasztrófavédelem és üzletmenet-folytonosság az információtechnológiában (A DR/BC tervezés alapjai)," *Híradástechnika*, vol. LIX évf. 2004/4. 2004., pp. 47-52.

[34] GOOD, I. D., "Producing secure digital information systems," in *[Proceedings 1988] Fourth Aerospace Computer Security Application*, Orlando, 1998., pp. 180-222. DOI:10.1109/ACSAC.1988.113438

[35] GORDON, A. L., LOEB, P. M., "Budgeting Process for Information Security Expenditures," *Communications of the ACR*, vol. 49. no. 1., January 2006., pp. 121-125, DOI:10.1145/1107458.1107465

[36] Gramm-Leach-Bliley Act (GLBA) of 1999, Public Law 106-102

[37] HAIG, Z., *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó, 2018.

[38] HASHIM, K., AZIZI, N., "Enterprise Level IT Risk Management," in *Proceedings of the 8th WSEAS International Conference on APPLIED COMPUTER SCIENCE (ACS'08)*, Venice, 2008., ISBN 960-474-028-4., pp. 401-404.

[39] Health Insurance Portability and Accountability Act (HIPAA), of 1996, Public Law 104-191

[40] High level structure, identical core text, common terms and core definitions, in ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 5th ed. Geneva, Switzerland: ISO, 2014, pp. 126-136.

[41] HONFI, V., ILLÉSI, Z., "Mennyire vigyázunk az értékeinkre?," , vol. Logisztika-Informatika-Menedzsment Nemzetközi Konferencia 2019, Zalaegerszeg, 2019. ISBN 9786155607769

[42] HORVÁTH, D., MITEV, A., *Alternatív kvalitatív kutatási kézikönyv*. Budapest: Alinea Kiadó, 2015.

[43] HORVÁTH, K. G., *Közérthetően nemcsak az IT biztonságról.* Budapest, Magyarország: Kormányzati Informatikai Fejlesztési Ügynökség, 2013.

[44] HORVÁTH, Z., "TISAX, az autóipar új információbiztonsági követelményrendszere," *Magyar Minőség*, június 2020., ISSN 1789-5510., pp. 4-15.

[45] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 - 16 CFR Part 681.

[46] ISACA Budapest Chapter. (2011) Információbiztonsági helyzetkép 2011. https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2011.pdf (Letöltés ideje: 2015.06.20.)

[47] ISACA Budapest Chapter. (2012) Információbiztonsági helyzetkép 2012. https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2012.pdf (Letöltés ideje: 2015.06.20.)

[48] ISACA Budapest Chapter. (2015) Információbiztonsági helyzetkép 2015. https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2015.pdf (Letöltés ideje: 2016.01.25.)

[49] ISACA Budapest Chapter. (2017) Információbiztonsági helyzetkép 2017. https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2017.pdf (Letöltés ideje: 2018.03.16.)

[50] ISACA Budapest Chapter. (2019) Információbiztonsági helyzetkép 2019. https://higherlogicdownload.s3.amazonaws.com/ISACA/a33a1b3f-fd2b-4dc7-a080-308f6288e925/UploadedImages/Informaciobiztonsagi_helyzetkep/ISACA_Infobizt_helyzetkep_2019.pdf (Letöltés ideje: 2019.12.28.)

[51] ISACA, COBIT 4.1., 2007.

[52] ISACA, *COBIT 5 for Assurance*. Rolling Meadows: ISACA, 2013., ISBN 978-1604203394

[53] ISACA, *COBIT 5 for Information Security*. Rolling Meadows, IL: ISACA, 2012., ISBN 978-1604203394

[54] ISACA, *COBIT 5 for Risk*. Rolling Meadows, IL: ISACA, 2013., ISBN 978-1604204575

[55] ISACA, COBIT 5. Rolling Meadows, IL: ISACA, 2012.

[56] ISO 31000:2009 Risk management – Principles and guidelines

[57] ISO/20000-2:2012 Information technology - Service management - Part2: Guidance on the application of service management systems

[58] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[59] ISO/IEC 27001:2005, Information technology Security techniques - Information security management systems – Requirements

[60] ISO/IEC 27035-2 Information security incident management – Part 1: Principles of incident management

[61] IT Governance Institute, *Mapping of ITIL v3 with COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute, 2013., ISBN 978-1-60420-035-5

[62] JAKUS, A., TICK, A., "IT biztonsági kockázatok és kockázatkezelés," *Hadmérnök*, vol. 1, no. XII. évfolyam 1. 2017., pp. 182-202. http://hadmernok.hu/171_15_jakus.pdf (Letöltés ideje: 2017.10.15.)

[63] KOVÁCS, L., *A kibertér védelme*.: Dialóg Campus Kiadó, 2018.

[64] KUCSERA, C., "Megalapozott elmélet: Egy módszertan fejlődéstörténete," *Szociológiai Szemle*, vol. 3. 2008., pp. 92-18. https://szociologia.hu/dynamic/SzocSzemle_2008_3_092_108_KucsereCs.pdf (Letöltés ideje: 2018.07.20.)

[65] LEWIN, K., „Action Research and Minority Problems," *Journal of Social Issues*, vol. 2, no. 4., 1946., pp. 34-46. DOI:10.1111/j.1540-4560.1946.tb02295.x

[66] MICHELBERGER, P., *Információ-, folyamat- és vállalatbiztonság*. Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2018., ISBN 9789634490920

[67] MOLNÁR, D., „Empirikus kutatási módszerek a szervezetfejlesztésben," *Humán innovációs szemle*, vol. 1-2. 2010., pp. 61-72, http://humanexchange.hu/site/uploads/file/61-72_md.pdf (Letöltés ideje: 2018.8.12.)

[68] MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények

[69] MSZ ISO/20000-1:2013 Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei

[70] MUHA, L., "A magyar köztársaság kritikus információs infrastruktúrájának védelme," Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.

[71] MUHA, L., "Az informatikai biztonság egy lehetséges rendszertana," *Bolyai Szemle*, vol. 17. no. 4. 2004., pp. 137-156.

[72] MUHA, L., KRASZNAY, C., *Az elektronikus információs rendszerek biztonságának menedzselése*.: NKE, 2018., ISBN 978-615-5491-65-8

[73] MUHA, L., SZÁDECZKY, T., *Irányítási rendszerek*. Budapest, Magyarország: NKE, 2014., ISBN 9786155491511

[74] MUHA, L., TÓTH, G., "A bankbiztonság vizsgálata kockázatelemzéssel," *Hadmérnök*, vol. 6. no. 4., December 2011., pp. 204-215. http://www.hadmernok.hu/2011_4_muha_toth.pdf (Letöltés ideje: 2015.06.29.)

[75] NASSAR, A. A., "Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen," *International Journal of Scientific Research in Multidisciplinary Studies*, vol. 3. no. 11. December 2017., pp. 4-13. DOI:10.26438/ijsrms/v3i11.413

[76] NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations, 2nd ed. Gaithersburg, MD: NIST, 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Letöltés ideje: 2016.10.05.)

[77] NIST SP 800-61 Computer Security Incident Handling Guide, 2nd ed.: NIST, 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Letöltés ideje: 2017.11.10.)

[78] OGC, *ITIL Service Delivery*. London: TSO, 2000., ISBN 0 11 330017 4

[79] OGC, *ITIL Service Support*. London: OGC, 2000., ISBN 0 11 330015 8

[80] Payment Card Industry (PCI) Data Security Standard v3.1 Requirements and Security Assessment Procedures

[81] PORTER, E. M., *Versenystratégia*.: Akadémiai Kiadó, 2006. ISBN 9789630583497

[82] PwC. (2015) Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015. http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml# (Letöltés ideje: 2015.02.27.)

[83] REASON, P., BRADBURY, H., *Handbook of Action Research*.: Thousand Oaks, CA, 2001.

[84] REDMILL, F., "ALARP Explored," Computing Science, University of Newcastle upon Tyne, CS-TR-1197, 2010., http://www.scsc.org.uk/pubs/Alarp%20explored.pdf (Letöltés ideje: 2015.12.19.)

[85] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[86] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

[87] RODRIGUEZ, A., FERNANDEZ-MEDINA, E., PIATTINI, M., "A BPMN Extension for the Modeling of Security Requirements in Business Processes," *IEICE TRANSACTIONS on Information and Systems*, vol. E90-D. no. 4. pp. 745-752, 2007., DOI:10.1093/ietisy/e90-d.4.745

[88] ROECKLE, H., SCHIMPF, G., WEIDINGER, R., "Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization," in *RBAC '00 Proceedings of the fifth ACM workshop on Role-based access control*, New York, NY, 2000., pp. 103-110. DOI:10.1145/344287.344308

[89] Sarbanes-Oxley Act (SOX) of 2002, Public Law 107-204

[90] SHAMELI-SENDI, A., JABBARIFAR, M., DAGENAIS, M., SHAJARI, M., „System Health Monitoring Using a Novel Method: Security Unified Process," *Journal of Computer Networks and Communications*, vol. 2012. p. 20., DOI:10.1155/2012/151205

[91] SHARKASI, Y. O., "Addressing Cybersecurity Vulnerabilities," *ISACA Journal*, vol. 5, pp. 1-11, 2015., https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/addressing-cybersecurity-vulnerabilities (Letöltés ideje: 2015.10.39.)

[92] SHEIKHPOUR, R., MODIRI, N., "Mapping Approach of ITIL Service Management Processes to ISO/IEC 27001 Controls," *JOURNAL OF COMPUTING*, vol. 3. no. 7., 2011. ISSN 2151-9617

[93] SMIT, J., KREUTZER, S., MOELLER, C., CARLBERG, M., "Industry 4.0," Policy Department A: Economic and Scientific Policy, European Parliament Directorate General for Internal Policies, Brussels, 2016.

[94] Social Security Number Protection Act of 2011

[95] SZÁDECZKY, T., *Az IT biztonság szabályozása*.: GlobeEdit, 2018., ISBN 978-620-2-4864-1

[96] SZÁDECZKY, T., *Szabályozott biztonság*. Pécs: PTE ÁJK, 2011. https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/szadeczky-tamas/szadeczky-tamas-vedes-ertekezes.pdf (Letöltés ideje: 2015.03.10.)

[97] SZERB, L., ULBERT, J., „The Examination of the Competitiveness in the Hungarian SME Sector: A Firm Level Analysis," *Acta Polytechnica Hungarica*, vol. 6. no. 3. 2009., ISSN 1785-8860., pp. 105-123.

[98] The Open Group, *FAIR – ISO/IEC 27005 Cookbook*. Reding, UK: The Open Group, 2010., ISBN 1-931624-87-9

[99] The Standish Group, "Chaos Report, Project Smart, 2014," 2014., http://www.projectsmart.co.uk/docs/chaos-report.pdf (Letöltés ideje: 2015.03.02.)

[100] TURNER, H. et al., "Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks?," *Security & Privacy, IEEE*, vol. 13. no. 3. June 2015., pp. 40-47. DOI:10.1109/MSP.2015.60 (Letöltés ideje: 2017.01.10.)

[101] YIN, K. R., *Case study research*. Beverly Hills, California: Sage Publications, 1984.

[102] ZAINAL, Z., "Case study as a research method," *Jurnal Kemanusiaan*, vol. 9. 2007.

[103] ZHENG, X., HU, B., MAO, Y., "Applied analysis of a supply chain management model in the construction industry," in *E -Business and E -Government (ICEE)*, 2011., pp. 1-4. DOI:10.1109/ICEBEG.2011.5881465

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

[104] BEINSCHRÓTH, J., DOMBORA, S., "Az információbiztonság kérdése az agilis projektmenedzsmentben," in XXXII. Kandó konferencia : Kandó a tudomány hajóján, Budapest, 2016., ISBN 978-963-7158-07-0., pp. 1-8.

[105] BEINSCHRÓTH, J., DOMBORA, S., "Informatikai stratégia tervezés," in Óbudai Egyetem, vol. XXXIII. Kandó Konferencia 2017, Budapest, 2017., ISBN 978-963-7158-08-7.,pp. 39-51.

[106] DOMBORA, S., "ÁLLAMI SZERVEZETEK INFORMÁCIÓBIZTONSÁGÁNAK FEJLESZTÉSE," in MŰSZAKI TUDOMÁNY AZ ÉSZAK-KELET MAGYARORSZÁGI RÉGIÓBAN 2015, Debrecen, 2015., ISBN 9789637064326., pp. 207-212.

[107] DOMBORA, S., "Az informatikai szolgáltatások biztonsága," in Az informatikai biztonság kézikönyve : Informatikai biztonsági tanácsadó A-tól Z-ig, 36th ed., SZENES, K., Ed. Budapest, Magyarország: Verlag Dashöfer Szakkiadó Kft, 2010., ISBN 9639313122., pp. 6.10.1-6.10.64.

[108] DOMBORA, S., "Characteristics of Information Security Implementation Methods," in Management, Enterprise and Benchmarking in the 21st Century III., MICHELBERGER, P., Ed., 2016., ISBN 978-615-5460-77-7., pp. 57-72.

[109] DOMBORA, S., "Integrated Incident Management Model For Data Privacy And Information Security," in XIV. International May Conference on Strategic Management – IMCSM18 : Book of Proceedings, vol. 1. Bor, 2018., ISSN 2620-0597., pp. 319-328.

[110] DOMBORA, S., "Parameters and Guidelines of Enforceable Information Security Management Systems," INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS, vol. 17. no. 3-A. 2019., pp. 485-491. DOI:10.7906/indecs.17.3.7

[111] DOMBORA, S., "Szervezetek információbiztonságának elemzése és fejlesztése," in Tanulmánykötet a 6. Báthory-Brassai nemzetközi konferencia előadásaiból, RAJNAI, Z. et al., Eds. Budapest: Óbudai Egyetem, 2015, vol. 1., ISBN 978-615-5460-38-5., pp. 365-382.

[112] DOMBORA, S., "Valós idejű adatok az adatbázisban," IT BUSINESS: HETI HÁTTÉRMAGAZIN, BUSINESS, TECHNOLÓGIA, vol. 5. 2007., ISSN 1589-3464., pp. 34-34.

[113] DOMBORA, S., HORVÁTH, K. G., "Információbiztonság integrált megvalósítása MSZ ISO/IEC 27001:2014, és IBTV. (NIST SP 800-53 REV 4) alapon," in Kommunikáció 2015, 2015., ISBN 978-615-5527-55-5., pp. 43-56.

[114] DOMBORA, S., MICHELBERGER, P., " Factors causing information security gaps," *Webology*, vol. 19. no. 2. 2022., ISSN: 1735-188X., pp. 7106-7120.

[115] DOMBORA, S., MICHELBERGER, P., "Információbiztonság szerepe az üzleti folyamatokban," *International Journal of Engineering and Management Sciences*, vol. 1. no. 1. 2016., pp. 1-13., DOI:10.21791/IJEMS.2016.1.17

[116] MICHELBERGER, P., DOMBORA, S., "A felhasználói profil szerepe az információbiztonságban," PRO PUBLICO BONO: MAGYAR KÖZIGAZGATÁS; A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA, vol. 3. no. 4. 2015., ISSN 2063-9058., pp. 34-50.

[117] MICHELBERGER, P., DOMBORA, S., "A possible tool for development of information security - SIEM system," EKONOMIKA, vol. 62. no. 1. March 2016., pp. 125-140. DOI:10.5937/ekonomika1601125M

[118] MICHELBERGER, P., DOMBORA, S., "Competitiveness or Process Security," in XII International May Conference on Strategic Management (IMKSM 2016) and XII Students Symposium on Strategic Management, Belgrade, 2016., pp. 25-35.

8.2 További tudományos közlemények

[119] DOMBORA, S., "Adatbázisok megvalósítása (adatbázisok, adatbáziskezelők, adatbázisok felépítése, adatbázisok tervezése)," Oktatási segédlet az Informatikai projektellenőr képzéshez, 49 db dia, Magyarország, 2016.

[120] DOMBORA, S., "Bevezetés (informatika, informatikai függőség, informatikai projektek, mérnöki és informatikai feladatok találkozása, technológiák)," Oktatási segédlet az Informatikai projektellenőr képzéshez, 23 db dia, Magyarország, 2016.

[121] DOMBORA, S., "Informatikai rendszerek integrációja integrációs technológiák (xml, integráció a felhővel, intelligens rendszerek integrációja, elsődleges szolgáltatás és adatközpontok, az integráció biztonsága)," Oktatási segédlet az Informatikai projektellenőr képzéshez, 36 db dia, Magyarország, 2016.

[122] DOMBORA, S., "Informatikai rendszerek integrációja: Integrációs technológiák," Oktatási segédlet az Informatikai projektellenőr képzéshez, 31 db dia, Magyarország, 2016.

[123] DOMBORA, S., "Legacy rendszerek, adatok, törzsadat menedzsment," Oktatási segédlet az Informatikai projektellenőr képzéshez, 34 db dia, Magyarország, 2016.