ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

KEMENDI ÁGNES

A vállalati biztonsági háló meghatározó tényezői

Témavezető: Prof. Dr. Michelberger Pál egyetemi tanár

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024.04.22.

Tartalomjegyzék

1 Summary 3

2 A kutatás előzményei 4

3 Célkitűzések 6

4 Vizsgálati módszerek 6

5 Új tudományos eredmények 9

6 Az eredmények hasznosítási lehetősége 14

7 Irodalomjegyzék 16

8 Publikációk 25

8.1 A tézispontokhoz kapcsolódó tudományos közlemények 25

8.2 További tudományos közlemények 26

1 Summary

In my doctoral thesis, I approach the issue of corporate security holistically and examine the determining factors of security, including its information and communication technology and human aspects. During the examination of the determining factors of corporate security, I use a network science approach to reveal the connections between the determining factors of corporate security. My research was conducted on companies and can be interpreted regardless of company size (for large, small and medium-sized enterprises), however, regarding its practical application, the individual context needs to be considered. The subject matter needs to be addressed due to the emerging impact of changes in the business and risk environment, such as the new industrial revolutions of industry 4.0 and 5.0, the digital transformations, the new risks posed in relation to cybersecurity, the challenges of human factor or the readiness related to COVID-19 pandemic.

The main objective of my doctoral thesis was to present the corporate safety-net concept, i.e., the control system that covers the company and ensure corporate security in a comprehensive manner. In my research I aimed to identify the determining factors of the corporate safety-net, to analyse the linkage amongst the elements of the corporate safety-net, to offer a solution for process security measurement in the context of standard management systems and to analyse the role of standard management systems in process security.

The results of the scientific reach are the following:

1. I verified the network-like nature of the internal controls in corporations. The internal control system can be interpreted as a network. A network-like relationship can be identified between the key factors of corporate security.
2. I identified the defining elements of the corporate safety-net. The key finding of the research is that the key element of the corporate safety-net is top management commitment that is the most important factor determining a company's safety culture and corporate security.
3. I developed a new Balanced Scorecard model, the Safety Balanced Scorecard, which covers the safety pillars in the context of standard management systems and serves as a framework for measuring process safety.
4. I proved that the use of information management systems is suitable for increasing the process security and the company's security level. The certification of management systems provides assurance about the level of process safety.

2 A kutatás előzményei

A doktori értekezésemben a vállalati biztonság tématerületét a vállalati belső kontrollrendszer aspektusából holisztikusan közelítem meg, és vizsgálom a biztonság meghatározó tényezőit, annak információs-és kommunikációs technológiai és humán aspektusait egyaránt. A vállalati biztonság szempontjából meghatározó tényezők vizsgálata során hálózattudományi megközelítés segítségével tártam fel a vállalati biztonság meghatározó tényezői közötti összefüggéseket. A kutatásomat vállalatokra vonatkozóan végeztem. A kutatásom vállalatmérettől függetlenül értelmezhető nagyvállalatokra, valamint kis- és középvállalatokra egyaránt, gyakorlati alkalmazására vonatkozóan azonban egyéni kontextusba helyezés és mérlegelés szükséges. A kutatásommal kapcsolatban érintett terület a mesterséges intelligencia szerepe és hatásai, mellyel jelen kutatásban nem foglalkozom részletesen a tématerületen tapasztalható dinamikus, evolúciós fejlődés miatt. A kutatásomnak nem célja a kapcsolódó keretrendszerek, szabványok, és jogszabályok lefedése.

A folyamatosan változó üzleti és kockázati környezetben szükséges, hogy a vállalatok a biztonságos vállalati működés érdekében felkészültek legyenek az információs és kommunikációs technológiához (továbbiakban: IKT), és az emberi tényezőhöz köthető kockázatok kezelésére, az előre nem látható természeti események vagy pandémia hatásainak kezelésére.

A ma vállalatában az IKT-hoz kapcsolódó kockázatok kezelése kurrens témát jelent. Mindemellett, a humán kockázatok jelen vannak a vállalati folyamatokban és rendszerekben, ezért a vállalatbiztonság szempontjából a humán kockázatok kezelése szintén meghatározó. A vállalati működés során definiálni kell a szükséges biztonsági folyamatokat a biztonságos működés érdekében. Az integrált kockázatkezelés a vállalati stratégiából származtatva történik, és a vállalat valamennyi folyamatára kiterjed [1].

A vállalati folyamatok kontrollált végrehajtása a biztosíték arra, hogy a folyamatok megfelelően lezajlanak és elérik céljukat. A kontrolling szabályzókör, a PDCA ciklus néven ismert tervezés, megvalósítás, ellenőrzés és korrigálás a folyamatok kontrollált végrehajtását segíti. A PDCA ciklus logikája meghatározó a kontrolling funkcióban, a belső kontroll folyamatokban, a folyamatok teljesítménymérése (pl.: a kiegyensúlyozott mutatószámrendszer alkalmazása) során, és a szabványos irányítási rendszerek szempontjából egyaránt.

A szabványos irányítási rendszerek a vállalati célkitűzések megvalósulását segítik. Az irányítási rendszerek működtetése javítja a vállalati folyamatok működését és megbízhatóságát, ezáltal szerepük van a vállalati biztonság szempontjából is.

A hálózatok fogalmát adaptáltam a vállalati biztonsági folyamamtokra. A biztonsági folyamatok a vállalati stratégiához kapcsoltan és az operatív folyamatok szintjére beépülve a vállalati belső kontrollok rendszerét, a vállalati biztonság hálózatát írják le. A biztonsági folyamatok működéséről a biztonsági folyamatok teljesítényének mérése tud helyzetjelentést adni.

A kutatásomhoz kapcsolódó főbb fogalmak ismertetése

Vállalatbiztonság: vállalatbiztonság állapotában a vállalat hosszú távon képes stratégiai terveivel összhangban működőképességét, és jövedelemtermelő képességét biztosítani, és azt nem várt események esetében eredményesen és hatékonyan helyreállítani [2].

Folyamatbiztonság: folyamatbiztonság állapotában a vállalati folyamatok (bemenet-folyamat-kimenet) zavartalanul működnek, és váratlan esemény (például vis major) esetén eredményesen és hatékonyan helyre tudnak állni [3].

Biztonsági folyamatok: A kívánt biztonsági szint megteremtése érdekében alkalmazott folyamatokat biztonsági folyamatoknak, másnéven kontroll folyamatoknak nevezem. Kontrollok alatt azokat a tevékenységeket értem, melyek biztosítják, hogy a folyamat hibamentesen, illetve adott elfogadható tűréshatáron belüli hibaszázalékkal megy végbe [S8].

Incidens: nem várt negatív biztonsági esemény, mely a normál üzletmenetre kedvezőtlen hatással van.

Kontroll funkció: A kontroll funkció több szinten jelenik meg a vállalati működés során: a teljes vállalatra érvényes, valamennyi munkavállalóra kiterjedő elvek formájában, valamint a működési folyamatokba épített ellenőrzés, kontroll tevékenységek formájában. Egyes vállalati funkciók kontroll funkciót is ellátnak, és egyes funkciók kifejezetten kontroll funkciót töltenek.

Információbiztonság: információbiztonság állapotában megvalósul az információ bizalmas kezelése, sértetlensége és rendelkezésre állása [173].

Digitális átalakulás / transzformáció: digitális átalakulás alatt a digitális technológia üzleti folyamatokba történő integrálását értem.

Biztonsági háló – a kontrollok biztonsági hálózata: A vállalatot behálózó kontrollrendszert kontrollok biztonsági hálózatának, röviden *biztonsági hálónak* nevezem. A fogalmat az [S8] publikációmban definiáltam.

3 Célkitűzések

Kutatásom során a vállalati biztonságot meghatározó tényezőket vizsgálom.

Célkitűzéseim:

1. A vállalati belső kontrollrendszert alkotó biztonsági kontrollok közötti kapcsolat elemző vizsgálata
2. A vállalati biztonsági háló meghatározó tényezőinek azonosítása
3. Vállalati biztonsági kiegyensúlyozott mutatószámrendszer kidolgozása
4. Szabványos irányítási rendszerek szerepének vizsgálata a biztonsági szint növelésében

A kutatási téma kidolgozásához a következő hipotéziseket állítottam fel:

Az I. hipotézis (a továbbiakban: H1) szerint feltételezem, hogy a belső kontrollrendszer hálózatként értelmezhető. A hálózattudomány segítségével a belső kontroll folyamatok vállalatot behálózó jellege igazolható.

A II. hipotézis (a továbbiakban: H2) szerint feltételezem, hogy a belső kontrollhálózat működése szempontjából azonosítható olyan tényező, amely a hálózat működését biztonsági szempontból döntően meghatározza.

A III. hipotézis (a továbbiakban: H3) szerint feltételezem, hogy a szabványos irányítási rendszerekhez kötve biztonsági területek definiálhatók. A kiegyensúlyozott mutatószámrendszer alkalmazható az egyes biztonsági területekre vonatkozó teljesítménymérési rendszer felállítására.

A IV. hipotézis (a továbbiakban: H4) szerint feltételezem, hogy az információbiztonsági irányítási rendszerek alkalmazhatók a folyamatbiztonság és a vállalati biztonsági szint növelésére. Az irányítási rendszerek tanúsítása biztosítékul szolgálhat a folyamatbiztonságról.

4 Vizsgálati módszerek

Szakirodalmi kutatás és szekunder elemzés

A kutatásom során több tudományterületet érintő, transzdiszciplináris megközelítést alkalmaztam [4]. A disszertációmhoz kapcsolódó kutatási terület feltárását szakirodalmi kutatással, és szekunder adatok elemzésével kezdtem meg a hipotézisek vizsgálatához (H1, H2, H3, H4) kapcsolódóan.

A szekunder kutatási eredményekhez kapcsolódóan bemutatom a globális kockázati környezetben tapasztalható tendenciákat, melyek tanácsadó cégek globális vállalati kockázatkezelésre irányuló felmérései alapján kerültek meghatározásra [5; 6; 7; 8; 9]. Ismertetem az Európai Unió tagállamaira vonatkozóan elvégzett, a vállalatok IKT biztonságát feldolgozó kutatás eredményeit, és a vállalatok szervezeti-, és kompetencia kihívásait az ipar 4.0 és 5.0-hoz kapcsolódóan. Bemutatom a szabványos irányítási rendszerek tanúsítási adatai alapján készített elemzésem eredményeit.

A primer kutatásom során a tématerülethez illeszkedő kvalitatív kutatási módszertant alkalmaztam, melyet az egyes hipotézisekhez kapcsolódóan részletesen ismertetek. Fontos kritérium a kinyert adatok érvényessége és megbízhatósága a tématerülethez kapcsolódó problémakör lefedésénél. A szenzitív témakör, az adatok nem számszerű, hanem minőségre vonatkozó jellege, a tématerület minél mélyebb, alaposabb, leíró megismerése, a kérdéskör egyedisége, komplexitása, és a gyakorlatiasság kritériumának szem előtt tartása indokolja a kvalitatív kutatási módszer választását [10; 11; 12; 13].

A belső kontrollrendszer tartalomelemzése

Kvalitatív kutatást végeztem a vállalatbiztonságot meghatározó kontrollok hálózati jellegének vizsgálatára a H1 hipotézishez kapcsolódóan. A kvalitatív adatok elemzésére választott módszer a tartalomelemzés. A tartalomelemzés szisztematikus módszer az adatok elemzésére [10; 23]. Az elemzés a témára és a kontextusra fókuszál, és hangsúlyozza a variációt, mint a hasonlóságokat és különbségeket a szövegrészek között, lehetőséget biztosít nemcsak az egyértelmű, leíró tartalom, hanem a látens, értelmező tartalom elemzésére is [24]. A vizsgált minta a Magyarországon jelen lévő autóipari vállalatok, ahol a biztonság kérdésköre stratégiai célkitűzésként jelenik meg. A kutatási kérdések vezérfonala mentén a vizsgált vállalatok kontrollrendszerét, és kontrollfolyamatainak hálózatát a vállalatok éves beszámolói alapján „külső szemlélőként” vizsgáltam.

Folyamat kontrollhálózatának modellezése

A H1 hipotézishez kapcsolódóan a vállalati belső kontrollrendszer kontextusában modelleztem egy folyamat kontrollhálózatát, a folyamathoz rendelt kontrollok rendszerét, és vizsgáltam az emberi tényező vállalati biztonságban betöltött szerepét. „Hálózatok mindenhol vannak” [25]. A hálózatok absztrakt dolgokat is leírhatnak, mint például egy személy és egy feladat kapcsolata [26]. A bevételszerzési folyamat kontrollhálózatát modelleztem a folyamathoz rendelt kontrollok, a kapcsolódó emberi tényező, valamint az emberi kockázatok vonatkozásában.

Szakértői kutatás

Kvalitatív kutatást végeztem a vállalati biztonságot meghatározó tényezőkről. A biztonsági háló meghatározó tényezőit szakértői kutatás keretében vizsgáltam, és a megalapozott elmélet módszertana alapján elemeztem. A tématerületen kiemelkedően jártas, nagy értékű tapasztalattal, szakmai referenciával és releváns képzettséggel rendelkező személyeket kértem fel interjúalanyként. A szakértői kutatás a H1, H2 és H4 hipotézisek igazolásához kapcsolódik. A grounded theory (GT), azaz megalapozott elmélet módszertant alkalmaztam, melynek során az interjúkból kinyert adatokból az adatelemzés eredményeként alakul ki az új elmélet, a megalapozott elmélet [12; 14; 15; 16; 17]. A grounded theory eredeti módszertanát Glaser és Strauss fejlesztette ki. A megalapozott elmélet fő komponensei az adatgyűjtés, a kódolás, az elemzés, a memó készítés és az elméleti kategorizáció [18]. A strukturált interjúk alapjául szolgáló kérdéssor, az interjú vezérfonala inherens jelleggel tartalmazza a kutatási témával kapcsolatos a priori ismereteimet, ezért a Glaser féle megközelítés adaptálását elvetettem. A grounded theory Charmaz féle konstuktivista megközelítését alkalmaztam [15; 19].

Kiegyensúlyozott mutatószámrendszer alapú vállalatbiztonsági modell

A H3 hipotézishez kapcsolódóan a kiegyensúlyozott mutatószámrendszer (BSC – Balanced Scorecard) megközelítést szakirodalmi elaboráció alapján kutattam, és a standard irányítási rendszerek alapján fejlesztettem tovább. A modell-alkotási folyamatot a szabványos irányítási rendszerek alapos kutatása kísérte. Az új BSC különböző biztonsági szempontokat (kontrolling területeket) fed le, amelyek a szabványos irányítási rendszerekhez kapcsolódnak. A modell felhasználja a kiegyensúlyozott mutatószámrendszer négy alappillérét (pénzügyi, vevők, belső folyamatok/működés, innováció és tanulás nézőpontja), és a vállalati irányítási rendszerekhez kapcsolódó irányítási rendszerszabványokra, a Nemzetközi Szabványügyi Szervezet irányítási rendszerekre vonatkozó szabványaira épül. Az alapul szolgáló BSC négy aspektusa összefüggő rendszert képez, és átláthatóvá teszi az egyes aspektusok elemei közötti ok-okozati kapcsolatokat. Az irányítási rendszerszabványok lényege a folyamatok egységesítése, ezek felhasználása a modell egyetemleges alkalmazhatóságát segíti elő.

Szabványos irányítási rendszerek biztonsági jellemzői

A H4 hipotézishez kapcsolódóan a szabványos irányítási rendszerek és a folyamatbiztonsági szint közötti kapcsolat megállapítására a megalapozott elmélet (grounded theory) módszert alkalmaztam, mellyel a szakértői kutatásom eredményeit dolgoztam fel. A szabványos irányítási rendszerek biztonsági szerepét megközelítettem szakirodalmi feldolgozás és tartalomelemzés segítségével is.

5 Új tudományos eredmények

Az értekezés elején megfogalmazott hipotézisek elfogadása vagy elutasítása:

I. hipotézis: („A belső kontrollrendszer hálózatként értelmezhető. A hálózattudomány segítségével a belső kontroll folyamatok vállalatot behálózó jellege igazolható.") **igazolást nyert,** mert bizonyítottam, hogy a belső kontrollrendszer egy komplex rendszer és hálózatként viselkedik. A belső kontrollrendszer működésében a hálózatszerű összefüggések értelmezhetők és meghatározók.

II. hipotézis: („A belső kontrollhálózat működése szempontjából azonosítható olyan tényező, amely a hálózat működését biztonsági szempontból döntően meghatározza.") **igazolást nyert,** mert a kutatási eredményeim igazolják, hogy az elkötelezett vezető szerepe kulcs csomópont a vállalati biztonsági háló működése szempontjából. A vezetői elkötelezettség áll a vállalati biztonsági háló működését meghatározó tényezők működése mögött. A biztonsági háló további meghatározó tényezői is a vezetőtől eredeztethetők.

III. hipotézis: („A szabványos irányítási rendszerekhez kötve biztonsági területek definiálhatók. A kiegyensúlyozott mutatószámrendszer alkalmazható az egyes biztonsági területekre vonatkozó teljesítménymérési rendszer felállítására.") **igazolást nyert,** mert az új biztonsági fókuszú kiegyensúlyozott mutatószámrendszer kontrolling területei, azaz a modell biztonsági csoportjai a szabványos irányítási rendszerekhez kapcsoltan kerültek meghatározásra és átfogó megközelítést jelent a biztonsági folyamatok teljesítménymérésére.

IV. hipotézis: („Az információbiztonsági irányítási rendszerek alkalmazhatók a folyamatbiztonság és vállalati biztonsági szint növelésére. Az irányítási rendszerek tanúsítása biztosítékul szolgálhat a folyamatbiztonságról.") **igazolást nyert,** mert az információ szerves része a vállalati folyamatoknak, melynek biztonsága a digitális korban tapasztalható jelentős kockázati kitettség következtében kulcs kockázati területté vált mind a folyamatbiztonság, mind a vállalatbiztonság szempontjából. Az információbiztonsági irányítási rendszerszabványban megfogalmazott átfogó követelményrendszer megvalósítása révén elérhető a folyamatbiztonság, és az azt átfogó vállalatbiztonság szintének növelése, melyről a tanúsítás bizonyosságot is nyújt.

Az értekezésem tárgyát képező kutatómunkám új tudományos eredményeit az alábbi tézisekben mutatom be:

Tézis 1: Igazoltam a kontrollok vállalatot behálózó jellegét. A belső kontrollrendszer hálózatként értelmezhető.

A hálózatok, valamint a hálózatszerű működés adaptálható vállalati biztonsági kontextusban, megalkotva a biztonság hálózatát. A biztonság hálózatát a vállalatot behálózó kontrollrendszer, jelenti, mely a kockázatkezelési tevékenység eredménye. A folyamatokhoz rendelt kontrollok hálózata a belső kontrollrendszer megvalósulása a vállalati folyamatokban. A belső kontrollhálózat a biztonsági kultúra leírása kontroll aspektusból. A vállalat kontrollrendszerét meghatározó kontrolloknak a vállalati működés minden szintjén jelen kell lenniük. A hosszú távú sikeres vállalati működés érdekében a vállalati stratégia, a kockázatkezelés és a vállalati folyamatok integrált kezelése szükséges. A biztonság hálózatának fogalma jól illusztrálja a vállalati biztonsági rendszer összetettségét, és a biztonsági háló elemei közötti összefüggő, és kölcsönös kapcsolatban álló relációt.

A biztonság hálózatának megteremtéséhez kontrollok szükségesek. A belső kontrollrendszer hálózatszerűen működik, hálózatszerűen összekapcsolódó és egymást erősítő elemekből áll. A belső kontrollrendszer erősíti a vállalatbiztonságot, ezáltal értéket állít elő. A belső kontrollrendszer integráló jellegű, kapcsolódik a vállalati stratégiához, a vállalati működés valamennyi szintjén megjelenik, része a vállalati folyamatoknak és az üzleti célok érdekében szükséges.

A vállalati biztonsági háló „kemény” és „lágy” elemeinek együttesen kell, hogy biztosítsák a folyamatok biztonságát és a hosszú távú sikeres vállalati működést. A biztonsági háló kemény elemeinek tekinthetők a technológiák, rendszerek, folyamatok, szabályzatok és eljárások. A biztonsági háló lágy elemei az emberi tényezőhöz köthetők.

A kontrollhálózatot meg kell tervezni, működtetni, és szükség szerint átértékelni, újra kell definiálni. A digitális átalakulás átalakítja a vállalati folyamatokat, és annak hatását a vállalat kontrollhálózatára kezelni kell. A vállalati folyamatok változása esetén a kontrollok újraértékelésére és aktualizálására van szükség. A belső kontrollhálózatot egy élő rendszernek kell kezelni, a mindennapi működés részeként működtetni kell és biztosítani kell, hogy változások esetén a kontrollhálózat szükség szerint adaptálásra kerüljön, reziliens legyen, és fenn tudja tartani a kívánt biztonsági szintet.

A hálózati jellemzők rávilágítanak a kontrollhálózat erős és gyenge pontjaira egyaránt, mely a hálózat hibatűrő képességéből és sebezhetőségéből származtatható. Marginális incidens, hiba felmerülése esetén a hálózat működőképes marad. Amennyiben a kontrollhálózatot meghatározó kulcstényező kiesik, az az egész rendszer működésére hatással van. A vezetői elkötelezettség döntő jelentőségű a biztonsági háló működése szempontjából. Az információbiztonság a hálózat sebezhetőségéből kifolyólag szintúgy. Az információbiztonság megvalósítása éppúgy az elkötelezett vezető támogatásának a függvénye.

Kapcsolódó publikációim: [S6] [S8] [S10] [S11]

Tézis 2: Azonosítottam a vállalati biztonsági háló meghatározó tényezőit. A belső kontrollhálózat működése szempontjából létezik olyan tényező, amely a biztonsági hálózat működését döntően meghatározza.

A kutatási eredményeim igazolják, hogy a vezetői elkötelezettség a vállalati biztonsági háló kulcseleme és annak működését döntően meghatározza. A vezetői elkötelezettség szerepe és megnyilvánulásai a biztonsági kultúra fejlesztésében, illetve előmozdításában fundamentálisak, ide tartozik int. al. a biztonsági kérdésekkel kapcsolatos döntéshozatal, büdzsé allokálása, a folyamatos fejlesztésekben és kockázatmenedzsmentben betöltött szerep, a biztonságtudatosság intézményesítése, digitális kompetenciák, készségek, digitális érettség, és kontrollkörnyezet erősítése. A vállalatvezető szerepmodell is. A kialakított *biztonsági kultúra* jellemzi a vállalatot, illetve a vállalatbiztonságot. Ha a vállalati kultúra része a biztonságos működésre való odafigyelés, a biztonság „mindenki” felelőssége, és a vezetőktől kezdve a munkavállalókig mindenki elkötelezett, akkor az az üzleti folyamatokban is megjelenik. A biztonság értéket jelent a vállalatok számára.

A digitális kor magával hozta a digitális átalakulás jelenségét, mely a biztonsági háló tartópilléreit, az információs és kommunikációs technológiákat, a rendszereket és embereket mozgatja, és átalakítja a folyamatokat. Az információbiztonság kezelése a vállalati biztonsági háló szempontjából központi kérdéssé vált. A digitális átalakulás sikeres végrehajtása az emberi tényező központi szerepére is rávilágít: a biztonsági háló működése szempontjából kritikus a humán kockázatok kezelése, melynek részeként a szükséges digitális kompetenciák és készségek rendelkezésre kell, hogy álljanak. A digitális átalakulás a kompetenciák és készségek átgondolt fejlesztését teszi szükségessé, mely biztonsági célokat is szolgál.

A digitális átalakulási folyamatok kapcsán kritikus tényező a biztonsági szempont. A biztonsági szempontnak már projektindításkor a folyamat részének kell lennie.

A digitális kor újonnan megjelenő biztonsági fenyegetéseinek való adaptív ellenállás gyors válaszkészséget, reakciót kíván a vállalatoktól, mely jellemzően erőforrás függvénye is. A biztonsági háló működését mutatja a változásokra adott adekvát válasz és a kontrollhálózat naprakészsége.

A biztonsági kontrollok vállalati folyamatokat, például HR, pénzügy, jog, IT folyamatokat lefedő hálózatára, kontrollok rendszerére van szükség, mely együttesen tudja megvalósítani a biztonsági törekvéseket. A vállalati biztonság fenntartása érdekében a *folyamatok szerves része*ként kell kezelni a folyamatok biztonságos működéséhez kapcsolódó kontrollokat. Az üzleti folyamatok biztonságos működése a kapcsolódó kockázatok megfelelő kezelését követeli meg, melyhez biztonsági folyamatok, kontrollok, biztonságos eszközök, szoftverek és biztonságtudatos emberek, az emberi tényezőben rejlő kockázatok kezelése szükségesek. A biztonságos működés a biztonsági kultúra részeként valósul meg az üzletmenet-folytonosság érdekében. A kontrollált folyamatok működtetéséhez alkalmas eszközök a szabványos irányítási rendszerek. Az irányítási rendszerek kontrolling szabályozóköre a folyamatos fejlesztések révén erősíti a biztonsági háló robusztusságát és adaptív ellenálló képességét.

Kapcsolódó publikációim: [S1] [S2] [S3] [S4] [S5] [S6] [S7] [S8] [S9] [S10] [S11]

Tézis 3: Kidolgoztam egy új kiegyensúlyozott mutatószámrendszer (BSC – Balanced Scorecard) modellt, a Biztonsági Balanced Scorecard-ot, amely vállalati biztonsági pilléreket fed le a szabványos irányítási rendszerekkel összefüggésben, és keretként szolgál a folyamatbiztonság teljesítményének mérésére.

A Biztonsági Balanced Scorecard a vállalat biztonsági hálóját lefedő biztonsági elemeket tartalmazó és a biztonsági folyamatok teljesítménymérésére alkalmas modellt definiál.

A teljesítménymérés biztonsági folyamatok esetében is fontos, segít láthatóvá tenni a biztonsági folyamatokat és alapul szolgál a biztonsági folyamatok működésével kapcsolatos vezetői döntéshozatalnak. A jól meghatározott teljesítménymutatók a stratégiai célkitűzésekből származnak. A biztonsági folyamatok teljesítménymutatói biztonsági csoportonként is értelmezhetők. A biztonsági csoportok felállíthatók a szabványos irányítási rendszerek analógiáját és logikai struktúráját követve. Az új BSC modell a stratégiai célkitűzésekből származóan adott irányítási rendszerhez kapcsolódóan jeleníti meg a főbb biztonsági teljesítmény célokat, és az azok megvalósulásáról képet adó teljesítménymutatókat.

A szabványos irányítási rendszerekhez kapcsolódó Biztonsági kiegyensúlyozott mutatószámrendszer új megközelítésként alkalmazható a biztonsági folyamatok teljesítményének mérésére.

A Biztonsági kiegyensúlyozott mutatószámrendszer megközelítés használható a folyamatbiztonság-mérés keretrendszerének létrehozására a szabványos irányítási rendszerek kontextusában. Ebben az új keretrendszerben az egyes biztonsági csoportok különböző vállalati stratégiai célkitűzéseket céloznak meg, és összekapcsolják a megfelelő ISO-szabvány(oka)t az adott biztonsági csoporttal, amely átfogó megközelítést jelent a biztonsági folyamatok teljesítményének mérésére. A Biztonsági BSC jógyakorlatot mutat be biztonsági célkitűzésekre és teljesítménymutatókra. A Biztonsági BSC visszaadja a hálózati működési modellt. Bár a teljesítménymutatóknak a vállalat egyedi céljaihoz kell igazodniuk, az azonosított teljesítménymutatók sok esetben általánosan használhatók. A modell alkalmazása képet ad a vállalati biztonsági kontrollok működéséről és segít demonstrálni a biztonsági folyamatok értékét.

Kapcsolódó publikációim: [S12]

Tézis 4: Bizonyítottam, hogy egy jól működő információbiztonsági irányítási rendszer alkalmas a folyamatbiztonság és a vállalati biztonság szintjének növelésére. A tanúsított irányítási rendszerek bizonyosságot jelentenek a folyamatbiztonság vonatkozásában.

Szakirodalmi feldolgozás, tartalomelemzés és szakértői kutatás segítségével bizonyítottam az információbiztonsági irányítási rendszerek szerepét a folyamatbiztonság és az azt átfogó vállalatbiztonság szintjének növelésében. Az információbiztonság központi szereppel bír vállalatbiztonság szempontjából. Egy jól működő információbiztonsági irányítási rendszer alkalmas a folyamatbiztonság növelésére, mely egyúttal erősíti a biztonsági kultúrát, és a vállalatbiztonságot is.

A szabványos irányítási rendszerek alkalmazása segíti a vállalatokat célkitűzéseik elérésében. A vállalati folyamatok akkor működnek jól, ha teljesülnek a mögöttes biztonsági célok. Az irányítási rendszerek működése folyamatorientált megközelítésű. Az irányítási rendszerszabványok céljai biztonságorientáltak. A szabványok a folyamatos fejlesztési szemléletmódhoz kapcsolódnak. Nagy hangsúly kerül bennük a fejlesztésre és a képzésre. Ezek a tényezők meghatározók a folyamatteljesítmény, a folyamatbiztonság, és az azt felölelő vállalatbiztonság szempontjából. Az irányítási rendszerek a folyamatos fejlesztések révén erősíti a biztonsági háló robusztusságát és adaptív ellenálló képességét.

A folyamatokhoz szervesen kapcsolódik az információ. A folyamatok biztonságához szükséges az információ biztonsága. Az információbiztonsági irányítási rendszer a folyamatok részeként valósul meg. A folyamatbiztonság nem statikus, hanem a folyamatosan működő kontrollhálózat eredménye. A digitális kor kihívásainak való megfeleléshez jól működő információbiztonsági irányítási rendszerre van szükség.

A tanúsított irányítási rendszereket független testület tanúsítja szabványos, formális és elismert folyamaton keresztül, ami tovább növeli az adott irányítási rendszerek megbízhatóságát. Az irányítási rendszer független tanúsító szervezet általi tanúsítása komoly követelményeket támaszt. Ha ezek a követelmények teljesülnek, a vállalat képes demonstrálni az irányítási rendszer teljesítményét, ami biztosítékot nyújt a folyamatbiztonságról. Az irányítási rendszerek tanúsítása bizonyítékul szolgál az irányítási rendszerek megfelelő működéséről, mely az üzleti kapcsolatokhoz is szükséges lehet.

Kapcsolódó publikációim: [S11] [S12]

6 Az eredmények hasznosítási lehetősége

A kutatás a vállalati biztonsági rendszert hálózati kontextusba helyezi, mely a vállalati biztonsági rendszert horizontális és vertikális irányban is átfogja, rávilágít a vállalati alrendszerek közötti kapcsolatokra. A kontrollok hálózati kontextusban történő kezelése és az integrált kockázatkezelés szemlélete a vállalati biztonságot egy olyan dinamikus kontextusba helyezi, melyek lehetővé teszi az ok-okozati összefüggések feltárását, és elősegíti a kontrollkörnyezetre ható belső és külső tényezők reziliens kezelését. A reziliencia, az adaptív ellenálló képesség, a biztonsági rendszer „megbirkózási” képessége az ipar 4.0, illetve 5.0 korszakában olyan kulcstényező, mely a hosszú távú sikeres vállalati működés alapja. A folyamatokhoz rendelt kontrollok hálózata tulajdonképpen a belső kontrollrendszer megvalósulása a vállalati folyamatokban. A kontrollok hálózata a vállalati kockázati tűréshatárral összhangban segíti a kockázatok kezelését, és a kívánt biztonsági szint elérését. A szemléletmód a hosszú távú sikeres vállalati működés szempontjából meghatározó jelentőséggel bír, annak alkalmazását felsővezetői szinten javasolt kiemelt prioritásként kezelni, és stratégiai szintről eredeztetve a mindennapi működésbe tudatosan beépíteni a biztonságtudatosság, a biztonsági kultúra, és a vállalati biztonság érdekében. A kutatás rávilágít a vezetői elkötelezettség vállalati biztonságban betöltött meghatározó szerepére.

A teljesítménymérés fontos a vállalati biztonsági funkció esetében is. A biztonsági folyamatok teljesítménymérése hozzájárul ahhoz, hogy a biztonsági folyamatok hozzáadott értéke meg tudjon mutatkozni a vállalaton belül. A szabványos irányítási rendszerek alkalmazása segíti a vállalatokat célkitűzéseik elérésében és a biztonsági szintjük növelésében. A szabványos irányítási rendszerekkel összhangban kezelt Biztonsági Balanced Scorecard a biztonsági elemekre vonatkozóan segíti a vezetői döntéshozatalt, támogatja a transzparenciát, a folyamatos ellenőrzést, és elősegíti a folyamatos fejlesztést. A modell valamennyi vállalatra mérettől és üzleti profiltól függetlenül alkalmazható, és a vállalati igények szerint testre szabható. A teljesítménymérést érdemes a tervezés-végrehajtás-ellenőrzés, és beavatkozás ciklussal ötvözve alkalmazni. A biztonsági folyamatok teljesítményének mérése a biztonsági folyamatok működéséről szolgáltat kulcsinformációkat a vezetőségnek, és felhasználható a fejlesztendő területek meghatározására.

A kutatásom a teoretikus absztrakción túlmenően alkalmas a vállalati biztonság gyakorlati megközelítésére; bemutatja, és jógyakorlatul szolgál az üzleti élet szereplőinek a biztonsági kérdésekkel kapcsolatos döntéshozatalhoz, illetve rámutat a biztonsági kérdések átfogó, és sokszor kevéssé nyilvánvaló szerepére a vállalati életben.

A kutatás eredményei igazolják a folyamatokban részt vevő emberi tényező kritikus szerepét a biztonságos működésben a technikai, technológiai megoldások, például IKT eszközök, szoftverek biztonságos üzemeltetése mellett. A kutatás rávilágít arra, hogy a biztonságra, és a biztonságtudatosságra fordított erőforrások (munkaidő, tréning költség stb.) elengedhetetlenek. A megfogalmazott eredmények alkalmazását a vállalat-, és információbiztonság érdekében javaslom. A vállalati biztonság szempontjából érdemes a hálózatszerű összefüggésekben / kapcsolatokban / kölcsönhatásokban rejlő szinergiákban gondolkodni, és azt a vállalatbiztonság erősítésére felhasználni.

Mindazonáltal, a kutatásom által lefedett tématerület további kutatások kiindulópontja lehet. A vizsgált területekre vonatkozóan további kutatási kérdések fogalmazhatók meg. A vállalati biztonság szempontjából a fenntartható vállalati működés biztosítása is fontos szempont. Az értekezésben érintőlegesen foglalkoztam a vállalati biztonság azon aspektusával, hogy a vállalat működése a környezetére nézve is biztonságos és fenntartható legyen. A vállalati társadalmi felelősségvállalás vetületeként mindezt kezelni kell, mely további kutatás keretei között vizsgálható.

7 Irodalomjegyzék

[1] Dionne, G. (2019). Risk Management: Theories and Applications, John Wiley & Sons
[2] Michelberger, P. (2013). Vállalatbiztonság. In Nagy, I. Z. (szerk.) Vállalkozásfejlesztés a XXI. században III.: tanulmánykötet (pp. 35-52). Óbudai Egyetem
[3] Michelberger, P. (2022). Információ-, folyamat- és vállalatbiztonság (3. kiadás). Óbudai Egyetem
[4] Velencei, J. (2015). Puhatolódzó megoldások nyomában. Óbudai Egyetem
[5] Deloitte Insights. (2021). Global risk management survey (12th ed.)
[6] Metricstream. (2021). The state of risk management survey report
[7] Protiviti. (2020). The State of Risk Management Survey Report
[8] Willis Towers Watson. (2020). Global reputational risk management survey report (It's time to harness technology to improve reputational risk management)
[9] SAS. (2021). From Crisis to Opportunity: Redefining Risk Management
[10] Malhotra, N. K., & Simon J. (k. m.). (2009): Marketingkutatás. Akadémiai Kiadó
[11] Gyulavári T., Mitev A. Z., Neulinger Á., Neumann-Bódi E., Simon J., Szűcs K. (2017). A marketingkutatás alapjai. Akadémiai Kiadó. https://doi.org/10.1556/9789630598880.
[12] Kelemenné Erdős, A. (2014). A közforgalmú közlekedési szolgáltatás és piac vizsgálata marketing és fenntarthatósági nézőpontból. Budapesti Műszaki és Gazdaságtudományi Egyetem
[13] Panda, S. (2019). Comparative Analysis of Qualitative And Quantitative Research. Lib.I.Sc. Project, 1-11, https://ssrn.com/abstract=4183924
[14] Glaser, B. G., & Strauss, A. L. (1965). Awareness of Dying. Aldine.
[15] Mills, J., Bonner, A., & Francis, K. (2006). The development of constructivist grounded theory. International journal of qualitative methods, 5 (1), 25-35.
[16] Timmermans, S., & Tavory, I. (2007). Advancing ethnographic research through grounded theory practice. In Bryant, A., & Charmaz, K. (szerk.), The SAGE Handbook of grounded theory (pp. 493-513). SAGE Publications Ltd. https://doi.org/10.4135/9781848607941
[17] Mitev, A. Z. (2012). Grounded theory, a kvalitatív kutatás klasszikus mérföldköve (Grounded theory, the classic milestone of qualitative research). Vezetéstudomány - Budapest Management Review, 43 (1), 17-30. https://doi.org/10.14267/VEZTUD.2012.01.02
[18] Glaser, B. (1992). Basics of Grounded Theory Analysis. Sociology Press.
[19] Charmaz, K. (2000). Grounded theory: Objectivist and constructivist methods. (2nd Edition). Sage Publications
[20] Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. Health Services Research, 34(5 Part 2), 1189–1208.
[21] Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. Qualitative Social Work: Research and Practice, 1.(3), 261–283. https://doi.org/10.1177/1473325002001003636
[22] Staller, K. M. (2021). Big enough? Sampling in qualitative inquiry. Qualitative Social Work, 20(4), 897–904. https://doi.org/10.1177/14733250211024516
[23] Lindgren, B.-M., Lundman, B., Graneheim, U. H. (2020): Abstraction and interpretation during the qualitative content analysis process, International Journal of Nursing Studies, 108, https://doi.org/10.1016/j.ijnurstu.2020.103632
[24] Graneheim, U. H., Lindgren, B. M. & Lundman, B. (2017): Methodological challenges in qualitative content analysis: A discussion paper. Nurse Education Today, 56, 29-34.
[25] Barabási-Albert, L. (2006). A hálózatok tudománya: a társadalomtól a webig, Magyar Tudomány, 167(11), 1298–1308. http://www.matud.iif.hu/06nov/03.html

[26] Temesi, J. & Varró, Z. J. (2017). Operációkutatás. Akadémiai Kiadó
[27] Berek, L. (2014). Biztonságtechnika. Nemzeti Közszolgálati Egyetem
[28] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management - Integrated Framework Executive Summary. https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf
[29] Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39(4), 60-66.
[30] Kern, S., Baumer, T., Groll, S., Fuchs, L., & Pernul, G. (2022). Optimization of Access Control Policies, Journal of Information Security and Applications, 70, https://doi.org/10.1016/j.jisa.2022.103301
[31] Daubner, L., Macak, M., Matulevičius,R., Buhnova,B., Maksović, S.,& Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management, Journal of Information Security and Applications, 73, https://doi.org/10.1016/j.jisa.2023.103433
[32] Tworek, K. (2023). IT reliability as a source of sustainability for organisations operating during the COVID-19 pandemic. Engineering Management in Production and Services,15(1), 29-40. https://doi.org/10.2478/emj-2023-0003
[33] Bakhtina, M., Matulevičius, R., & Seeba, M. (2023). Tool-supported method for privacy analysis of a business process model, Journal of Information Security and Applications, 76. https://doi.org/10.1016/j.jisa.2023.103525
[34] Marquez-Tejon, J., Jimenez-Partearroyo, M., & Benito-Osorio, D. (2021). Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management, Security Journal, 35(2), 600-627. https://doi.org/10.1057/s41284-021-00292-4
[35] Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability, 15(7), 5828.
[36] Hoyt, R. E., & Liebenberg, A. P. (2011). The value of Enterprise Risk Management, Journal of Risk and Insurance. https://doi.org/10.1111/j.1539-6975.2011.01413.x
[37] Nocco, B. W. & Stulz, R. M. (2006). Enterprise Risk Management: Theory and Practice, Journal of Applied Corporate Finance. https://doi.org/10.1111/j.1745-6622.2006.00106.x
[38] Manab, N. A., Aziz, N. A. A., & Othman, S. N. (2017). The effect of corporate governance compliance and sustainability risk management (SRM) success factors on firm survival. International Journal of Development and Sustainability, 6 (11), 1559-1575. https://repo.uum.edu.my/id/eprint/23170/
[39] Caraiman, A.-C., & Mates, D. (2020). Risk management in corporate governance. Proceedings of the 14th International Conference on Business Excellence2020, pp. 182-201, https://doi.org/10.2478/picbe-2020-0018, https://sciendo.com/pdf/10.2478/picbe-2020-0018
[40] Kocziszky G., & Kardkovács K. (2020). A compliance szerepe a közösségi értékek és érdekek védelmében. Akadémiai Kiadó
[41] Kolnhofer-Derecskei, A. (2018). "Relations between risk attitudes, culture and the endowment effect", Engineering Management in Production and Services, 10(4), 7-20. https://doi.org/10.2478/emj-2018-0019
[42] Banham, R. 2004. Enterprising views of risk management. Journal of Accountancy 197 (6), 65-71.
[43] Hall, J. (2007). Internal Auditing and ERM: Fitting in and Adding Value, The Institute of Internal Auditors Research Foundation, https://global.theiia.org/about/about-the-iia/Public%20Documents/Sawyer_Award_2007.pdf
[44] Iványos, J. (2020). Útmutató az integrált kockázatkezelés megvalósításához. Trusted Business Advisor.

[45] Aven, T., & Ylönen, M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?, Reliability Engineering & System Safety, 189, 279-286. https://doi.org/10.1016/j.ress.2019.04.035, https://www.sciencedirect.com/science/article/pii/S0951832018312250
[46] IWA 31:2020 (en) Risk management — Guidelines on using ISO 31000 in management systems, https://www.iso.org/obp/ui/fr/#iso:std:iso:iwa:31:ed-1:v1:en
[47] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control - Integrated Framework Executive Summary. https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf
[48] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). COSO Internal Control – Integrated Framework Principles. https://www.coso.org/_files/ugd/3059fc_77d5d0f3d569439990b170bd3b909d7e.pdf
[49] ISACA. (2012). CObIT5. A Business Framework for the Governance and Management of Enterprise IT.
[50] ISACA (2019) Control Objectives for Information and related Technology - COBIT 2019
[51] Naicker, V. and Mafaiti, M. (2019). "The establishment of collaboration in managing information security through multisourcing", Computers & Security, 80, 224-237. https://doi.org/10.1016/j.cose.2018.10.005
[52] Ahlan, A. R., & Arshad, Y. (2012). Understanding Components of IT Risks and Enterprise Risk Management, In Emblemsvag, J. (szerk.), Risk Management for the Future - Theory and Cases. IntechOpen. https://doi.org/10.5772/32023. https://www.intechopen.com/chapters/36108
[53] Safa, N.S., Maple, C., Watson, T., & Von Solms, R. (2018), "Motivation and opportunity based model to reduce information security insider threats in organisations", Journal of Information Security and Applications, 40, 247-257, https://doi.org/10.1016/j.jisa.2017.11.001
[54] Sönmez, F.Ö. (2019). "A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks' Efficiency", Procedia Computer Science, 160, 181–188. https://doi.org/10.1016/j.procs.2019.09.459
[55] Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020), "Risk management practices in information security: Exploring the status quo in the DACH region", Computers & Security, Vol. 92 https://doi.org/10.1016/j.cose.2020.101776
[56] Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020), "Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach", Procedia Manufacturing, 44, 647-654 https://doi.org/10.1016/j.promfg.2020.02.244
[57] Tøndel, I.A., Line, M.B., & Jaatun, M.G. (2014). "Information security incident management: Current practice as reported in the literature", Computers & Security, 45, 42-57. https://doi.org/10.1016/j.cose.2014.05.003
[58] Ahmad, A., Maynard, S.B., & Shanks, G. (2015). "A case analysis of information systems and security incident responses", International Journal of Information Management, 35, 717-723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001
[59] Solak, S., & Zhuo, Y. (2020), "Optimal policies for information sharing in information system security", European Journal of Operational Research, 284, 934-950, https://doi.org/10.1016/j.ejor.2019.12.016
[60] Diesch, R., Pfaff, M., & Krcmar, H. (2020), "A comprehensive model of information security factors for decision-makers", Computers & Security, 92. https://doi.org/10.1016/j.cose.2020.101747

[61] Leuprecht, C., Skillicorn, D.B., & Tait, V.E. (2016), "Beyond the Castle Model of cyber-risk and cyber-security", Government Information Quarterly, Vol. 33(2), 250-257. https://doi.org/10.1016/j.giq.2016.01.012
[62] Nguen Bao Ngo, T. & Tick, A. (2021). Cyber-security risks assessment by external auditors, Interdisciplinary Description of Complex Systems 1334-4684 1334-4676 19 (3) pp. 375-390 2021, https://doi.org/10.7906/indecs.19.3.3
[63] National Institute of Standards and Technology U.S. Department of Commerce. (2020). NIST Special Publication (SP) 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5
[64] De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations. Springer Nature Switzerland AG.
[65] Jaeger, L., Eckhardt, A. and Kroenung, J. (2021). "The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis", Information & Management, 58(3). https://doi.org/10.1016/j.im.2020.103318
[66] Angraini, Alias, R.A., & Okfalisa (2019), "Information Security Policy Compliance: Systematic Literature Review", Procedia Computer Science, 161, 1216–1224 https://doi.org/10.1016/j.procs.2019.11.235
[67] Schmitz, C., & Pape, S. (2020). "LiSRA: Lightweight Security Risk Assessment for decision support in information security", Computers & Security, 90. https://doi.org/10.1016/j.cose.2019.101656
[68] Samonas, S., Dhillon, G., & Almusharraf, A. (2020). "Stakeholder perceptions of information security policy: Analyzing personal constructs", International Journal of Information Management, 50, 144-154. https://doi.org/10.1016/j.ijinfomgt.2019.04.011
[69] Liu, C., Wang, N., & Liang, H. (2020). "Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment", International Journal of Information Management, 54. https://doi.org/10.1016/j.ijinfomgt.2020.102152
[70] Abraham, S., & Chengalur-Smith, I. (2019). "Evaluating the effectiveness of learner controlled information security training", Computers & Security, 87. https://doi.org/10.1016/j.cose.2019.101586
[71] Karjalainen, M., Siponen, M., & Sarker, S. (2020). "Toward a stage theory of the development of employees' information security behaviour", Computers & Security, 93. https://doi.org/10.1016/j.cose.2020.101782
[72] Shameli-Sendi, A. (2020). "An efficient security data-driven approach for implementing risk assessment", Journal of Information Security and Applications, 54. https://doi.org/10.1016/j.jisa.2020.102593
[73] Ekler, P., & Pásztor, D. (2020). Alkalmazott mesterséges intelligencia felhasználási területei és biztonsági kérdései – Mesterséges intelligencia a gyakorlatban. Scientia et Securitas, 1(1), 35–42. https://doi.org/10.1556/112.2020.00006
[74] Barabási-Albert, L. (2008). Behálózva – A hálózatok új tudománya. Helikon Kiadó
[75] Blahó, A., Czakó, E., Poór, J. (szerk.). (2016). Nemzetközi menedzsment. Akadémiai Kiadó. https://doi.org/10.1556/9789630597548.
[76] Bakacsi, G. (2018): A hálózatoké a jövő. In Aczél, P. Csák, J. & Z. Szántó, O. (szerk.), Társadalmi jövőképesség – Egy új tudományterület bemutatkozása (pp. 269–300). Budapesti Corvinus Egyetem Társadalmi Jövőképesség Kutatóközpont
[77] Velencei, J. (2008). Az üzleti döntéshozó tudásmegosztása az e-korszakban 112 p. Budapesti Műszaki és Gazdaságtudományi Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola

[78] Chikán A. (2020). Vállalatgazdaságtan. Akadémiai Kiadó. https://doi.org/10.1556/9789634545897.
[79] Chikán, A., & Demeter, K. (2004). Az értékteremtő folyamatok menedzsmentje. Aula Kiadó
[80] Dobák M., & Antal Z. (2016). Vezetés és szervezés. Akadémiai Kiadó. https://doi.org/10.1556/9789630598262.
[81] Jelen, T., & Mészáros, T. (2018). Tervezés. Akadémiai Kiadó. https://doi.org/10.1556/9789634542193.
[82] Kadocsa, Gy. (2009). Menedzsment mérnöki ismeretek. Amicus Kiadó
[83] Poór J. (szerk.). (2017). Menedzsment-tanácsadási kézikönyv. Akadémiai Kiadó. https://doi.org/10.1556/9789634540113.
[84] Institute of Internal Auditors (IIA). (2020). The IIA's three lines model An update of the Three Lines of Defense Position Paper. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf
[85] Institute of Internal Auditors (IIA). (2013). The Three Lines of Defense in Effective Risk Management And Control January 2013 Position Paper, pp. 1-7.
[86] Chambers, R. (2020). New IIA Three Lines Model Offers Timely Evolution of a Trusted Tool, Internal Auditor. https://iaonline.theiia.org/blogs/chambers/Pages/New-IIA-Three-Lines-Model-Offers-Timely-Evolution-of-a-Trusted-Tool.aspx
[87] Institute of Internal Auditors. (n.d.). The IIA's New Three Lines Model An update of the Three Lines of Defense. https://global.theiia.org/about/about-internal-auditing/Pages/Three-Lines-Model.aspx
[88] OCEG. (n.d.). What is GRC?, https://www.oceg.org/about/what-is-grc/
[89] Mitchell, S. L. (2007). GRC360: A framework to help organisations drive principled performance. International Journal of Disclosure and Governance, 4, 279–296. https://doi.org/10.1057/palgrave.jdg.2050066
[90] Euler, L. (1741). Solutio problematis ad geometriam situs pertinentis Commentarii academiae scientiarum. Petropolitanae, 8, 128–140, http://eulerarchive.maa.org/docs/originals/E053.pdf
[91] Winston, W. L. (2003). Operációkutatás I-II. Aula Kiadó.
[92] Hernandez, E., & Menon, A. (2019). Corporate Strategy and Network Change. SSRN, https://ssrn.com/abstract=3350502, http://dx.doi.org/10.2139/ssrn.3350502
[93] Erdős, P. & Rényi, A. (1959). On random graphs, I. Publicationes Mathematicae Debrecen, 6, 290–297. https://snap.stanford.edu/class/cs224w-readings/erdos59random.pdf
[94] Erdős, P., & Rényi, A. (1960). On the evolution of random graphs. Publ. Math. Inst. Hung. Acad., 5, 17–61. http://snap.stanford.edu/class/cs224w-readings/erdos60random.pdf
[95] Gilbert, E. N. (1959). "Random Graphs". Annals of Mathematical Statistics, 30(4), 1141–1144.
[96] Barabási, A-L. & Albert, R. (1999). Emergence of scaling in random networks. Science, 286(5439), 509–512. https://doi.org/10.1126/science.286.5439.509
[97] Francsovics, A. (2011): Vezetői számvitel és controlling. Óbudai Egyetem Keleti Károly Gazdasági Kar
[98] Maczó, K. (2007). Controlling a gyakorlatban. Kempelen Farkas Hallgatói Információs Központ, Digitális Tankönyvtár
[99] Anthony, R. N., & Govindarajan, V. (2009). Menedzsmentkontroll-rendszerek. Panem Kft.

[100] Anthony, R. N. (1965). Planning and control systems: a framework for analysis. Harvard Business School.
[101] Strauss, E. (2013). Management Control Systems: A Review, Journal of Management Control. https://doi.org/10.1007/s00187-012-0158-7
[102] Malina, M. A., & Selto, F. H. (2001). Communicating and Controlling Strategy: An Empirical Study of the Effectiveness of the Balanced Scorecard, SSRN. http://dx.doi.org/10.2139/ssrn.278939
[103] Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard: measures that drive performance. Harvard Business Review, 70(1), 71-79.
[104] Kaplan, R. S., & Norton, D. P. (1993). Putting the balanced scorecard to work. Harvard Business Review, 71(5), 134–147.
[105] Szilágyi, Gy. A. (2019). A szervezeti kapcsolati háló, mint a működésbiztonság emberi tényezője, Óbudai Egyetem, Biztonságtudományi Doktori Iskola
[106] Aven, T., & Ylönen, M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?. Reliability Engineering & System Safety, 189(September 2019), 279-286, https://doi.org/10.1016/j.ress.2019.04.035
[107] Labodová, A. (2004). Implementing integrated management systems using a risk analysis based approach. Journal of Cleaner Production, 12 (6), 571-580. https://doi.org/10.1016/j.jclepro.2003.08.008
[108] Fiore, A. P., Facin, A.L. F., & Muniz, J. Jr. (2023). Information security and quality management systems integration: challenges and critical factors. International Journal for Quality Research, 17(3), 635-650.
[109] Deloitte. (2011). Global risk management survey (7th ed.)
[110] ISACA, & CMMI Institute and Infosecurity Group. (2020). State of enterprise risk management.
[111] DuPont Sustainable Solutions. (2017). Lack of Internal Alignment and Commitment of Resources to Manage Risk Threaten Corporate Business Performance, Global Survey of Executives Exposes Critical Areas of Concern for CEOs and Their Management Teams
[112] Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (angolul: General Data Protection Regulation, röviden: GDPR)
[113] Li, Q. and Wu, Y. (2020). "Intangible capital, ICT and sector growth in China", Telecommunications Policy, 44(1), https://doi.org/10.1016/j.telpol.2019.101854
[114] Hughes, B.B., Bohl, D., Irfan, M., Margolese-Malin, E. and Solórzano, J.R. (2017). "ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance", Technological Forecasting and Social Change, 115, 117-130 https://doi.org/10.1016/j.techfore.2016.09.027
[115] Jorgenson, D.W. and Vu, K.M. (2016), "The ICT revolution, world economic growth, and policy issues", Telecommunications Policy, 40(5), 383-397. https://doi.org/10.1016/j.telpol.2016.01.002
[116] Kolade, O., Owoseni, A. (2022). Employment 5.0: The work of the future and the future of work. Technology in Society, 71. https://doi.org/10.1016/j.techsoc.2022.102086
[117] Peng, G. (2017). Do computer skills affect worker employment? An empirical study from CPS surveys. Computers in Human Behavior, 74, 26-34.
[118] Falck, O., Heimisch-Roecker, A. and Wiederhold, S. (2021). Returns to ICT skills. Research Policy, 50(7). https://doi.org/10.1016/j.respol.2020.104064

[119] Pedersen, T., Scedrova, A. and Grecu, A. (2022). The effects of IT investments and skilled labor on firms' value added. Technovation, 116. https://doi.org/10.1016/j.technovation.2022.102479
[120] Skare, M., de las Mercedes de Obesso, M. and Ribeiro-Navarrete, S. (2023). Digital transformation and European small and medium enterprises (SMEs): A comparative study using digital economy and society index data. International Journal of Information Management, 68. https://doi.org/10.1016/j.ijinfomgt.2022.102594
[121] Coronado, E., Kiyokawa, T., Ricardez, G.A.G., Ramirez-Alpizar, I.G., Venture, G. and Yamanobe, N. (2022). Evaluating quality in human-robot interaction: A systematic search and classification of performance and human-centered factors, measures and metrics towards an industry 5.0. Journal of Manufacturing Systems, 63, 392-410.
[122] Maddikunta, P. K.R., Pham, Q-V, Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T.R., Ruby, R. and Liyanage, M. (2022). Industry 5.0: A survey on enabling technologies and potential applications. Journal of Industrial Information Integration, 26, https://doi.org/10.1016/j.jii.2021.100257
[123] International Organization for Standardization (ISO). (2021). THE ISO SURVEY OF MANAGEMENT SYSTEM STANDARD CERTIFICATIONS – 2020 – EXPLANATORY NOTE. https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_and_overview_on_ISO_Survey_2020_results.pdf?nodeid=21899356&vernum=-2 (letöltés dátuma: 2022.06.02.)
[124] International Organization for Standardization (ISO). (2021). 1. ISO Survey 2020 results - Number of certificates and sites per country and the number of sector overall. ISO Survey of certifications to management system standards - Full results https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 (downloaded: 2022.06.02.)
[125] International Organization for Standardization (ISO). (2019). ISO 9001: 2015 How to use it, https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100373.pdf
[126] Keen, R. (2022). Benefits of and Environmental Management System. https://www.iso-9001-checklist.co.uk/ISO-14001/benefits-of-an-environmental-management-system.htm
[127] International Organization for Standardization (ISO). (2021). 2. ISO Survey 2020 results - Number of sectors by country for each standard. ISO Survey of certifications to management system standards - Full results https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 (downloaded: 2022.06.02.)
[128] Project Management Institute. (2020). Projektmenedzsment útmutató PMBoK Guide. Akadémiai Kiadó. https://doi.org/10.1556/9789634545019
[129] DAMA International. (2017). Guide to the Data Management Body of Knowledge (2nd Edition) (DAMA-DMBOK2)
[130] Audi AG . (2020). Annual Report. <https://www.audi.com/en/company/investor-relations/annual-reports.html>
[131] Daimler Group. (2020). Annual Report. <https://www.daimler.com/documents/investors/reports/annual-report/daimler/daimler-ir-annual-report-2020-incl-combined-management-report-daimler-ag.pdf>
[132] Suzuki. (2020). Annual Report. <https://www.globalsuzuki.com/ir/library/annualreport/pdf/2020/2020.pdf><https://www.globalsuzuki.com/ir/library/annualreport/pdf/2020/2020_fs.pdf>
[133] Groupe PSA . (2019). Annual Report. <https://www.groupe-psa.com/en/publication/2019-annual-results/>
[134] European Court of Auditors. (2019). The EU's response to the „dieselgate" scandal, Briefing paper.

<https://www.eca.europa.eu/lists/ecadocuments/brp_vehicle_emissions/brp_vehicle_emissions_en.pdf>
[135] Rao, S. R. (2014). Perspective SOX Controls - Driving Transformation of the Order-to-Cash Value Chain. Infosys Limited External Document. https://www.infosysbpm.com/offerings/functions/sales-fulfillment/white-papers/Documents/SOX-controls.pdf
[136] Szilágyi, Gy. A. (2015). Determining delay risks of processes deriving from personal professional competences," 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY), 205-208, https://doi.org/10.1109/SISY.2015.7325380
[137] Trusted Business Partners Technical Department of ENISA Section Risk Management ENISA. (2006). Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools
[138] Reason, J. (1999). The 'Swiss Cheese' model.
[139] Reason, J. (2000). Human error: models and management. BMJ, 320(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768
[140] Takácsné Gy. K. & Benedek A. (2016). Bizalmon alapuló együttműködés vizsgálata a kis- és középvállalatok körében. In Csiszárik-Kocsir, A. (szerk.), Tanulmánykötet - Vállalkozásfejlesztés a XXI. században VI. (pp. 379–390). Keleti Faculty of Business and Management Óbuda University
[141] Schneier, B. (2003). Beyond fear – Thinking sensibly about security in an uncertain world. Springer-Verlag Copernicus Books. https://doi.org/10.1007/b97547
[142] Hadnagy, C. (2011). Social engineering: The art of human hacking. Wiley Publishing.
[143] Mitnick, K. D. & Simon, W. L. (2002). Art of depiction: Controlling the human element of security. Wiley Publishing.
[144] Magyar Nemzeti Kibervédelmi Intézet (2019). Az információbiztonság lélektana (Psychology of Information Security).
[145] Rajnai Z. (2017). Információbiztonság tudatosság. Műszaki Tudományos Közlemények, 37–42. https://www.eme.ro/publication-hu/mtk/mtk7/MTK7_02_Rajnai-plen.pdf
[146] Mendes Jr, De Jesus Alvares I., & Alves, M. D. C. (2023). The balanced scorecard in the education sector: A literature review. Cogent Education, 10(1). https://doi.org/10.1080/2331186X.2022.2160120
[147] Tawse, A., & Tabesh, P. (2023). Thirty years with the balanced scorecard: What we have learned. Business Horizons, 66(1), 123-132.
[148] Madsen, Dag Øivind and Stenheim, Tonny. (2015). The Balanced Scorecard: A Review of Five Research Areas. American Journal of Management, Vol. 15(2), 24-41. https://ssrn.com/abstract=2612643
[149] van der Aalst, W. M. P., La Rosa, M. & Santoro, F. M. (2016). Business Process Management: Don't Forget to Improve the Process!. Business and Information Systems Engineering, 58(1), https://doi.org/10.1007/s12599-015-0409-x
[150] Giannopoulos, George, Holt, Andrew, Khansalar, Ehsan and Cleanthous, Stephanie (2013) The use of the balanced scorecard in small companies. International Journal of Business and Management, 8(14), pp. 1-22. ISSN (print) 1833-3850. http://dx.doi.org/10.5539/ijbm.v8n14p1
[151] Amer, F., Hammoud, S., Khatatbeh, H., Lohner, S., Boncz, I., & Endrei, D. (2022). The deployment of balanced scorecard in health care organizations: is it beneficial? A systematic review. BMC Health Services Research, 22(1), 1-14.
[152] Peters, D. H., Noor, A. A., Singh, L. P., Kakar, F. K., Hansen, P. M., & Burnham, G. (2007). A balanced scorecard for health services in Afghanistan. Bulletin of the world Health Organization, 85(2), 146-151.

[153] Mohamed, S. (2003). Adaptation of the balanced scorecard to measure organizational safety culture. Journal of Construction Research, 4(01), 45-57.
[154] Mearns, K., & Ivar Håvold, J. (2003). Occupational health and safety and the balanced scorecard. The TQM Magazine, 15(6), 408-423.
[155] Beheshti, A. R., Kamali, K., Arghami, S., & Mohammadi, A. (2018). Assessing the Performance of the Health, Safety and Environment Management System (HSE) using the Modified Balanced Scorecard Model. Journal of Iranian Medical Council, 1(2), 87-95.
[156] Azour, F., Moussami, H. E., Dahbi, S., & Ezzine, L. (2017). Integration of health and safety at work and environment perspectives in the balanced scorecard. In Proceedings of the International Conference on Industrial Engineering and Operations Management Rabat Morocco (pp. 1113-1121).
[157] Alolah, T., Stewart, R. A., Panuwatwanich, K., & Mohamed, S. (2014). Determining the causal relationships among balanced scorecard perspectives on school safety performance: Case of Saudi Arabia. Accident Analysis & Prevention, 68, 57-74.
[158] Lin, W. C., & Cheng, H. H. (2021). Improving maritime safety through enhancing marine process management: The application of balanced scorecard. Management Decision, 59(3), 604-615.
[159] Fatkieva, R., & Krupina, A. (2020). Enterprise Information Security Assessment Using Balanced Scorecard. In Advances in Automation: Proceedings of the International Russian Automation Conference, RusAutoCon 2019, September 8-14, 2019, Sochi, Russia (pp. 1147-1157). Springer International Publishing.
[160] Herath, T. C., Herath, H. S., & Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. Information Systems Frontiers, 25(2), 681-721.
[161] Tallau, L. J., Gupta, M., & Sharman, R. (2010). Information security investment decisions: evaluating the balanced scorecard method. International Journal of Business Information Systems, 5(1), 34-57.
[162] Humphreys, E. (2011). Information security management system standards, Datenschutz und Datensicherheit – DuD, 35 (1), 7-11. https://doi.org/ 10.1007/s11623-011-0004-3
[163] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2),92-100. https://doi.org/ 10.4236/jis.2013.42011
[164] Arsenault, B. (2023). Your Biggest Cybersecurity Risks Could Be Inside Your Organization, Harvard Business Review, https://hbr.org/2023/03/your-biggest-cybersecurity-risks-could-be-inside-your-organization
[165] van Zadelhogg, M. (2016). The Biggest Cybersecurity Threats Are Inside Your Company, Harvard Business Review, https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company
[166] Pokorádi, L. (2008). Rendszerek gráfmodellezése. Gép: a gépgyártás műszaki folyóirata, 59(8), 59-62.
[167] ISO 9001:2015 Quality management systems — Requirements
[168] ISO 14001:2015 Environmental management systems — Requirements with guidance for use
[169] ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements
[170] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements
[171] ISO 22316: 2017 Security and resilience Organizational resilience Principles and attributes

[172] ISO/IEC 27000 Family information security management
[173] ISO/IEC 27000:2018 Information technology Security techniques Information security management systems Overview and vocabulary
[174] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements
[175] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
[176] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection Guidance on managing information security risks
[177] ISO 28000:2022 Security and resilience — Security management systems — Requirements
[178] ISO 28001:2007 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance
[179] ISO 31000:2018 Risk management — Guidelines
[180] ISO 33001: 2015 Information technology Process assessment Concepts and terminology
[181] ISO 37001:2016 Anti-bribery management systems — Requirements with guidance for use
[182] ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use
[183] ISO 50001:2018 Energy management systems — Requirements with guidance for use
[184] ISO 13485:2016 Medical devices Quality management systems Requirements for regulatory purposes
[185] ISO 22000:2018 Food safety management systems Requirements for any organization in the food chain
[186] ISO 39001:2012 Road traffic safety (RTS) management systems Requirements with guidance for use

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

[S1] Michelberger, P., & Kemendi, Á. (2020). Data, information and ITsecurity - Software support for security activities. *Problems of management in the 21st century*, 15(2), 108–124. https://doi.org/10.33225/pmc/20.15.108
[S2] Kemendi, Á. (2021). HR process safety & security in the industry 4.0. era. *Bánki Közlemények*, 4(1), 55–60.
[S3] Kemendi, Á., Michelberger, P., & Mesjasz-Lech, A. (2021). ICT security in businesses – efficiency analysis. *Entrepreneurship and sustainability issues*, 9(1), 123–149. https://doi.org/10.9770/jesi.2021.9.1(8)
[S4] Michelberger, P., & Kemendi, Á. (2021). Projektkockázatok és kockázatos projektek. *International Journal of Engineering and Management Sciences / Műszaki és Menedzsment Tudományi Közlemények*, 6(2), 164–189, https://doi.org/10.21791/IJEMS.2021.2.14.
[S5] Kemendi, Á. (2021). E-commerce safety and security in the industry 4.0 era. *National Security Review: Periodical of the Military National Security Service*, (1), 195–217.
[S6] Kemendi, Á. (2022). Integrált kockázatkezelés. *Biztonságtudományi Szemle*, 4(1), 43–61.

[S7] Kemendi, Á., Michelberger, P., & Mesjasz-Lech, A. (2022). Corporate risk management: development and applications. In: Živan, Živković (szerk.) *An international serial publication for theory and practice of Management Science* - IMCSM 2022 Bor, Szerbia: University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD) pp. 85-100.

[S8] Kemendi, Á. (2022). A biztonság hálózata - a kontrollok biztonsági hálózata. *Jelenkori Társadalmi és Gazdasági Folyamatok*, 17(1–2), 77–90. https://doi.org/10.14232/jtgf.2022.1-2.77-90

[S9] Kemendi, Á., Michelberger, P., & Mesjasz-Lech, A. (2022). Industry 4.0 and 5.0–organizational and competency challenges of enterprises. *Polish Journal of Management Studies*, 26(2), 209–232. https://doi.org/10.17512/pjms.2022.26.2.13.

[S10] Kemendi, Á. (2023). Humán kockázatok hálózatkutatási szempontból. *Belügyi Szemle*, 71(2), 317–334. https://doi.org/10.38146/BSZ.2023.2.8

[S11] Kemendi, Á. (2023). A vállalati biztonsági háló meghatározó tényezői, *Scientia et Securitas*, https://doi.org/10.1556/112.2023.00152

[S12] Kemendi, Á., & Michelberger, P. Process security methods and measurement in the context of standard management systems. *Engineering Management in Production and Services, EMPAS megjelenés alatt*

8.2 További tudományos közlemények

[S13] Francsovics, A., Kemendi, Á., & Piukovics, A. (2019). Controlling as a Management Function. In *17th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2019)* (pp. 35–42).

[S14] Mesjasz-Lech., A., Kemendi, Á., & Michelberger, P. (2024). Circular manufacturing and Industry 5.0. assessing material flows in the manufacturing process in relation to e-waste streams, *Engineering Management in Production and Services, 16*(1), 114-133. https://doi.org/10.2478/emj-2024-0009