ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

KEMENDI ÁGNES

A vállalati biztonsági háló meghatározó tényezői

Témavezető: Prof. Dr. Michelberger Pál egyetemi tanár

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024.04.22.

Szigorlati / Komplex vizsga bizottsága:

Elnök:

Dr. Takácsné Prof. Dr. György Katalin

Tagok:

Dr. habil. Velencei Jolán

Dr. habil. Kerti András

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Pokorádi László

Titkár:

Dr. Szikora Péter

Tagok:

Dr. habil. Velencei Jolán

Dr. Szilágyi Győző

Dr. habil. Kiss Gábor

Bírálók:

Dr. Kolnhofer-Derecskei Anita

Dr. Katona Ferenc

Nyilvános védés időpontja:

2024.

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK
MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott Kemendi Ágnes kijelentem, hogy

„A vállalati biztonsági háló meghatározó tényezői”

című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2024.04.22.

Kemendi Ágnes

TARTALOMJEGYZÉK

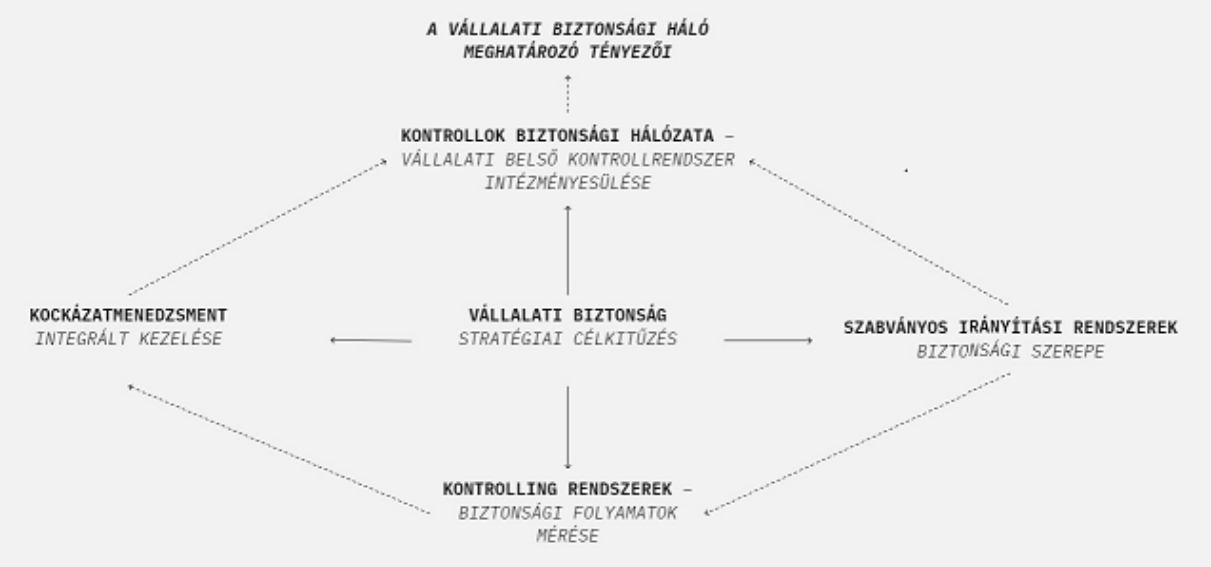
BEVEZETÉS – A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A ma vállalata komplex biztonsági kihívásokkal szembesül, dinamikusan változó és digitális transzformációk, valamint digitális innovációk által meghatározott üzleti-, kockázati-, és kontrollkörnyezetben működik, behálózzák az információs és kommunikációs technológiák, mely a biztonság területén is felkészültséget igényel. A folyamatos változásokhoz való alkalmazkodás meghatározó a vállalati életben. A vállalati biztonság stratégiai jelentőségű. A hosszú távú sikeres vállalati működés szempontjából alapvető a biztonság területének kezelése.

A vállalatokra a működési környezete, mint például a piaci környezet, vevői igények, elvárások, a technikai-, technológiai környezet, gazdasági környezet nagy hatást gyakorol. A kockázati környezetben jelen lévő tradicionális kockázatok mellett az újonnan megjelenő biztonsági fenyegetések kezelése a vállalatok szemszögéből rendkívül aktuális témát jelent. A digitális kor innovatív légkörében újabb és újabb fenyegetettségek jelennek meg, melyek az információbiztonság szerepét piedesztálra emelik, és egyúttal az emberi tényezőkben rejlő kockázatokra is kiemelt figyelmet kell fordítani. A napjaink működési környezetét meghatározó ipari forradalmakhoz, az ipar 4.0-hoz és ipar 5.0-höz kapcsolódó digitális átalakulás, valamint a COVID-19 világjárvány meghatározó próbatételt jelentenek a vállalati biztonság szempontjából.

A kutatás arra keresi a választ, melyek azok a tényezők, melyek a turbulensen változó üzleti, és kockázati környezetben a vállalatok biztonságos működését elő tudják segíteni, azaz melyek a vállalatot behálózó belső kontrollrendszer, az ún. vállalati biztonsági háló működésének meghatározó tényezői. A kutatási témám mögött meghúzódó aspirációm a biztonság szerepének láthatóvá tétele és bemutatása annak, hogy a biztonság az üzleti sikerekhez hogyan járul hozzá.

A biztonságtechnika területei közül a vállalatbiztonsággal foglalkozom. A vállalatbiztonsági területek kutatásban lefedett része a vállalat belső kontroll rendszerére, a vállalati folyamatokat behálózó biztonsági elemekre fókuszál. A vállalati biztonság kérdéskörének vizsgálata összetett. A doktori értekezésemben a vállalati biztonság kérdéskörét 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 tárom fel a vállalati biztonság meghatározó tényezői közötti összefüggéseket.



1. ábra Az értekezés tartalmi struktúrája

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. Az értekezésemben vizsgálom az emberi tényező biztonságban betöltött szerepét.

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 a 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, például a kiegyensúlyozott mutatószámrendszer alkalmazása során, és a szabványos irányítási rendszerek szempontjából is. 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. Az értekezésemben vizsgálom a kontrolling rendszerek és eszközök, valamint a szabványos irányítási rendszerek vállalati biztonságban betöltött szerepét.

A hálózatok fogalmát adaptáltam a vállalati biztonsági folyamatokra. 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 kutatásomat vállalatokra vonatkozóan végeztem. A kutatásom vállalatmérettől függetlenül értelmezhető nagyvállalatokra, valamint kis- és középvállalatokra is, azonban gyakorlati alkalmazására vonatkozóan egyéni kontextusba helyezés és mérlegelés szükséges. A kutatásommal kapcsolatban érintett terület a mesterséges intelligencia szerepe és hatásai, mellyel jelen értekezésben nem foglalkozom részletesen a tématerületen tapasztalható dinamikus, evolúciós fejlődés miatt. Az értekezésemnek nem célja a kapcsolódó keretrendszerek, szabványok és jogszabályok lefedése.

A kutatási témámat a karrierutam során megszerzett tapasztalataimból merítettem, mely során számos vállalat működésébe nyertem betekintést a pénzügyi kimutatásokon és a vállalati folyamatokon keresztül. Elsajátítottam a folyamatos fejlesztés szemléletét. Megismertem az irányítási rendszerek működését. Lehetőségem volt a vállalatokat entitás szintű és operatív folyamatok szintjén is megismerni. Megtapasztaltam, hogy mennyire összefügg minden mindennel, és mennyi kapcsolódási pont van. A rendszerek szinte „szólj! s ki vagy, elmondom” módjára képet adnak a vállalat működéséről, és folyamatairól. A folyamatokhoz kapcsolódik az emberi tényező. Állandó a változás, és adaptív ellenálló képességre van szükség. A biztonság értéket teremt, ugyanakkor a biztonsági törekvések megvalósítása a gyakorlatban nehézkes lehet.

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.

A vállalati folyamatok működése során a biztonsági elemek, azaz a kontrollok biztosítják a szükséges biztonsági szintet. Kontrollok alatt azokat a tevékenységeket értem, melyek biztosítják, hogy a folyamat hibamentesen, illetve adott elfogadható tűréshatáron belüli hibaszázalékkal megy végbe [S8]. A biztonsági kontrollok meghatározása a kockázatok azonosítása, elemzése és értékelése alapján történik. A folyamatok folyamatos kontrolljára, és fejlesztésére jó eszköz a PDCA módszer, például a PDCA ciklus (Plan-Do-Check-Act) tervezés-végrehajtás-ellenőrzés, és beavatkozás lépéseinek alkalmazása az információbiztonsági folyamatokra.

Incidens: nem várt negatív biztonsági esemény, mely a normál üzletmenetre kedvezőtlen hatással van. A biztonsági esemény kezelését az incidenskezelési eljárás szerint kell lefolytatni, és lépéseket kell tenni arra, hogy az újra ne következzen be. Incidens származhat például emberi hibából, a bizalmasság, sértetlenség és rendelkezésre állás megsértéséből, rendszer hibás működéséből vagy szabályzatoknak való nemmegfelelésből.

Kontroll funkció: A kontroll funkció több szinten jelenik meg a vállalati működés során: a teljes vállalatra érvényes, valamennyi munkavállalóra kiterjedő elvek formájában, például az etikai / viselkedési kódex, mely az entitás egészére érvényes, valamint a működési folyamatokba épített ellenőrzés, kontroll tevékenységek formájában. Egyes vállalati funkciók kontroll funkciót is ellátnak, például a kontrolling, számvitel, jelentéstétel (riporting), HR. Továbbá, egyes funkciók kifejezetten kontroll funkciót töltenek be, például kockázatkezelés, megfelelés (compliance), és a biztonságért felelős csoportok, például IT biztonság, fizikai biztonság. Összességében, a kontroll funkció része valamennyi vállalati folyamatnak, megjelenik mindazon elveken, szabályzatokon, eljárásokon, tevékenységeken keresztül, melyek a belső kontrollrendszer megvalósulását, és működését segítik. A kontroll funkció valamennyi vállalatnál azonosítható, komplexitása azonban vállalatmérettől függ. Működését nagyobb, jellemzően tőzsdei vállalatoknál önálló támogató funkció (belső kontroll csoport) segíti [S8].

Információbiztonság: információbiztonság állapotában megvalósul az információ bizalmas kezelése, sértetlensége és rendelkezésre állása [173]. Magában foglalja az informatikai biztonságot, az infokommunikációs biztonságot, papír alapú adathordozók biztonságát, és az emberi tényezővel kapcsolatos információbiztonsági kockázatok kezelését is.

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

Biztonsági háló – a kontrollok biztonsági hálózata: A belső kontrollrendszer összetett és behálózza a vállalatot. A vállalatot behálózó kontrollrendszert kontrollok biztonsági hálózatának, röviden *biztonsági hálónak* nevezem. Az értekezés kontextusában a háló kifejezést eltérően alkalmazom a matematika területén alkalmazott háló definíciójától. A biztonsági háló kontextusában a hálózatokra jellemző kétirányú áramlás is megengedett az éleken. A biztonsági háló tulajdonképpen a (belső) *kontrollhálózat,* melyre az értekezésben *kontrollok rendszere*ként is hivatkozom. A kontrollhálózat a teljes vállalati működési rendszerre vonatkozóan a vállalati biztonsági hálót / kontrollhálózatot jelenti, mindemellett egy adott folyamatra vonatkozóan az adott folyamat kontrollhálózata is értelmezhető. A folyamatokhoz rendelt kontrollok hálózata a belső kontrollrendszer megvalósulása a vállalati folyamatokban. A biztonság hálózatának fogalma jól illusztrálja a vállalati biztonsági rendszer összetettségét, és a biztonsági háló elemei közötti összefüggő, és kölcsönös kapcsolatban álló relációt. A fogalmat az [S8] publikációmban definiáltam.

A disszertáció felépítése

Az értekezésemben a kutatási célkitűzések és hipotézisek meghatározását a kutatási módszerek részletes bemutatása követi. Szakirodalmi áttekintésen keresztül vezetem fel a tématerületet, a vállalatbiztonság modellezését. Ezt követően szekunder és primer adatokon alapuló kutatási eredményeimet ismertetem, és állapítom meg az értekezés téziseit.

1. KUTATÁSI CÉLKITŰZÉSEK ÉS HIPOTÉZISEK

A 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.

2. KUTATÁSI MÓDSZEREK

2.1. 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 kutatási célkitűzések megvalósításához további vizsgálatokat folytattam. 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].

2.2. A belső kontrollrendszer tartalomelemzése

Kvalitatív kutatást végeztem a vállalatbiztonságot meghatározó kontrollok hálózati jellegének vizsgálatára a H1 hipotézishez kapcsolódóan, melynek feltárásához a következő kérdésekből indultam ki:

1. *Hogyan jelenik meg a kontroll funkció / belső kontrollrendszer a vállalat éves beszámolójában? Milyen modellt követ? Mely kapcsolódó funkciók azonosíthatók? Hogyan jelenik meg a biztonság és védelem pl. információbiztonság (information security), biztonság és védelem (safety and security) a vállalat éves beszámolójában?*
2. *Hogyan jelennek meg a kockázati tényezők, és bizonytalanságok a vállalat éves beszámolójában?*
3. *A humán erőforrás szerepe miként azonosítható biztonság és védelmi kontextusban?*
4. *Rés a pajzson esetek. Szerepelnek a vállalati éves jelentésben vállalati botrányok, csalások? Amennyiben igen, milyen a vezetőség válasza?*

5. *Milyen kontextusban jelenik meg a hálózat (network) kifejezés a vállalat éves beszámolójában? Mennyiben jelenik meg a vállalati belső kontrollrendszer hálózatként, és miként definiálható a hálózati struktúra?*

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 minta: A vizsgált minta a Magyarországon jelen lévő autóipari vállalatok, ahol a biztonság kérdésköre stratégiai célkitűzésként jelenik meg. A mintába a Magyarországon működő négy autóüzem - Suzuki, Opel, Audi, Mercedes – anyavállalata került. A vizsgált vállalatok közül három vállalat tőzsdén jegyzett anyavállalathoz kötődik (Audi, Mercedes, Suzuki), míg egy vállalat (Opel) jelenleg magántulajdonban lévő vállalat. Az autóipari szektor választását indokolja, hogy az autóiparon belül kiemelkedően megjelennek az ipar 4.0. által generált technológiai újdonságok, lehetőségek és fenyegetettségek, folyamatos változások és fejlesztések, melyek napjainkban meghatározó jelentőséggel bírnak. A szektor magasan standardizált folyamatokkal működik. A gyártás során a mesterséges intelligencia alkalmazása jelentős. A gyártósorokon az ember és robot együttesen dolgozik. A választott iparágat magát is jellemzi a hálózatszerű működés, példaként említhető a Catena-X Autóipari Hálózat, melynek célja, hogy egységes szabványt hozzon létre az információk és az adatok megosztására az autóipari értéklánc egészében. A kutatás elsődlegesen a vállalati belső biztonsági háló elemeinek megismerésére irányul, így a hálózatszerű működés iparági formáját alapvetően nem tekintettem a vizsgálat tárgyának, csak amennyiben az releváns volt a vizsgált tématerület vonatkozásában.

A tulajdonosi érdek védelme kapcsán magas kontrolltudatosság, a pénzügyi beszámolóhoz kapcsolódó belső kontrollok (ICFR – Internal Control over Financial Reporting) megjelenése, továbbá a vállalatméretből kifolyólag nagyfokú rendszerszemlélet, és dokumentáltság feltételezhető. A kutatás tárgya a kontrollhálózat feltárása, melyhez a minta jó alapul szolgál.

A kutatási kérdések vezérfonala mentén a vizsgált vállalatok kontrollrendszerét, és kontrollfolyamatainak hálózatát a vállalatok éves beszámolói alapján „külső szemlélőként" vizsgáltam. Az éves beszámolók tartalomelemzését tételes adatrögzítő íveken rögzítettem.

2.3. 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.

2.4. 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 szakértői kutatás a H1, H2 és H4 hipotézisek igazolásához kapcsolódik. Az interjúkérdéseket az 1. sz. Melléklet tartalmazza. A szakértői megkérdezéseket 2023. 03-04. hónapokban online formában és telefonon végeztem. Az interjúkészítés során tíz kérdésből álló kérdéssor alapján strukturált interjúkat folytattam annak érdekében, hogy a kapott válaszok minden esetben összehasonlíthatóak legyenek, és a transzparens adatelemzést biztosítani tudjam. Az interjú strukturált jellege lehetővé tette, hogy az interjúkészítés során az objektivitást fenntartsam, és az interjúalanyokat válaszadásuk során ne befolyásoljam. Szabad válaszadásra ösztönöztem az interjúalanyokat, semleges kutatói álláspontot képviselve.

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].

Az interjúkérdésekre adott válaszok szó szerinti jegyzőkönyve alapján végeztem az adatelemzést, melynek során soronként elemeztem az interjúszövegeket. Az interjúszövegekből először az iniciális nyitott kódokat emeltem ki, mely alapján meghatároztam a tematizált nyitott kódokat. Ezt követően az axiális kódolás következett, azaz kapcsolatokat, összefüggéseket kerestem. A kódolás következő szakaszában tovább tömörítettem a kinyert adatokat, szelektív kódokat határoztam meg. Végül az elméleti kódok meghatározására került sor.

A kódolást többször ellenőriztem, szükség esetén azt felülbíráltam. A kódolási eljárás az elsődleges cél, a megalapozott elmélet létrehozásán túl az adatelemzés megbízhatóságát is erősíti.

A minta: A tématerületen kiemelkedően jártas, nagy értékű tapasztalattal, szakmai referenciával és releváns képzettséggel rendelkező személyeket kértem fel interjúalanyként, akiknek szakmai tapasztalata, illetve vevőköre jellemzően több szektorból tevődik ki. A kutatást összesen négy hazai és egy külföldi interjúalany részvételével végeztem.

Az interjúalanyokról és az általuk képviselt szakterületről készített összefoglaló a teljesség igénye nélkül: Három kifejezetten informatika, információbiztonság, illetve szoftverfejlesztés területen kiemelten elismert és jártas cégalapító, tulajdonos, illetve ügyvezető (a továbbiakban: biztonsági szakértők csoportja) szakértővel készítettem interjút. A szakértők jellemzően több évtizedes és több iparágból származó szakmai tapasztalaton túl releváns szakmai képesítésekkel is rendelkeznek. A biztonsági szakértők csoportjába tartozó interjúalanyokhoz köthető vállalatok köre képviseli többek között a bank és pénzügyi szektort, biztosítókat, energiaipart, építőipart, légitársaságokat, egészségügyet, kiskereskedelemet, médiát és távközlést. Az interjúalanyok, valamint vállalataik oktatási, és képzési tevékenységet is folytatnak int. al. informatika, információbiztonság, és üzletmenet-folytonosság területeken. Két interjúalany egyetemi oktató is, egyikük az MTA köztestületének tagja. Az interjúalanyok szakmai képesítései magában foglalják Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Data Privacy Solutions Engineer (CDPSE), ISO 9000-, ISO 27001-, illetve ISO 22301 vezető auditor, Six Sigma. A biztonsági szakértők mellett megkerestem egy HR szolgáltatás, pénzügy, kontrolling területen jártas hazai és egy pénzügy, kontrolling, belső kontroll területen jártas külföldi cégvezetőt is. A mintába került munkaerőkölcsönzéssel foglalkozó vállalatot képviselő ügyvezető kiterjedt vevőkörrel rendelkező, dinamikusan bővülő digitális átalakulásban érintett nagyvállalatot képvisel. A mintába került külföldi interjúalany szintén széleskörű tapasztalattal rendelkezik digitális átalakulással kapcsolatban.

Valamennyi hazai interjúalany országosan elismert, több évtizedes szakmai tapasztalattal rendelkezik, akik szakmai fórumokon, és nyilvános szerepléseiken keresztül is a szakma meghatározó szereplői. A hazai minta esetében az interjúalanyok által reprezentált vállalatoknál a nettó árbevétel nagyságrendje: ~ 1-70 Mrd vállalatcsoport szinten; létszámadat ~ 40-6000 fő. Fő tevékenység: 6202. Információ-technológiai szaktanácsadás; 6203. Számítógép-üzemeltetés; 6201. Számítógépes programozás; illetve 7820. Munkaerőkölcsönzés.

Az interjúalanyok a nyújtott szolgáltatásaikon, illetve termékeiken keresztül a hazai, és nemzetközi állapotokra is rálátnak. Az interjúalanyok kapcsolatban állnak nagy, ismert vállalatokkal. Az általuk reprezentált egyes vállalatok külföldi irodával, illetve irodákkal is rendelkeznek. A kutatás reprezentálja a hazai és nemzetközi állapotokat is. Az interjúalanyok, és a vállalataik által reprezentált kapcsolati háló biztosítja a szakértői kutatás széleskörű lefedettségét. Az interjúalanyok több évtizedes releváns szakmai tapasztalata, és betöltött pozíciójuk további súlyt ad válaszaiknak.

Az interjúalanyok kiválasztása megalapozta a kinyert adatok hitelességét és megbízhatóságát. Az interjúalanyok gondosan átgondolt, céltudatos kiválasztása nagyban elősegítette a telítettségi szint elérését [20; 21; 22]. Az interjúalanyok válaszai összhangban voltak egymással és egymást erősítették, ezáltal az elméleti telítődés viszonylag kis elemszámú minta mellett megvalósult.

2.5. 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.

2.6. 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.

3. VÁLLALATBIZTONSÁG MODELLEZÉSE

A fejezetben a vállalatbiztonság területét holisztikusan közelítem meg, vizsgálom a biztonság szerepét (3.1. fejezet), a vállalati kockázatokat és kockázatkezelést (3.2. fejezet), a hálózatok illeszkedését a vállalati kontextushoz (3.3. fejezet), valamint a kontrolling rendszereket (3.4. fejezet) és a szabványos irányítási rendszereket (3.5. fejezet).

3.1. A biztonság szerepe

A biztonság a biztonságtudomány kulcsfogalma [27]. Sok vállalatvezető gyakori aggodalmát jelentik a kockázatkezelés, a megfelelési folyamatok és az ellenőrzési tevékenységek költségei a megszerzett értékhez képest. Ahogy a vállalati kockázatkezelési gyakorlatok fejlődnek, fontossá válik, hogy a kockázatot, a megfelelőséget, az ellenőrzést és még az irányítást is átfogó tevékenységeket hatékonyan koordinálják annak érdekében, hogy a szervezet számára maximális hasznot hozhassanak. Ez jelentheti az egyik legjobb lehetőséget a vállalati kockázatkezelés számára, hogy újradefiniálja fontosságát a szervezet számára" [28; p.7]. A belső szabályzatoknak, előírásoknak, jogszabályoknak, szabványoknak, illetve szerződéseknek való megfelelés (compliance) megközelítése olyan koherens üzleti folyamat (nem egy projekt) irányába fejlődik, amely magában foglalja a szervezet minden aspektusát. Eszerint a megfelelést üzleti folyamatként kezelik és mérik, mely néhány nagyobb szervezetet arra késztet, hogy biztonsági vezetőt (chief security officer) vagy kockázati vezetőt (chief risk officer) nevezzenek ki annak érdekében, hogy a biztonsági megfeleléssel a szervezet egészében és folyamatosan foglalkozzanak [29].

A biztonsági kockázatok egyre összetettebbé váltak, és a vállalatoknak az újonnan megjelenő biztonsági fenyegetéseket is kezelniük kell. A modern vállalatok szervezeti felépítése és IT infrastruktúrája is folyamatosan változik [30]. A digitális rendszerek ki vannak téve a kibertámadás kockázatának [31]. Az IT megbízhatóság kulcsfontosságú a szervezetek túlélése és fenntarthatósága szempontjából; a negatív hatások, a COVID-19 világjárvány okozta hatások mérséklése érdekében javasolt az IT megbízhatóság előmozdítása és a szervezetek fenntarthatóságának forrásaként való figyelembevétele [32]. Ezenkívül a digitalizáció új irányokat szab, és olyan lehetőségeket, kockázatokat és kötelezettségeket hoz, mint például a magánélet védelme (például az adatvezérelt döntéshozatalra való áttérés az azonosítható személyekkel kapcsolatos érzékeny adatokra hagyatkozik) [33].

A vállalati működés szempontjából meghatározó a változásokhoz való folyamatos alkalmazkodás, mely a reziliencia képességét követeli meg. „Ahogy a szervezetek egyre jobban integrálják a vállalati kockázatkezelést a stratégiával és a teljesítménnyel, az megteremti a reziliencia erősítésének lehetőségét” [28; p.8]. A vállalati kockázatkezelési (ERM – Enterprise Risk Management) modell összehangoltan járul hozzá a szervezeti rezilienciához [34]. A biztonsági stratégiák hatékony integrálásával a vállalatok reziliensebbé válhatnak az információbiztonsági fenyegetésekkel és kibertámadásokkal szemben [35]. A vállalati biztonság közvetlen kapcsolatát a szervezet ellenálló (reziliencia) képességével a Nemzetközi Szabványügyi Szervezet (ISO – International Organization for Standardization) is bemutatja az ISO 22316: 2017 Biztonság és reziliencia - Szervezeti reziliencia - Elvek és Tulajdonságok szabványban [171]. A szabvány szerint a leginkább reziliens szervezetek képesek előre látni és reagálni a fenyegetésekre és lehetőségekre, amelyek belső és külső környezetük hirtelen vagy fokozatos változásaiból fakadhatnak. A reziliencia javítása stratégiai szervezeti célkitűzés kell, hogy legyen, mely a helyes üzleti gyakorlat és a hatékony kockázatkezelés eredménye [34].

Az ERM és az ERM vállalatértékre gyakorolt hatása között feltételezett a pozitív kapcsolat [36]. Mikroszinten vagy üzleti egységek szintjén az ERM értéket generál, azaz minden lényeges kockázat „tulajdonban van”, makro- vagy vállalati szinten a felső vezetés az ERM segítségével azonosítani, mérni és elfogadható szintre tudja korlátozni a vállalat nettó kitettségét [37]. A vállalat túlélését befolyásolja a vállalatirányítási megfelelés, a vezetés és a kockázati kultúra [38]. A kockázatkezelés elengedhetetlen a vállalati sikerhez, és fontos a vállalati hírnévkezelés szempontjából [39].

3.2. Vállalati kockázatok és kockázatkezelés

A kockázatok elleni védelem az egész vállalat működését áthatja, ebből kifolyólag a kapcsolódó kockázatokhoz kötődően a szükséges és elégséges biztonsági háló az egész vállalati működésben is megjelenik. A biztonság kérdésköre stratégiai jelentőségű, ennek részterületei: személy- és vagyonvédelem, az adat-, információ- és információtechnológiai védelem, az integritási, korrupciós és egyéb humán kockázatok kezelése, az üzletbiztonság, az üzletmenet-folytonosság és a váratlan havária események (kockázatok) kezelése, illetve azok elhárítása [40].

A potenciális kockázatok belső -, és külső kockázatok formájában vannak jelen. Külső kockázatok a jogszabályi kockázatok, országkockázat, hitel-/kamat-/árfolyamkockázatok, beszállítói/partner kockázat, ügyfélkockázatok, természeti-, környezeti kockázat, biztosítási kockázatok [40].

A belső kockázatok a szervezeti működésre vezethetőek vissza, ide tartoznak a berendezések meghibásodásával kapcsolatos technológiai-, vagyoni-, gazdálkodási-, likviditási- és adósságkockázatok, reputációs kockázatok, információs technológia kockázatok, HR-, etikai és korrupciós kockázatok is [40]. A kockázati attitűdök nem egységesek egyes országokban és országon belül [41].

A működési kockázatok jellemzően technológiai, és emberi tényezőkhöz köthetőek. A működési kockázatoknak pénzügyi következményeik vannak, melyek mérsékelhetők a kockázatkezelési politikával (például biztosítások kötése főleg tiszta kockázatra, egy természeti csapásra). A kríziskezelés, és az üzletmenetfolytonosság kiemelt területeket jelentenek. A kritikus üzleti folyamatok helyreállításához szükséges idő minimalizálása kulcsfontosságú. A kockázati tényezők kihatnak egymásra, ami egyik oldalról működési kockázat, a másik oldalról pénzügyi kockázatként megjelenik. A stratégiai kockázatok megjelennek a működési kockázatokban, és viszont. A COVID-19 pandémia működési kockázatnak indult, azonban stratégiai kockázattá vált. A pandémia formájában elháríthatatlan külső kockázat következett be, melynek hatása elsőként az operatív folyamatok működésében jelentkezett, majd magát az üzletmenetfolytonosság biztosítását tette bizonytalanná, és többek között a működési modell átalakítását is sok esetben szükségessé tette [S5]. A pandémiás kockázat ezáltal stratégiai kockázattá vált [S7]. A pandémiához kapcsolódóan megfigyelhető volt, hogy voltak vállalatok, melyek nem tudták fenntartani működésüket, és azokra a vállalatokra, melyek működőképesek maradtak jellemző volt, hogy adaptálódtak a körülményekhez, többek között, ahol erre lehetőség volt, átálltak az otthoni munkavégzésre, vagy átkerült a fókusz az elektronikus kereskedelmi csatornákra, melyhez megfelelő technológiai apparátus biztosítására volt szükség [S5; S7]. Ez utóbbi a digitális átalakulással kapcsolatos stratégiai döntések meghozatalát is megkövetelte, melynek a kockázati kitettségre is hatása volt [S7]. Az IKT és az emberi kockázatok tipikusan működési kockázatok, ugyanakkor integrált szemléletben a vállalati stratégiához kapcsolódó stratégiai területek. A digitális átalakulások világában a technológiai és a humán erőforrás területek érintettsége meghatározó, és kulcs stratégiai területekké váltak.

A kockázatkezelés hagyományos és vállalati szintű kezelése között határozott különbség van [42]. A két kockázatkezelési megközelítés közötti alapvető különbségeket a KPMG LLP. foglalta össze, és bemutatta, hogy a hagyományos kockázatkezelési megközelítés leginkább a kockázatok kezelésének folyamatos és reaktív rendszere [43].

A vállalati kockázatkezelés célja, hogy egy olyan keretrendszert teremtsen, amely képes biztosítani, hogy a vállalat a kockázatokat, és bizonytalanságokat kezelni tudja [1]. A kockázatkezelés többet jelent a vállalat kockázati kitettségének minimalizálásánál, és célja a vállalat vagy portfólió értékének maximalizálása a különböző kockázatokhoz kapcsolódó költségek csökkentésével [1].

Iványos János „a kockázatkezelés és a kontroll nem ugyanannak „az éremnek a két oldalát" jelentik" [44; p.7] állítása elgondolkodtató, kérdés, hogyan értelmezzük az érem két oldalát. Maga a kockázatkezelés és a kontroll közötti kapcsolat és logikai összefüggés véleményem szerint vitathatatlan, és a kettő között átjárhatóság van. A kockázatkezelés a szervezet minden szintjén megjelenő döntési folyamatok részét képező vezetői feladat, a kontrollok kialakítása és működtetése a vezetői döntések megfelelő végrehajtását szolgálja [44]. A vállalat operatív szintjén kontrollokat végrehajtó munkavállalók a kontrolltevékenységben betöltött szerepük révén a vállalati biztonsági célkitűzések megvalósításához járulnak hozzá. A kontroll tevékenységet végrehajtó értéket állít elő, mely visszacsatol a biztonsági folyamatok megfelelő teljesítményére, ezáltal a kockázatkezelési folyamat működésére. A magam részéről a kockázatkezelés és kontrollok közötti kapcsolatok hangsúlyozását javaslom.

A kockázatkezelés folyamata a vállalatok stratégiai fejlesztésének része, és azt a legmagasabb szinten kell meghatározni. Az ISO 31000 kockázatkezelés sztenderd egyik alapelve azt mondja, „a kockázatkezelés értéket teremt és őriz" [179]. Az integrált kockázatkezelés értelmében valamennyi kockázatot értékelni, kontrollálni, és monitorozni kell a vállalat kitettségének megfelelően [1]. Az ISO 31000 kockázatkezelési szabvány a kockázatot a bizonytalanság vállalati célokra való pozitív és/vagy negatív hatásaként értelmezi [44; 179], mindez rámutat arra, hogy a kockázatkezelés a vállalati stratégiai célok szintjén integráltan kezelendő. A kockázatkezelés integrálódik, beágyazódik a szervezet irányítási rendszerébe, szervezeti és működési folyamataiba [44]. A vállalati szintű kockázatkezelés során a kockázatok az üzleti stratégia kontextusába vannak helyezve, és „a kockázat mindenki felelőssége". Ezzel a megközelítés szigorúan elhatárolódik attól, hogy a szervezet tagjai arra hivatkozzanak, hogy mindez nem tartozik az ő felelősségi körükbe [43].

Szabványok és keretrendszerek

A szabványok, például ISO 31000 kockázatkezelési szabvány erőteljesen befolyásolják a kockázat, és biztonság területet, annak ellenére, hogy erőteljes kritikai hangok kérdőjelezik meg a minőségüket [45; 179]. Az ISO 31000 szabvány értelmében a kockázatkezelés célja értékteremtés és annak védelme. Az integrált kockázatkezelés ISO 31000 szerinti megvalósítása segíti a vállalatot céljai elérésében, és a reziliencia megteremtésében negatív hatások esetén [46; 179].

A szabványok elősegítik a transzparenciát, az összehasonlíthatóságot, és ezáltal a költséghatékonyabb ellenőrzést is. A szabványokban a hatályuk alá tartozó terület pontosan le van fektetve, ezáltal beazonosítható, hogy mire vonatkozik, és mire nem. Nem elvárható, hogy taxatív megoldást kínáló lexikont keressünk benne, hanem inkább egy jógyakorlatokat tartalmazó keretrendszerként érdemes rájuk tekinteni, amit adaptálni kell.

A COSO (Committee of Sponsoring Organizations') belső kontroll integrált keretrendszer a belső kontrollok vonatkozásában, és a COBIT keretrendszer (COBIT – Control Objectives for Information and Related Technologies) IT-specifikusan használható eredményesen a releváns vállalati kontrollrendszer kialakítása és működtetése során [47; 48; 49; 50]. A belső kontrollrendszer a kontrollkörnyezet, kockázatértékelés, kontrollok, információs és kommunikációs folyamat és monitoring elemeiből épül fel [47; 48].

A Vállalati kockázatkezelés (ERM) a kockázatokat az üzleti folyamatok kontextusába helyezi; mindenkinek van valamilyen felelőssége a szervezeten belül, és a végső felelős az ügyvezető/CEO [28; 43]. A COSO vállalati kockázatkezelés integrált keretrendszere (COSO Enterprise Risk Management – Integrated Framework) fókuszba helyezi a kockázatkezelést. A COSO ERM keretrendszer a kontrollkörnyezet, célok felállítása, események azonosítása, kockázatértékelés, kockázati válaszok, kontrolltevékenységek, információ és kommunikáció, és monitoring elemeket, komponenseket tartalmazza [28]. A COSO keretrendszer a vállalati célkitűzéseket stratégiai, operatív, riporting és megfelelési célkitűzések szerint értelmezi. A COSO keretrendszer a belső kontrollrendszer integritását mutatja be, és szemlélteti, hogy az üzleti célok - stratégiai, operatív, riporting és megfelelési célok – érdekében milyen kontrollfolyamatok valósulnak meg a különféle vállalati szinteken [28]. A COSO-kocka ezt a keretrendszert vizuálisan jeleníti meg, mely jól illusztrálja az egyes dimenziók, azaz a célkitűzések, komponensek és vállalati szintek közötti kapcsolatokat.

Információbiztonsági kockázatok és kockázatkezelés

Az információbiztonság a vállalati biztonság része. A mai vállalatok a folyamatos valós idejű információcsere korában működnek. Az információ a döntéshozatali folyamat alapja, a hatékony verseny megköveteli a szervezetektől az információkhoz való hozzáférést és az információ terjesztését az érintettek között [51]. Az IKT rendszerek szerepe a vállalati üzleti célok, vezetői döntéshozatal, valamint a stratégiai versenyelőny támogatása [52]. Az informatikai rendszerek a vállalati folyamatokról adnak állapotjelentést, és a vállalati stratégia mindennapi megnyilvánulásaiként is értelmezhetőek. Az IKT technológiák hatékony alkalmazása értéket állít elő, hozzájárul az üzleti célokhoz, és ezáltal a hosszú távú vállalati sikerességhez.

Az információs technológia annak számos előnye mellett valójában fő problématerületté is vált az információbiztonsági kérdések kapcsán a technológiára támaszkodó szervezetek számára [53]. A biztonsággal kapcsolatos feladatok nagyon összetettek lehetnek [54]. Szükséges a bevált gyakorlatok azonosítása [55; 56; 57], annál is inkább, mivel a vállalatok továbbra sem tanulnak a biztonsági incidensekből [58]. A számítógépes információs rendszerek biztonsága – amit általában kiberbiztonságnak is neveznek – fontos működési kérdés szinte minden egyes szervezet esetében [59].

Az információbiztonsági tényezők modellje a döntéshozók számára azt mutatja, hogy vannak olyan kulcsfontosságú biztonsági indikátorok, amelyek közvetlenül befolyásolják a szervezet biztonsági állapotát, míg más mutatók csak közvetetten kapcsolódnak egymáshoz. Az azonosított kulcsfontosságú biztonsági mutatók: Fizikai biztonság” (a gyakorlatban: épületek, irodák, szerverek és hardverek fizikai védelme), „Sebezhetőség” (a gyakorlatban: a rendszereken és szoftvereken belüli ismert sérülékenységek), „Hozzáférés-szabályozás” (a gyakorlatban: a rendszerekhez, alkalmazásokhoz, adatokhoz, infrastruktúrához való hozzáférés kezelése és szabályozása), „Infrastruktúra” (a gyakorlatban: az összes rendszer, szoftver és a köztük lévő kapcsolatok ismerete, és hogy azok védettek-e vagy sem; az összes rendelkezésre álló rendszer „erősítése”, fenyegetési modellek készítése és az infrastruktúra biztosítása minden hálózati rétegben), „Tudatosság” (a gyakorlatban: minden olyan téma, amely az embereket érinti, és nem kezelhető technológiával) [60]. Itt érdemes megemlíteni a „védelem mint falak” megközelítésű úgynevezett Kastély modellt is a kiberbiztonságról, miszerint „belül” biztonságos és „kívül” veszélyes. Ez a megközelítés ugyanis egy vakfoltot hagy maga után. A tendencia az, hogy a vállalatok egyre inkább felnyitják falaikat és „szivárgóbbá” teszik az átjáróikat, és külső falakat a technológiai fejlődés egyre inkább tönkreteszi. Ráadásul, a millenniumi generáció hajlamos keverni a szakmai és a magánéletet.

Mindezek a tényezők a kiberbiztonság új megközelítését teszik szükségessé [61]. A vállalati folyamatok tervezése és működése során biztosítani kell azt, hogy a vállalat ellenálló tudjon maradni az IKT biztonsági kihívásokkal szemben. Annál is inkább, mert a külső auditorok is több kockázatot azonosítanak, ezáltal több audit díj merül fel a kiberbiztonsági támadást elszenvedett vállalatok esetében [62].

Az informatikai kockázatok kulcskockázatok a vállalati biztonság szempontjából, melyek kezeléséhez speciális kockázatkezelési keretrendszerek nyújtanak támaszt. A keretrendszerek megjelenítik azt, hogy a vállalati kockázatkezelési folyamatok egyes elemei összekapcsolódnak, azok integráltan kezelendők, beleértve az IKT folyamatokat.

A COSO keretrendszernek is része az információ és kommunikáció, azonban mint IT folyamatspecifikus funkcionális területre vonatkozóan több szabvány és ajánlás is alkalmazható, mint a CObIT az IT irányítás- és menedzsment keretrendszere és a NIST 800-53-as amerikai biztonsági és adatvédelmi ellenőrzések dokumentum [50; 63]. Az információbiztonság területére vonatkozik az ISO/IEC 27000 információbiztonság-irányítás szabványcsalád [172]. Az információbiztonság kockázatmenedzsmenttel foglalkozó szabványa az ISO/IEC 27005 szabvány, mely információbiztonsági kockázatokra vonatkozik [176]. A CObIT alkalmazása többek között az IT kockázatkezelés megvalósítását segíti. A CObIT 5 alapelvek és annak megvalósítását segítő tényezői lehetővé teszik a szervezet számára, hogy IT beruházásait a céljaival összhangba hozza, és a beruházásokon keresztül realizálni tudja azok értékét. Az alapelvek – az érintettek igényeinek kielégítése; a vállalat teljeskörű lefedése; egységes, integrált keretrendszer alkalmazása; átfogó, holisztikus megközelítés megvalósítása, és az irányítás (governance) és menedzsment szeparálása – hozzájárulnak, hogy a vállalat az IT irányításnak és a menedzsmentnek holisztikus keretrendszerét megteremthesse. Mindennek a megvalósítását az elvek, szabályok és keretrendszerek, folyamatok, szervezeti struktúrák, egyéni és vállalati kultúra, etika és viselkedés, információ, szolgáltatások, infrastruktúra és alkalmazások, valamint humán erőforrás, képességek és készségek teszik lehetővé [49]. A CObIT 5 frissített változata, a CObIT 2019 hat alapelve átstrukturálva és pontosítva jeleníti meg az eredeti öt alapelvet: értékteremtés az érintettek számára; holisztikus megközelítés, dinamikus irányítási rendszer, az irányítás és menedzsment külön funkciók; vállalati igényekre szabott, és teljeskörű (end-to-end) irányítási rendszer [64].

Az információbiztonsági fenyegetések csökkentésének kulcsfontosságú eszköze az információbiztonsági politikák létrehozása és betartatása [65]. Az információbiztonsági politika egy belső dokumentum, amely biztosítja az információs eszközök és az információtechnológiai biztonságát egy speciális eljárással, hogy támogassa a szervezet célkitűzéseit [66].

Az információbiztonsági politika magában foglalja az információbiztonsági fenyegetések felmérését is, amely az információbiztonság területén a döntéshozók egyik legfontosabb kötelezettsége [67], és figyelembe kell vennie az érintettek visszajelzéseit az alkalmazott biztonsági módszerekről [68].

A folyamatos biztonsági incidensek fő oka az, hogy az alkalmazottak nem tartják be a vállalati információbiztonsági politikát [69]. A vállalatok információbiztonsági képzés során fel tudják hívni a munkavállalók figyelmét az IKT-biztonsággal kapcsolatos jógyakorlataira [70]. A munkavállalók információbiztonsági magatartásának fejlesztése szempontjából fontos a képzés [71]. Jelenleg az információbiztonságot illetően a munkavállalói magatartás és a társadalmi tényezők ugyanolyan fontosak, mint a vállalat fizikai és logikai erőforrásai [72].

A digitális átalakuláshoz kapcsolódóan górcső alá kell venni a kockázatokat, és azok kezelését. A COVID-19 pandémia alatt a digitális átalakulás az üzletmenet-folytonosság biztosításának feltételévé vált. A digitális átalakulással összefüggő projektkockázatok kezelése kulcsfontosságú, amelyekre összpontosítani kell. A technológiai innovációk változtatásokat generálnak a vállalati folyamatokban, a folyamatok változásai az ellenőrzések, kontrollok újraértékelését követelik meg. A digitális átalakulással járó stratégiai projektek, változási, illetve modernizálási törekvések a vállalatok folyamatait és kontrollkörnyezetét jelentősen megváltoztatják. A digitális átalakulással összefüggésben a biztonsági aspektus kezelése az átalakulási projektek sikere szempontjából is meghatározó. A használt szoftverek biztonsági aspektusainak vizsgálata, és kezelése elengedhetetlen. Az elsődleges védelmet az jelenti, hogy a szoftverfejlesztők a különféle fejlesztési és tervezési hibákat elkerülik [73]. Az információs rendszerek védelme óriási szereppel bír a digitális világban.

3.3. Hálózatok vállalati kontextusban

A mai agilis üzleti környezethez való adaptációhoz szorosan kapcsolódik a hálózatos szervezeti felépítés felé történő elmozdulás és a vállalati folyamatok folyamatcentrikus átrendezése. A vállalati folyamatok folyamatcentrikus szemlélete és kezelése révén folyamatláncok jelennek meg, amelyek az alkotó folyamatok hálózataként értelmezhetők. A folyamatokhoz kontroll és ellenőrzési tevékenységeket kell rendelni, melyek sikeres megvalósulása a kívánt biztonsági szint elérését segíti.

A huszadik századi irányadó vállalati struktúra, a vállalati fastruktúra háttérbe szorul, és elmozdulás tapasztalható a horizontális, hálózatos szerkezet irányába. A vállalati fastruktúra szerint a vállalat szerkezete egy feje tetejére állított fához hasonló hálózatra épült, ahol a vezérigazgató a fa gyökere, a gyökértől távolodva csökken a felelősség. A fa modell merev, és nem képes a változásokhoz alkalmazkodni. A változó üzleti környezetben a dinamikus, hálózatos szervezeti felépítés válik szükségessé. Megnő többek között a munkacsoportok, munkaerőkölcsönzés szerepe, sok helyen megszüntetik a középvezetői állásokat, és kisegítőket emelnek ki fő felelőssé [74].

„Hálózatok mindenhol vannak" [25]. A vállalatok maguk is hálózati működésben gondolkodnak. A vállalati működés során jellemző a hálózati tagság. Vállalkozók körében végzett felmérés szerint a hálózatóké a jövő [75]. „Fenntartható hálózati csomópontként csak az tud fennmaradni, akinek az elosztás során követett méltányosságában a többi hálózati szereplő megbízik" [76; p.291]. „A vállalatok soha nem egyedül élik életüket" [74; p.219]. Kiemelkedő fontosságú a felsővezetők kapcsolata a többi vállalattal, a más szervezetektől való tanulás, mely kapcsolatokban a hálózatosság alapvető szerephez jut [74]. Az üzleti döntéshozó hálózati ember [77].

A hálózatok több vonatkozásban adaptálhatók a vállalati folyamatokra az üzleti életben, és több szinten is megjelennek a vállalatok „belső" és „külső" működésében. A hálózatok létrejönnek a teljes vállalatra és a vállalati folyamatokra vonatkozóan. Hálózatot alkotnak a vállalatok és vevők, banki utalások, szállítási rendszerek, a vállalati folyamatok, a folyamatot képező folyamatlépések, de egy projekt is. A vállalatok belső struktúrája is szorosan kapcsolódik a hálózatokhoz. A vállalatközi kommunikáció és a tranzakciók során a vállalat az üzleti partnerekhez, vevőhöz, beszállítókhoz, illetve szabályozó testületekhez is kapcsolódik. Mindez a vállalat kapcsolati hálózatát írja le.

A vállalatok üzleti modellje a küldetés megvalósítására kiválasztott tevékenységek hálóját takarja, annak konkretizálása [78]. Az üzleti modell tevékenységeken, és azok kapcsolatain keresztül teremt értéket az érintetteknek, kiemelten a fogyasztóknak és a tulajdonosoknak [78]. A vállalatok biztonsági hálója szorosan kötődik ezekhez a tevékenységekhez, és kapcsolatokhoz. A vállalati folyamatok az emberi tényező és az információs és kommunikációs technológiai (IKT) rendszerek „együttműködése" által valósulnak meg. A vállalati folyamatok egymáshoz kapcsolódó lépések láncolatai, nélkülözhetetlen a különféle folyamatok összekapcsolódása. Szükséges látni a folyamatok közötti összefüggéseket, mely segíthet kiküszöbölni bizonyos hibákat, illetve csökkenti bizonyos biztonsági események előfordulásának valószínűségét.

A kívánt biztonsági szint elérését kontrolltevékenységek (röviden kontrollok) működtetése segíti elő, amelyek biztosítják, hogy a folyamat hibamentesen, illetve adott elfogadható tűréshatáron belüli hibaszázalékkal működik.

A vállalat működését meghatározó folyamatok az egymással kapcsolatban lévő folyamatlépésekkel írhatók le, melyeket vizuálisan a folyamatlépésekről készített folyamattérképek ábrázolnak. A vállalati folyamatok hierarchiája a stratégiaitól, a taktikai és az operatív szintek irányába halad [75; 78; 79; 80; 81; 82; 83]. Az egyes szintekhez szabályzatok, folyamatleírások kapcsolódnak, melyeknek megfelelő kezelése a vállalat ellenálló képességét, és integritását erősíti, valamint alapját jelentik a sikeres változáskezelésnek, és külső minősítéseknek. Mindemellett ott van a „vezetőség hangja" és a vállalati kultúra „lágy" eleme, azaz a folyamatok mögött lévő ember is. A vállalati folyamatok, mint a beszerzés, értékesítés, vagy könyvvitel egymáshoz kapcsolódó folyamatlépések hálózataként is értelmezhetők. A számítástechnikai hálózattopológiával párhuzamot vonva a számítástechnikai hálózatok kapcsán ismert, hogy az egymásbaágyazottság jellegzetes hálózati topológia formájában jelentkezik, miszerint a főhálózat elemei maguk is komplex alhálózatok, és az alhálózatok felől a működési mechanizmus, míg a főhálózatok felől a működés célja ismerhető meg [76]. Az egymásbaágyazottság ezen jellegzetes hálózati topológiája jól illeszkedik a vállalati folyamatok, és stratégia rendszerére. Ugyanez mondható el a vállalati biztonsági rendszerről is.

A vállalati biztonsági rendszer szintjei az első, második, és harmadik vonal modellje [84] mentén is értelmezhetők, melyet korábban az első, második, és harmadik védelmi vonal modell volt [85]. Az IIA (IIA – The Institute of Internal Auditors) 2013-ban definiálta az effektív kockázatkezelés és kontroll három védelmi vonal modelljét. A 2020-ban kiadott modell a modern kockázatkezelés és irányítás területén bekövetkezett változásokra reflektál [86]. A vállalati vonalak a vállalati működés valamennyi szintjén megjelennek. Az első vonal maga az üzleti folyamatokba ágyazott kockázatkezelés. Az üzleti folyamatok vezetőinek felelősségi körébe tartozik a hatáskörükbe tartozó vállalati folyamatok kockázatainak azonosítása, megfelelő kezelése és kontrollok működtetése. Az első vonal az operatív folyamatok szintjén nyújt aktív védelmet. A második vonal szintén a vállalaton belüli védelmi háló eleme, mely elkülönül az üzleti folyamatoktól, kockázatokkal kapcsolatos ügyekben szakértői közreműködés, támogatás és nyomon követés szerepkörei vannak. A harmadik vonal a menedzsment felelősségi körétől független belső ellenőrzés formájában jelenik meg, és nyújt független bizonyosságot. Ezen felül szerepel a külső bizonyosság megszerzése külső audit formájában. Az erős irányítás és kockázatkezelés megteremtése érdekében a kulcs szervezeti szereplők együtt dolgoznak [87].

A belső kontrollrendszer egyes elemei – a kontrollkörnyezet, kockázatértékelés, kontrollok, információs és kommunikációs folyamat és monitoring [47; 48] – a szervezetet átfogó, hálózatszerű struktúrában jelennek meg. A COSO-kocka megjeleníti a stratégiai, megfelelési, riporting és operatív kockázatokat, a vállalati belső kontrollrendszer elemeit, illetve az egyes szervezeti egységeket. A COSO-kocka rámutat az egyes elemei közötti kapcsolatokra, és egyúttal szemlélteti a belső kontrollrendszer komplexitását (3.2. fejezet). A COSO-kocka szerkezete és logikai összefüggései megerősítik, hogy a belső kontrollrendszerről érdemes hálózatkutatási szemszögből gondolkodni, és hálózati kapcsolatokat értelmezni.

A vállalati védelmi háló pilléreit fedik le a GRC rendszerek: irányítás (governance), kockázatkezelés (risk), és megfelelés (compliance). A GRC rövidítést 2003-ban használták először, és az első lektorált tudományos kiadvány 2007-ben jelent meg [88]. Az irányítás, stratégia, kockázatkezelés, audit, jog, megfelelés, információs technológia, etika és vállalati társadalmi felelősségvállalás, minőségirányítás, valamint a humán tőke és kultúra mind olyan területek, melyek a GRC-hoz kapcsolódó folyamatokhoz tartoznak [89]. Ezek a folyamatok a szervezetet hozzásegítik céljai eléréséhez, igazodva annak határaihoz [89].

A hálózattudomány matematikai módszere és a hálózati modellezés

A hálózattudomány eszköze a gráfelmélet, melyet a hálózattudomány matematikai módszerként felhasznál. A gráfelmélet gyökerei az Euler-féle königsbergi hidak problémájához nyúlnak vissza, mely a következő volt: hét híd ívelt át a városon átmenő folyón, a folyó két szigetét is érintve. A kérdés az volt, hogy végig lehet-e menni az összes hídon úgy, hogy minden hídon csak egyszer mennek át, és visszatérnek a kiindulópontba. A gráf csúcsai a szárazföldi részeken találhatók, míg a hidak az élek. Euler bizonyította, hogy ez lehetetlen, mert a gráfban egy pontnak öt, és három pontnak három a fokszáma. Akkor és csak akkor létezne megoldás, ha minden csomópont fokszáma páros lenne [90].

Egy gráfot szimbólumok két halmaza definiál, ezek elemeit csúcsoknak, illetve éleknek hívjuk. Az él egy csúcspontokból álló rendezett pár, amely megadja a két csúcspont közötti mozgás vagy áramlás lehetséges irányát [91]. A hálózatok megváltoznak, ha a kapcsolatok vagy a csomópontok módosulnak [92]. A rendszerek és folyamatok modellezése során a rendszer elemei, illetve a folyamat állomásai közötti kapcsolat létezésének feltárása a legjelentősebb kérdés [166].

A véletlen hálózatok modelljeit Erdős és Rényi (1959; 1960) [93; 94], illetve velük egyidejűleg és függetlenül Edgar Gilbert (1959) állították fel [95]. Az Erdős–Rényi modellként is ismert (1959) modell a hálózatok véletlenszerűségén alapul.

Az Erdős–Rényi modell szerint minden él p valószínűséggel következik be, nagyságrendileg ugyanannyi él tartozik a csúcsokhoz, azaz körülbelül ugyanannyi a fokszáma. A véletlen hálózatok fokszámeloszlása egy haranggörbét követ.

Az emberi kapcsolatok esetében tapasztalható, hogy egy-egy ember nagy ismeretségi körrel rendelkezik, míg mások szűk ismeretségi körrel rendelkeznek, ennélfogva az Erdős–Rényi modell szerinti Poisson-eloszlással nem írhatók le. Már Karinthy Frigyes is végig vezette a „kis világ" gondolatát 1929-es Láncszemek című novellájában [74].

A Barabási-Albert-modell a skálafüggetlen hálózatok modellje. A skálafüggetlen hálózatok fokszámeloszlása hatványfüggvény szerinti eloszlást követ, mely tulajdonság két általános mechanizmus következménye: az egyik, hogy a hálózatok folyamatosan bővülnek új csúcsok hozzáadásával, valamint a másik, hogy az új csúcsok elsősorban olyan helyekhez kapcsolódnak, amelyek már sok kapcsolattal rendelkeznek [96]. „A legtöbb nagy hibatűrő képességgel bíró rendszernek közös tulajdonsága, hogy működőképességét egy bonyolult, szorosan összefüggő hálózat alkotja" [74]. A skálafüggetlen hálózatok jellemzője a hibatűrő képesség és a sebezhetőség. A műszaki hibák például nem tesznek különbséget csomópontok között, azok egyenlő valószínűséggel hatnak minden csomópontra. A támadásokra azonban nagyfokú az érzékenység [74].

A fentiek alapján a **H1** és **H2** hipotéziseket fogalmaztam meg:
H1: feltételezem, hogy a belső kontrollrendszer hálózatként értelmezhető. A hálózattudomány segítségével a belső kontroll folyamatok vállalatot behálózó jellege igazolható.

H2: feltételezem, hogy a belső kontrollhálózat működése szempontjából azonosítható olyan tényező, amely a hálózat működését biztonsági szempontból döntően meghatározza.

3.4. Kontrolling rendszerek szerepe

A vállalati hálózatok és biztonsági hálózat feltérképezéskor a kontrolling funkció is központi szerepet kap. „A kontrolling a múlt hibáit a jövőépítés szempontjából vizsgálja" [97; p.13]. A stratégia megvalósítása feletti ellenőrzés információs alapját a korszerűen szervezett vállalatnál a kontrolling rendszer jelenti [78].

A tudatos szervezetirányítás a kontrolling szabályzókör – a tervezés, az irányítás (mérés, elemzés) és a visszacsatolás - mentén történik. A kontrolling szabályozókör érvényesül a stratégiai, és operatív irányítás szintjén is [98]. Megkülönböztetünk stratégiai-, menedzsment-, és feladatkontrollt. A klasszikus vezetői funkciók között tárgyalt kontrollnak leginkább a menedzsmentkontroll felel meg.

A menedzsmentkontroll a stratégiai kontrollnál lényegesen rövidebb (általában éves) időtávra vonatkozik, és főként számszerűsített, pénzügyi jellegű standardok használata jellemzi [80]. A menedzsmentkontroll folyamaton keresztül a vezetők úgy befolyásolják a szervezet tagjainak magatartását, hogy az a stratégiájának megvalósítását biztosítsa [99]. „A kontrolling - az információ menedzsment szerinti vezetési funkció - a vállalati események tervezésére, ellenőrzésére, elemzésére, és irányítására szolgáló vezetési eszköz” [97; p.52]. A kontrolling funkciónak a biztonsági hálóban fontos szerepe van, benne van a szervezeti tanulás képessége, mely hosszabb távon jelentős hozzáadott értéket jelenthet, és a biztonság eszközeként is szerepe van.

A kontrolling rendszerekhez kapcsolódóan meghatározó a PDCA ciklus, mely módszertani eszközként és meghatározó folyamatos fejlesztési metódusként az ellenőrzési rendszerek mögött áll, és azok működését lényegében meghatározza. A PDCA ciklus szisztematikus és tartalmi végrehajtása a kulcs a folyamatos fejlesztések, és teljesítménynövekedés mögött. A kontrolling rendszerek lehetővé teszik a szervezet tevékenységének irányítását és ellenőrzését a szervezeti céloknak megfelelően. Anthony a szervezeti tervezést és irányítást stratégiai tervezésre, menedzsmentkontrollra és operatív ellenőrzésre szegmentálta [100]. Ezek a folyamatok a szervezeti hierarchiához és a megfelelő vezetési szintekhez kapcsolódnak [101]. Anthony munkája mérföldkő volt a menedzsmentkontrollban, de idővel kritizálták például szűk látásmódja miatt, amiért a pénzügyi és számviteli alapú kontrollokra összpontosított, valamint amiatt, hogy a menedzsmentkontrollt elválasztotta a stratégiai és az operatív kontrolltól [101].

Kiegyensúlyozott mutatószámrendszer – Balanced Scorecard (BSC)

A dinamikus, folyamatosan változó üzleti környezet igényeinek kielégítéséhez dinamikus kontrolling eszközökre van szükség, mint például a Balanced Scorecard, amely a pénzügyi és nem pénzügyi teljesítménymutatók kombinációját kínáló menedzsmentkontroll és stratégiai kommunikációs eszköz [102]. A BSC egy stratégiai teljesítményértékelési módszer, amely négy perspektívát ragad meg: a vevőt, azaz hogyan látnak minket a vevők; belső, azaz miben kell jeleskednünk; innováció és tanulás, azaz a fejlesztés és az értékteremtés folytatható; és pénzügyi, azaz hogyan látnak bennünket a részvényesek. A BSC a legkritikusabb mérőszámokra összpontosít, és minimalizálja az információs túlterheltséget a korlátozott számú mérőszám miatt [103]. A kiegyensúlyozott mutatószámrendszer négy perspektívája összefügg, és a stratégiából kell levezetni.

A perspektívák összefüggenek egymással, ebből fakadóan ezeket a kapcsolatokat érdemes összefüggésükben kezelni. Például a folyamatos fejlesztés az innováció egy részhalmaza; a kapcsolódó projektek a bemeneti, feldolgozási és kimeneti oldalon a pénzügyi tervhez kapcsolódnak: a folyamatos fejlesztési (CI – continuous improvement) projektek általában olyan erőforrásokat igényelnek, mint az idő, pénz, melyek költségtényezők. A CI-projektek eredményeképp egyszerűbb folyamatok jönnek létre, amelyek kevesebb erőforrást igényelnek, beleértve az emberi erőforrásokat is. Mindez azt jelenti, hogy közvetlen anyagi haszon van, amely mérhető, és a forrásokat más feladatokra, munkákra lehet fordítani. A megváltozott folyamat a tanulási perspektívában is megjelenik. A fejlesztés egyúttal a belső folyamatok perspektívájába is beépül, amely a vevői perspektívában meghatározott módon értéket generál a vevők számára. Az egyes cselekvések hatásait minden oldalról értékelni kell. A fenti példa is illusztrálja az egyensúlyra való törekvést a kiegyensúlyozott eredménymutatóban. A perspektívák összekapcsoltsága jól reprezentálja a folyamatok, ideértve a biztonsági folyamatok vállalatot behálózó kontextusát.

A vevők szempontjából a kulcstényezőket a termékek és szolgáltatások ára, minősége, és rendelkezésre állása jelentik. A belső folyamat szempont azokra az intézkedésekre összpontosít, amelyek a legnagyobb hatással vannak a vevők elégedettségére. A pénzügyi intézkedések a tulajdonosi értékhez kapcsolódnak. A működés és annak pénzügyi aspektusai közötti kapcsolatot jól meg kell ragadni. A gyorsan változó világban a vállalat innovációs, fejlesztési és tanulási képessége olyan kritikus sikertényezővé vált, amely közvetlenül kapcsolódik a vállalat értékéhez. A meglévő termékeket, szolgáltatásokat és folyamatokat folyamatosan fejleszteni kell, és innovatívoknak kell lenniük az új termékek és szolgáltatások szükség szerinti bevezetéséhez. A vállalatoknak javítaniuk kell azon képességeiket, hogy értéket biztosítsanak a vevőknek és a tulajdonosoknak. A belső vállalati folyamatok szerves részévé kell tenni az innovatív változásokat, mely a folyamatokhoz kapcsolódó humán erőforrások megfelelő integrálását is szükségessé teszi. Az innováció és tanulás eredendően olyan vállalathoz kapcsolódik, amely folyamatosan értéket akar szállítani érdekelt feleinek [103; 104]. Az irányítási rendszerek is elősegítik ezt a hozzáállást. A szabványos irányítási rendszerek (3.5 fejezet) szintén a PDCA ciklusra épülnek, különböző területekre vonatkozóan segítik a tervezett eredmények elérését, mellyel biztonsági célokat is szolgálnak. Minden szabványos irányítási rendszerhez tartozik egy Innovációs és tanulási rész. A teljeskörű, végponttól végpontig terjedő folyamatokat folyamatosan fejleszteni kell**.** Az emberi erőforrások teljesítménycéljait illetően az embereket szükség szerint képezni, fejleszteni kell, és részt kell venniük az előírt képzéseken.

Folyamatbiztonság teljesítménymérése

A biztonság területe egyfajta egyedi funkció. Pragmatikusan, ha a biztonság jelen van, senki sem veszi észre a biztonsági erőfeszítéseket. Amennyiben azonban folyamathiba történik, akkor a biztonság szerepe a fókuszba kerül.

A folyamatbiztonság teljesítménymérése olyan egyedi gondolkodásmódot igényel, amely úgy tervezi meg és elemezi a vonatkozó számadatokat, hogy azok mutassák a folyamatban és a biztonsági erőfeszítésekben a tényleges és potenciális hiányosságokat, valamint a biztonság területén elért eredményeket. Ennek azonban az a feltétele, hogy megfelelően legyenek megtervezve, és illeszkedjenek a vállalati folyamatokhoz. A folyamatbiztonság a mögöttes biztonsági folyamatokon alapul, amelyek a vonatkozó biztonsági szabályzatokra és eljárásokra, valamint a biztonsági kultúrára épülnek. A biztonsági folyamatok teljesítményének mérése alapvető információkat szolgáltat a felsővezetés számára a biztonsági folyamatok status quo-járól, és alapul szolgál a fókuszba helyezendő területek és a kapcsolódó intézkedési tervek meghatározásához. A megfelelő mérőszámok a stratégiai célkitűzésekhez kapcsolódnak.

3.5. Szabványos irányítási rendszerek

A vállalati célkitűzések megvalósulását segítik elő a szabványos irányítási rendszerek, mint például a Nemzetközi Szabványügyi Szervezet folyamatközpontú szabványai. A legelterjedtebb minőségirányítási sztenderd, az ISO 9001 szabvány [167] bevezetése keretet ad a vállalati folyamatok szervezettségének, és a belső működésnek, melyhez szinergiahatásként járulhat a vállalat külső piaci megítélésének erősítése. A minőségirányítási szabvány mára meglehetősen elterjedtté vált, annak tartalmi elemei fundamentálisak, lefektetik egy olyan gondolkodásmód alapjait, mely hosszú távon képes a vállalati célkitűzések, és folyamatok támogatására. Mindezzel párhuzamosan a minőségirányítási rendszer ma már szükséges, de nem elégséges feltétele a biztonságos működésnek [105]. A minőségirányítási szabvány szorosan kapcsolódik a többi irányítási rendszerszabványhoz. A szabványok hasonló struktúrája lehetővé teszi azok integrált bevezetését.

Az informatikai területre vonatkozóan az ISO/IEC 27001 az információbiztonsági irányítási rendszer (IBIR) szabvány, illetve ISO/IEC 27000-es szabványcsalád kiemelt jelentőséggel bírnak (például ISO/IEC 27001, ISO/IEC 27002) [172; 174; 175]. Az ISO/IEC 27001 az információbiztonságot szervezeti szinten holisztikusan közelíti meg, foglalkozik az emberekkel, technológiával, folyamatokkal és szabályzatokkal is. Mindez információt nyújt az ügyfelek és érdekelt felek számára arról, hogy a vállalat elkötelezett az információk bizalmas kezelése iránt.

A szabványok széles spektrumot fednek le. A vállalati specifikumoknak megfelelően javasolt a szabványok bevezetése. A szabványok alkalmazása egyik oldalról a belső folyamatokra gyakorolt kedvező hatásai miatt szükséges; másik oldalról az üzleti partnerek elvárása annak bizonytékául, hogy a működésük megfelelő normaszintet követ.

A szabványokat pozitív hozadékai ellenére, erős kritika is éri [106]. Mindazonáltal szükség van rájuk, akárcsak a nemzetközi számviteli sztenderdekre is. A szabványok szerinti működés az átlátható, és összehasonlítható működés alapjait fekteti le, mely egyúttal növeli az üzleti partnerbe vetett bizalmat. Mindez egy olyan egységes nyelvet jelent, mint a matematika, melyet, aki ismer, megért, és az komfortot, biztonságot ad. Továbbá, azáltal, hogy a szabványok szerinti működés a biztonságos működés megteremtését is szolgálják, a vállalati biztonsági háló szempontjából is meghatározó szereppel bírnak.

A szabványos irányítási rendszerekkel növelhető a vállalat teljesítménye. A különálló irányítási rendszerek integrálása egyre inkább előtérbe kerül és megvalósíthatóbbnak tűnik [107], mellyel további szinergia hatások érhetők el.[1] Az egységes platform révén átláthatóbbak a folyamatok, a felesleges átfedések kiküszöbölhetők, könnyebben kezelhetők és ellenőrizhetők, ezáltal könnyebb a döntéshozatal. Ennek azonban a feltétele a bevezetési projekt megfelelő megvalósítása. Az egyes irányítási rendszerre már tanúsított szervezetek is kihívásokkal nézhetnek szembe egy új irányítási rendszer bevezetésekor, és a sikeres megvalósításhoz megfelelő kompetenciára és elkötelezettségre van szükség [108].

A tanúsított irányítási rendszerek szilárd követelményeken alapulnak, amelyek stabillá és átláthatóvá teszik a rendszert, és segítenek csökkenteni a kockázati kitettséget. A tanúsított irányítási rendszerek továbbá erősíthetik az üzleti bizalmat, hiszen az irányítási rendszer működését külső, független tanúsító testület által kiadott tanúsítvány is igazolja. Emiatt a következő hipotézis fogalmazódott meg.

[1] Integrált irányítási rendszere működő példa a RÁBA Nyrt., mely minőség, környezeti, egészségvédelmi és biztonságtechnikai politikájának megvalósításhoz autóipari minőségirányítási rendszer, környezetirányítási rendszer és munkahelyi egészségvédelem és biztonság szabványnak megfelelő integrált irányítási rendszert vezetett be. (letöltve 2024.04.18.)

A fentiek alapján a **H3 és H4** hipotéziseket fogalmaztam meg:

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

H4: feltételezem, hogy az információbiztonsági irányítási rendszerek alkalmazhatók a folyamatbiztonság és a vállalati biztonsági szint növelésére. Az irányítási rendszerek tanúsítása biztosítékul szolgálhat a folyamatbiztonságról.

3.6. Következtetések

A vállalati biztonság a technológiai tényezők, az emberi tényező és a kapcsolódó vállalati folyamatok biztonságára épül. A változásokhoz való folyamatos alkalmazkodás a reziliencia képességét követeli meg.

A folyamatosan változó üzleti és kockázati környezetben szükséges a biztonságos vállalati működés érdekében, hogy a vállalat felkészült legyen az információs és kommunikációs technológiához köthető kockázatok kezelésére, beleértve az IKT kockázatok emberi oldalát, a vállalati működés szempontjából az emberi tényező potenciális hibaforrásként történő kezelését, az előre nem látható természeti események vagy pandémia hatásainak kezelését. A vállalati folyamatok hálózatában részt vevő emberi tényező központi szereppel bír a vállalati biztonsági hálóban. A humán kockázatok jelen vannak a vállalati folyamatokban, ennek megfelelően a humán kockázatok kezelése a vállalatbiztonság szempontjából döntő jelentőségű.

A vállalati biztonság az üzleti folyamatok működése, és sikere érdekében szükséges, ezért a biztonsági folyamatok teljesítményének ellenőrzése és mérése stratégiai kérdés. A szabványos irányítási rendszerek segítik az vállalati célkitűzések megvalósítását, és a biztonsági folyamatok támogatására alkalmasak. Érdemes kihasználni az irányítási rendszerekben rejlő szinergiákat, és egységes alapokra helyezni a folyamatok teljesítménymérését. Mindennek alapjául szolgálhat a szabványos irányítási rendszerek biztonsági aspektusaira épülő kiegyensúlyozott mutatószámrendszer.

4. A BIZTONSÁG HÁLÓZATI VIZSGÁLATA

A fejezetben a belső kontrollrendszer elemző vizsgálatához kapcsolódóan elvégzett vizsgálataim eredményeit mutatom be: a belső kontrollrendszer egészét holisztikusan (4.1. fejezet), és egy vállalati folyamatán keresztül analitikusan (4.2. fejezet) közelítem meg.

4.1. A belső kontrollrendszer tartalomelemzése

Kvalitatív kutatást végeztem a vállalatbiztonságot meghatározó kontrollok hálózati jellegének vizsgálatára a H1 hipotézishez kapcsolódóan. A következőkben az éves beszámolókat – úgymint AUDI vállalat (Audi AG Annual Report, 2020) [130], MERCEDES vállalat (Daimler Group Annual Report, 2020) [131], SUZUKI vállalat (Suzuki Annual Report, 2020) [132], OPEL vállalat (Groupe PSA Annual Report, 2019) [133] – a kapcsolódó főbb kutatási célok mentén értékelem. [2]

A kapcsolódó vállalati folyamatok ismertetése a vizsgált beszámolókban különböző szintű. A vizsgált vállalatok esetében közös az a digitális transzformációs folyamat, mely az iparágat jellemzi, és az meghatározó a vállalati stratégia, valamint kockázatkezelés szempontjából is.

4.1.1. A belső kontrollrendszer / Kontroll funkció megjelenése

A belső kontrollrendszer és kontroll funkció szabályzatok szintjén is megjelenik az éves beszámolóban. Az Audi és Mercedes esetében tételes megnevezésre került, hogy a COSO modellt követi a belső kontrollrendszer. A Suzuki és Opel éves beszámolója nem tartalmaz konkrét modellt. Ugyanakkor az Audi éves jelentésében kiemeli, hogy a kockázatkezelési architektúra szisztematikus strukturálása érdekében az Audi csoport követi a három védelmi vonal modellt. A három védelmi vonal kifejezés maga nem jelenik meg a többi vállalat éves beszámolójában, egyes elemei azonban fellelhetőek esetükben is különböző részletezettséggel (1. táblázat).

[2] Az adatrögzítő íveken az 1-5. táblázatokban feltüntetett oldalszámok az éves beszámolókban szereplő tényleges oldalszámok, mely eltér a pdf dokumentum fejlécén szereplő oldalszámtól.

1. táblázat A belső kontrollrendszer / Kontroll funkció megjelenése az éves beszámolóban (Forrás: az éves beszámolók alapján a szerző szerkesztése)

AUDI vállalat	MERCEDES vállalat	SUZUKI vállalat	OPEL vállalat
1. Hogyan jelenik meg a kontroll funkció a vállalat éves beszámolójában?			
- támogató pillér - vállalati célok, átláthatóság, kockázat, megfelelés, integritás biztosítása, tudatosság erősítése - megfelelő és stabil folyamatok biztosítása - belső kontrollrendszer (ICS) kiterjedt felülvizsgálata és kiterjesztése. - kockázatkezelés (RMS) kiegészül a belső kontrollrendszerrel - központi GRC funkcióhoz szorosan kapcsolódik az RMS/ICS - kombinált riport az Igazgatótanács, Felügyelő Bizottság, Audit Bizottság számára (RMS, ICS, CMS- megfelelési rendszer) (pp. 71, 121-122)	- új vállalati struktúra - Daimler AG operatív és stratégiai menedzsment holding --> kontrolling, irányítási - és igazgatási funkciók, szolgáltatások a vállalatcsoport tagjai számára - központi szinten Pénzügy és Kontrolling, HR, Integritás és Jog (pp. 26, 37)	- megfelelési és kockázatkezelési rendszerek teljeskörű felülvizsgálata - valamennyi működési terület lefedése - belső kontrollrendszer erősítése (pp. 2-3)	- belső kontroll -, és kockázatkezelő funkciókért a menedzsment felel - pénzügyi beszámolási folyamat monitorozása, valamint a belső kontroll, - és kockázatkezelési rendszerek hatékonysága, illetve ahol releváns, a belső audit a számviteli és pénzügyi riporting eljárásokat illetően. Felelős: Pénzügy és Audit Bizottság. (p. 107)
Milyen modellt követ a belső kontroll rendszer? Keretrendszer (COSO; Turnbull report)			
COSO (p. 122)	COSO (p. 115)	*Konkrét modellt az éves beszámoló feldolgozása során nem azonosított a szerző.*	*Konkrét modellt az éves beszámoló feldolgozása során nem azonosított a szerző.*
A három védelmi vonal modell elemei hogyan érvényesülnek az éves beszámolóban?			
- a kockázatkezelési architektúra szisztematikus strukturálása érdekében az Audi csoport követi a három védelmi vonal modellt - a vállalat védelmét célozza jelentős kockázat bekövetkezése ellen - minden vonal rendszeresen és függetlenül jelent az Igazgatótanács és a Felügyelő Bizottság Audit Bizottsága felé - Első vonal: operációs kockázatkezelés divíziószinten; Második vonal: központi GRC funkció felelős az RMS/ICS és CMS alapvető működtetéséért; harmadik vonal: Belső audit, továbbá az RMS/ICS-t számviteli oldalról független auditor is vizsgálja. (pp. 123-125)	*A három védelmi vonal kifejezés maga nem jelenik meg a beszámolóban, egyes elemei azonban fellelhetőek. (pp. 69, 74, 82, 84, 114, 115, 116)*	*A három védelmi vonal kifejezés maga nem jelenik meg a beszámolóban, egyes elemei azonban fellelhetőek. (pp. 3, 26-41)*	*A három védelmi vonal kifejezés maga nem jelenik meg a beszámolóban, egyes elemei azonban fellelhetőek. (pp. 107-108)*
Mely kontroll témakörhöz kapcsolódó funkciók azonosíthatók (stratégia, megfelelés (compliance), vállalatirányítás (corporate governance), kockázatkezelés (risk management), kontrolling, etika stb.)?			
Etikus működés, Adatvédelem és adatbiztonság, Vállalatirányítás és Megfelelés, Vállalati kultúra, Korrupcióellenes működés, Stratégia (pp. 10, 79, 315, 318)	- integritás és megfelelőség (p. 82), stratégia (p. 26), műszaki megfelelési irányítási rendszer (tCMS) autóipari részlegekben. - a cél az összes jogi és szabályozási követelmény betartását biztosítani a teljes termékfejlesztési és tanúsítási folyamat során (p. 85), - antitröszt-megfelelés (p. 85), korrupcióellenes megfelelés (p. 85), adat-megfelelés (p. 86), pénzügyi bűncselekmények elleni megfelelés (p. 86), humán jogok tiszteletben tartása rendszer (p. 86)	Vállalatirányítási kódex, Etikai kódex, Megfelelés- és kockázatkezelés (pp. 26, 31)	Pénzügyi stratégia, pénzügyi kockázatkezelés (pp. 8, 70, 86)

AUDI vállalat	MERCEDES vállalat	SUZUKI vállalat	OPEL vállalat
Hogyan jelenik meg a kontroll funkció és a kockázatok kapcsolata? (internal controls and risks) (components of internal control: control environment, risk assessment, control activities, information and communicatio, and monitoring activities)?			
- kockázatoknak megfelelő belső kontrollok a teljes értéklánc mentén - RMS/ICS további fejlesztése - prioritás a rendszer szoros összekapcsolása a vállalati pénzügyi tervezéssel és menedzsmenttel, valamint a számviteli rendszerekkel - RMS/ICS szabályozási keretrendszere stratégiai jelentőségű. Belső vállalati politikában, szabályzatokban szilárdan megjelenik. (p. 123)	- a belső kontrollrendszer hatékonyságának szisztematikus értékelése a vállalati számviteli folyamat szempontjából. (kockázatelemzés; jelentős kockázatok azonosítása a vállalati számviteli és pénzügyi beszámolási folyamatokhoz; az ellenőrzések meghatározása és dokumentálása a csoportszintű irányelveknek megfelelően; rendszeres tesztelés véletlenszerű mintákon (kontrollok hatékonyságának felmérése, önértékelés alapja, ellenőrzési gyengeségek kiküszöbölése). - az Igazgatóság és a Felügyelő Bizottság Audit Bizottsága rendszeresen tájékoztatása - Felügyelő Bizottság; Belső ellenőrzési osztály; Külső auditorok szerepe (pp. 115-116)	A belső kontrollrendszerre vonatkozó alapvető szabályok a Megfelelési és Kockázatkezelés szekció alatt vannak ismertetve. (pp. 31-34)	Kockázati tényezők és bizonytalanságok' szekció alatt az éves management riport részeként, az éves beszámoló 8. oldalán található hivatkozás a belső kontrollokra. - A Csoport különböző működési egységei azonosítják és felmérik a kockázatokat, és folyamatosan értékelik a kapcsolódó belső kontrollokat, éves jelentéstétel az Igazgatóságnak. (p. 8)
Milyen kontroll funkcióhoz kapcsolódó kézikönyvek, szabályzatok-hoz és eljárásrendhez azonosíthatók? (handbooks, policies and procedures) (eg. Compliance, AML stb.)			
Magas stratégiai jelentősége miatt az RMS / ICS szabályozási keretrendszere mind a belső vállalati politikában mind a szabályzatokban szilárdan megjelenik. (p. 123)	A (belső kontroll) rendszer alapelveket és eljárásokat, valamint megelőző és detektív ellenőrzéseket tartalmaz." (p. 115)	Vállalatirányítási kódex (p. 26), Suzuki Group magatartási kódex (p. 26, 31), Megfelelési kézikönyv (Compliance Handbook) (pp. 33, 35), CSR Guidelines for Suppliers (biztonság és minőség elve elsődleges) (pp. 52-53)	Pénzügyi kockázatkezelési politika (p. 70), PSA Csoport kamatlábkockázat-kezelési politika (p. 71), PSA-csoport általános kockázatkezelési politika (p. 71), fedezeti politika (p. 73), devizapolitika (p. 73), tőkekezelési politika (p. 92)
Milyen kiemelt elemei vannak az éves beszámolónak a biztonság és védelem pl. információ biztonság (information security), biztonság és védelem (safety and security) szempontjából?			
A személyes adatok globális védelme és felelősségteljes kezelése (p. 292)	Vállalatbiztonság, Adatbiztonság, Információbiztonság, IT biztonság. Kiberbiztonság, Foglalkoztatottság biztonsága (pp. 40, 84, 115)	Személyes információ védelme (p. 35), Információbiztonság (p. 36), Katasztrófavédelem (p. 36), Biztonság és egészség védelme (p. 48), BCP (pp. 33, 36, 41, 52), Termékminőség/ Termékbiztonság (ISO 9001-et adaptálta) (pp. 46-47)	Egészségügyi és biztonsági kockázatok (p. 8), pénzügyi biztonság (p. 70), vevőknek szállított áruk és szolgáltatások ellenértékének fizetési biztonsága (p. 73), jelentős meghibásodás, üzemzavar vagy biztonsági sérülés, amely veszélyezteti az informatikai rendszereket vagy a társaságok járműveiben található elektronikus vezérlő rendszereket (p.109)

4.1.2. Kockázati tényezők és bizonytalanságok

Az irányítás (governance), kockázatkezelés (risk), és megfelelés (compliance) szerepe az éves beszámolókban domináns. Míg a kontroll funkció a vállalati kockázatkezeléssel együtt jellemzően stratégiai jelentőségű támogató pillérként azonosítható. A kockázatkezelés önálló szekcióként jelenik meg az éves beszámolókban (2. táblázat).

2. táblázat Kockázati tényezők és bizonytalanságok az éves beszámolóban (Forrás: az éves beszámolók alapján a szerző szerkesztése)

AUDI vállalat	MERCEDES vállalat	SUZUKI vállalat	OPEL vállalat
2. Hogyan jelennek meg a kockázati tényezők, és bizonytalanságok a vállalati éves beszámolóban? Hogyan jelenik meg a kockázatkezelés szerepe?			
Hogyan jelennek meg a kockázati tényezők, és bizonytalanságok a vállalati éves beszámolóban?			
- Kockázatok és lehetőségek jelentése szekció alatt az éves beszámoló ismerteti a kockázatkezelési rendszert, lehetőségkezelés működési elvét, valamint az Audi csoport "kockázatait és lehetőségeit" - Integritás, Megfelelés- és Kockázatkezelés funkció - Vállalati kockázatkezelésünk és a kockázatkezelési rendszer (RMS), vállalati irányelveik, a belső kontrollrendszer (ICS) és a Compliance Management System (CMS) támogatják munkájuk alappilléreit. (a vállalat céljainak fenntarthatóan védelme, az átláthatóság megteremtése és a kockázatok, a megfelelés és az integritás tudatosságának erősítése érdekében) (pp. 68, 71, 121)	- A Kockázat - és lehetőségkezelés a Csoport tervezési, kontrolling és jelentéstétel (reporting) folyamatának erőteljes eleme. - A Kockázat - és lehetőség jelentés önálló rész az éves beszámolóban. - "Az üzleti kockázatok és lehetőségek korai stádiumban történő azonosítása, valamint azok aktív felmérése és kezelése érdekében hatékony irányítási és kontrollrendszereket kerülnek alkalmazásra, egy átfogó kockázat- és lehetőségkezelési rendszerben megvalósítva." Az információs technológiai kockázatok és lehetőségek, valamint a személyi kockázatok és lehetőségek fel vannak tüntetve kockázati kategóriákként. (pp. 74, 114-129, 142)	A Vállalatirányítás szekció alatt Megfelelési- és kockázatkezelési rendszer, ill. a Működési kockázatok szekció alatt. (pp. 31-41)	Kockázati tényezők és bizonytalanságok' szekció az éves management riport részeként, az éves beszámoló 8. oldalán, ahol a főbb csoportra jellemző, valamint üzleti kockázatok jelennek meg. A kockázatkezelést főként a Vállalati Pénzügy funkció végzi, azonosítja a kockázatokat és csoport szabályzatokat határoz meg azok kezelésére. Pénzügyi kockázatkezelési politika (p. 70). (Kockázatok megjelennek az ún. statutory audit jelentés részeként is, ahol specifikus kockázatok lettek azonosítva fő audit kockázatokként. ld. statutory audit riport pp. 105-106)
Hogyan jelenik meg a kockázatkezelés szerepe?			
"- A lehetőségek és kockázatok konstruktív és nyílt kezelése elengedhetetlen az Audi számára a vállalkozói tevékenység tartós sikerének biztosítása érdekében. - A hatékony kockázatkezelési rendszer (RMS) konkrét célja - a törvényi előírások teljesítése mellett - a vállalat céljainak érvényesítése, az érdekeltek védelme a negatív vállalati fejlemények ellen, a kockázatok messzemenően gondos kezelési kötelezettségének teljesítése a hosszú távú életképesség és versenyképesség védelmeként. " (p. 121)	A Csoport tervezési, kontrolling és jelentéstétel folyamatának erőteljes elemeként jelenik meg (p. 74).	*Az éves beszámoló alapján egyre nagyobb hangsúlyt kap a funkció.*	Pénzügyi kockázatkezelési politika (p. 70), PSA Group kamatlábkockázat-kezelési politika (p. 71), PSA-csoport átfogó kockázatkezelési politika (p. 71). A Banque PSA Finance kockázatkezelési bizottsága (p. 87).

4.1.3. Emberi tényezők biztonsági szerepe

Az emberi erőforrások szerepe megjelenik stratégiai vonatkozásban, a vállalati kultúra kontextusában, a szervezeti tanulásban, és megjelennek etikai vonatkozások. További közös elem a vállalatok érintettsége a dízel emissziós botrányban. Kapcsolódó forrás a European Court of Auditors, 2019 tájékoztató dokumentuma [134]. Az eset erőteljes vezetőségi választ követelt meg. A „Rés a pajzson" eset kapcsán a biztonság és védelem, a belső kontrollrendszer korszerűsítése, fejlesztése, valamint a vállalati kultúra és tudatosság, szervezeti tanulás szerepe középpontba került (3. táblázat).

3. táblázat Emberi tényezők biztonsági szerepe (Forrás: az éves beszámolók alapján a szerző szerkesztése)

AUDI vállalat	MERCEDES vállalat	SUZUKI vállalat	OPEL vállalat
3. A humán erőforrás szerepe miként azonosítható biztonság és védelmi kontextusban?			
- munkahelyi egészség - és biztonság, -stratégiai HR tervezés, -"állásbiztonság", - emberi jogok tréning, - vállalati kultúra - motivált csoport képes a transzformációt megvalósítani, és kellőképp innovatív szakértelmet felhalmozni, - fenntartható koncepció a digitalizációhoz kapcsolódóan (pp. 60-62, 264, 272-274, 346)	- Integritási kódex - kötelező forma; törvények, szabályok betartása, elkötelezettség, vállalati értékek követése a gyakorlatban. - Értéktermelési folyamatok -> munka digitalizációja. Digitális átalakítás - munkabiztonsági garancia. Munkaköri leírások, feladatok és a követelményprofilok változása. - Változási folyamatok támogatása - képzési intézkedések a teljes munkaerőnek (pp. 77, 78, 83)	-Az emberi erőforrások - és munkavédelem fejlesztése kiemelt szerepet kap. - HR releváns biztonság és védelmi kérdések az éves beszámolóban - Személyes információk védelme, Biztonság és egészség védelme. (pp. 2-3, 33, 35, 37, 48-49)	Munkahelyi egészség és biztonsági kockázatokra talált hivatkozást a szerző. (p. 8)
Azonosítható az éves beszámolóból, hogyan biztosítja a vállalat, hogy a munkavállalók ismerik a kontrollokat? (Trainings)			
Hálapénzről szóló szabályzat az összeférhetetlenség és korrupció elkerüléséről; Web-alapú tréningek a korrupcióellenes, ill. közhivatalnokok kezelésével kapcsolatos témában; Web-alapú Etikai kódex és etikus döntéshozatal tréning (minden munkavállalónak kötelező); Web-alapú „Megfelelés-tudatosság" (Compliance awareness) tréning (pp. 79, 346)	Kiterjedt megfelelési tanfolyamokat kínálnak, amelyek az integritási kódexünkön alapulnak. A képzések tartalma és témái az adott célcsoport szerepéhez és funkcióihoz igazodnak. Rendszeresen elemzik a képzési programok szükségességét, szükség szerint kibővítik vagy adaptálják, és értékeléseket folytatnak. (p. 85)	- Megfelelési és a Kockázatkezelési rendszer (p. 31) részeként jelenik meg az éves beszámolóban. - HR Osztály folyamatos szemináriumai vezetőknek és alkalmazottaknak megfelelés témáról, vmint az egyes törvényekről / előírásokról (p.31). - kockázatkezelési tréning igazgatóknak, tisztségviselőknek, ügyvezető igazgatónak (p. 33). - tréningek a munkavállalók részére autógyártással kapcsolatos törvényekről és rendeletekről (p. 33), visszaélést bejelentő rendszer használatának elősegítése / oktatás, poszterek (p. 33).	Oktatásra és tréningre vonatkozó hivatkozást a K+F-re vonatkozó kontextusban azonosított a szerző. (p. 38)
Milyen a kockázat és kontroll tudatosság a szervezetben?			
Szoros együttműködés a vállalati - és HR stratégiák között, stratégiai HR tervezés, vállalati kultúra fejlesztése pl. Role Model Program (p. 62, 70, 78, 254, 261, 269, 272)	Rendszeresen ellenőrzésre kerülnek: - a Csoport egységes pénzügyi beszámolási, értékelési és számviteli irányelveinek folyamatos frissítése, rendszeres oktatása és betartása; - a belső kontrollrendszer hatékonyságát szisztematikusan értékelik a vállalati számviteli folyamat szempontjából; - a folyamatok a feladatok szétválasztására és a „négy szem elvére" a pénzügyi kimutatások elkészítése során, ill. az engedélyezési és hozzáférési szabályok a vonatkozó informatikai számviteli rendszerek számára stb. (pp. 114, 115)	A "Rés a pajzson" eset (ld. 5. pont) kapcsán kiemelkedő hangsúlyt kap a tudatosság, a biztonság és védelem, valamint a vállalati kultúra szerepe is. - az alapoktól áttekintik a megfelelési - és a kockázatkezelési rendszerünket, hogy lefedjük a Társaság összes tevékenységét, és megerősítsük a belső ellenőrzés felügyeletét. - a belső kontrollrendszer korszerűsítése. (pp. 2-3)	*A vizsgált éves beszámoló alapján tételes választ nem azonosított a szerző.*

4.1.4. „Rés a pajzson”

A „Rés a pajzson” esetek kapcsán azonosított akciólépések sorozata számos független, mégis összekapcsolódó elemet tartalmaz (4. táblázat). A vállalati kultúra fejlesztése, az etikai elvek követése, a munkavállalók, és vezetőség oktatása közvetetten, és a konkrét napi feladatok végrehajtása során tulajdonképpen közvetlenül is hozzájárul a belső kontrollrendszer erősítéséhez, és ezáltal a vállalat biztonsági szintjének növeléséhez. Ezek az elemek a kontrollok hálózati jellegét támasztják alá, és a kontrollhálózat teremtette biztonság és védelmi faktor szerepét definiálják.

4. táblázat „Rés a pajzson” esetek (Forrás: az éves beszámolók alapján a szerző szerkesztése)

AUDI vállalat	MERCEDES vállalat	SUZUKI vállalat	OPEL vállalat
4. Rés a pajzson esetek. Vállalati éves beszámolóban szerepelnek vállalati botrányok, csalások? Amennyiben igen, milyen a vezetőség válasza?			
Vállalati éves beszámolóban szerepelnek vállalati botrányok, csalások?			
Igen, dízel botrány (pp. 23, 64, 68, 69, 80)	Igen, dízel kipufogógáz-kibocsátással kapcsolatos botrány (pp. 16, 17, 40, 76)	Igen, a nem megfelelő magatartás a járművek utolsó ellenőrzésénél, 2017-ben feltárt incidens - nem megfelelő mintavétel az üzemanyag-fogyasztás és a kipufogógáz ellenőrzése során. (pp. 2-3, 33, 35, 40)	Igen, emissziós kontroll rendszer; beépített navigációs rendszer kapcsán törvényszegés a jogdíjfizetés elmaradása miatt (függő kötelezettségek) (p. 97)
Amennyiben igen, milyen a vezetőség válasza?			
-integritás és megfelelés program (ECI - etikus vállalati elvek) -Etikai Kódex, bejelentő rendszer és tréningek, kulturális változások. Aktív ún. speak up kultúra, integritás nagykövetek aktív hálózata. Integritás és vállalati kultúra központi kérdés. erősítette a rendszereit és folyamatait a korrupció megelőzés és trösztellenes viselkedés ellen és bevezette az üzleti partnerek átvilágítási folyamatát. -A csoport "ellapította a hierarchiát", laposabb struktúrát hozott létre, decentralizálta a döntéshozatalt és új vezetési és kollaborációs modellt vezetett be. Transzformáció. -Független Megfelelés Monitor megerősítése, hogy a csoport megtette a szükséges lépéseket a dízel botránnyal kapcsolatban. -Az amerikai EPA adminisztratív megállapodást kötött 2019-ben az Audi AG-val, mely megállapodás elismeri az intézkedéseket, melyeket 2015 óta a vállalat tett, hogy erősítse a megfelelés és kockázatkezelés funkciókat. (pp. 68-73)	-közös peres (class action) eljárás rendezése az USA-ban a dízel kipufogógáz-kibocsátással kapcsolatban (kb. 250 000 dízelmotoros jármű kibocsátáskontroll rendszere volt érintett). -műszaki megfelelőségi irányítási rendszer erősítése, szervizintéz-kedések az érintett járművek számára; országos kibocsátás-csökkentő program, és további projektek -Integritás "frissítése" - integritás kultúra további fejlesztése a Csoportban. A Felügyelő Bizottság foglalkozott az antitröszt eljárásokkal, és részletes jelentést kapott a dízel kipufogógáz-kibocsátással kapcsolatos kérdésekről. (pp. 16,17, 40)	-őszintén elnézést kértek helytelen magatartásuk miatt az üzemekben végzett végső járművizsgálat kapcsán -vezetői vállalati tudatosság növelése, szervezeti kultúra fejlesztése, cél biztosítani a törvények és előírások alapos betartását a Társaság valamennyi működési szintjén -végső ellenőrzési műveletek fejlesztése, pl. az ellenőrök terheinek csökkentését az ellenőrök számának növelésével és az ellenőrzési létesítmények fejlesztését, és előmozdították a vonatkozó intézkedéseket, hogy megbízhatóbb és pontosabb ellenőrzéseket lehessen végezni. További fejlesztések. - 2017-es incidens - nem megfelelő mintavétel az üzemanyag-fogyasztás és a kipufogógáz ellenőrzése- kapcsán az incidens feltárásának napjára megemlékeznek, aznap leáll a vállalat működése, felelevéníve, hogy mennyire fontos megőrizni a nem megfelelő cselekedetekkel szembeni tudatosságot. -biztonság és védelem kiemelt prioritás; - "minőség javítása" (pp. 2-3, 33, 35, 40)	*A vizsgált éves beszámolóban részletes esetismertetést és vezetőségi választ nem azonosított a szerző.*

4.1.5. Hálózatok

A hálózati jelleg megjelenik a globális vállalati hálózat (a termékek világszerte eljutnak a fogyasztókhoz), és kereskedői hálózat kontextusában is, mely mögött a vállalati üzleti modell hálózati jellege azonosítható. A beszámolókból kigyűjtött tényanyagot az 5. táblázat tartalmazza.

Az információ- és adatbiztonság tématerület valamennyi éves beszámoló közös metszete. A Suzuki éves beszámolója kiemeli a hálózatok szerepét az információbiztonság kontextusában, előtérbe kerül az információellenőrzés / információ kontroll szerepe. Az információrendszer és hálózat célja, hogy az információszivárgást és jogosulatlan hozzáféréseket megakadályozza, illetve fejlessze/elősegítse az információhoz való hozzáférést.

Az Audi éves beszámolójában a work@Audi kezdeményezés alatt megnevezi, hogy elmozdulás történik a tradicionális struktúrák és merev hierarchiáktól, át akarják gondolni a vezetést, nyitottságra, őszinteségre és tiszteletre van szükség az információ cserék és témák megvitatása során. A Csoport „ellapította a hierarchiát”, decentralizálta a döntéshozatalt és új vezetési - és kollaborációs modellt hozott létre. Mindez a jó visszajelzési kultúra és az új és agilis együttműködés alapja is. A felvázolt működési modell a Barabási-Albert László által megjelenített szervezeti transzformáció jelenségével hasonlatos, miszerint elmozdulás szükséges a merev fa modelltől a változó üzleti környezetben a dinamikus, hálózati modell felé.

Az Opel anyavállalata magántulajdonú, a vállalat éves beszámolója elsődlegesen a pénzügyi folyamatokra fókuszál, pénzügyi kockázatkezelés és pénzügyi stratégia jelennek meg kontroll témakörhöz kapcsolódó funkciókként. A menedzsment felelőssége a kontroll- és kockázatkezelés funkció felett megjelenik, továbbá kirajzolódik a monitorozási folyamat. A szöveges terjedelem a legrövidebbre szorítkozik, nagyságrendileg egy oldal. Az éves beszámoló „külső szemlélő” számára nem tárja fel érdemben a vállalati folyamatokat.

5. táblázat Hálózatok az éves beszámolóban (Forrás: az éves beszámolók alapján a szerző szerkesztése)

AUDI vállalat	MERCEDES vállalat	SUZUKI vállalat	OPEL vállalat
5. Milyen kontextusban jelenik meg a hálózat (network) kifejezés a vállalat éves beszámolójában?			
Mennyiben jelenik meg a vállalati belső kontrollrendszer hálózatként, és miként definiálható a hálózati struktúra? (NB: Belső kontrollrendszer behálózza a vállalat egészét, valamennyi tevékenységbe beágyazódik… Vállalati célkitűzések elérését segíti elő. Vállalatirányítás elválaszthatatlan eszköze.)			
-"integritás nagykövetek hálózata", Az integrált és inkluzív irányítási megközelítés részeként az RMS / ICS szorosan össze-kapcsolódik a megfelelőségi funkcióval (Központi Governance, Risk & Compliance (GRC) szervezet). RMS célja. - elmozdulás jelenik meg a tradicionális struktúráktól és merev hierarchiáktól a work@Audi kezdeményezés alapján (ld. Barabási) - "content wheel" középen az Audi csoport stratégiával (pp. 62, 122, 123, 318)	- a (belső kontroll) rendszer alapelveket és eljárásokat, ill. megelőző és detektív ellenőrzéseket tartalmaz (p. 115) - a hálózat szó: globális gyártási hálózat (p. 123), értékesítési hálózat (p. 28), rugalmas gyártási hálózat (p. 37, 42), globális K+F hálózat (p. 41), iparági, ill. iparágak közötti hálózatok (p. 80), mérnöki hálózat (p. 39), kontakt személyek hálózata (p. 83), Globális megfelelési területet összefogó hálózat (p. 86). - lokális kapcsolattartók nemzetközi hálózata a dolgozók számára integritás, megfelelés és jogi témákban. Cél, megfelelés a megfelelési területre vonatkozó standardoknak (p. 83). A hálózat kiértékeli a feltett kérdéseket, és amennyiben szükséges, megfelelő intézkedéseket tesz. Kiterjesztették az "integritás hálózatukat" is, mely az integritás további beágyazására törekszik a mindennapi rutinba (p. 83).	- a hálózatok szó a vállalat globális hálózatának (p. 5, 11) (termékek világszerte eljutnak a fogyasztókhoz), illetőleg információ biztonság (p. 36) kontextusában - az információs rendszer és hálózat célja, az információszivárgás és jogosulatlan hozzáférések megakadályozása, ill. az információhoz való hozzáférés fejlesztése/elősegítése. szervereket, melyek leállása súlyos kimenetelű hatást okozhat, és melyek a biztonság szempontjából fontos adatokat, pl. személyes adatokat mentenek, egy zárható kiszolgálóhelyiségbe telepítik, szeizmikus izolátorokkal stb. (p. 36) - bizalmas információ-ellenőrzési/ információ kontroll promóciós értekezlet; az egész Suzuki-csoport információ-ellenőrzési / információ kontroll rendszerének megerősítése (p. 36) - ISO 27001 minősítést szerzett 2020-ban. (p. 36)	A hálózatok szó a kereskedői hálózat kontextusában jelenik meg (pl. pp. 7, 30, 37).

4.1.6. Következtetések

A vizsgált vállalatok egy intenzív transzformációs folyamatban vesznek részt, mely összvállalati szinten alkalmazkodást kíván meg úgy a rendszerek, mint az emberi erőforrások stratégiai kezelése során is.

A hálózati struktúra visszatükröződik az üzleti modell szintjén, jellemző a globális hálózatszerű működés. A hálózatos jelleg a belső vállalati folyamatokban is megjelenik, mint például az információbiztonság hálózatszerű kezelése során. A vállalati védelmi vonalak – üzleti folyamatokba ágyazott kontrollok, kontroll- és megfelelés funkciók és külső/belső auditok – szintén hálózatszerűen jelennek meg a vállalati működésben. Az irányítás, a megfelelés, és a kockázatkezelés (GRC) funkciók integrált kezelése jellemző, és szerepük domináns. A kontroll funkció a vállalati kockázatkezeléssel együtt jellemzően stratégiai jelentőségű támogató pillérként jelenik meg.

A belső kontrollrendszer egyes elemei – a kontrollkörnyezet, kockázatértékelés, kontrollok, információs és kommunikációs folyamat, és monitoring – összefüggő rendszert képezve a vállalati biztonsági rendszer komplex, az egész vállalatot behálózó elemei. A belső kontrollrendszer és kontroll funkció megjelenik szabályzatok szintjén is. A vállalati – üzleti, logisztikai és technológiai – folyamatok szabályozása, leírása, és a működés megfelelő monitorozása a kívánt biztonsági szint elérését segíti. A belső kontrollrendszer egyes elemei szorosan összekapcsolódnak, és megfelelő működés esetén az egyes elemek egymást erősítik.

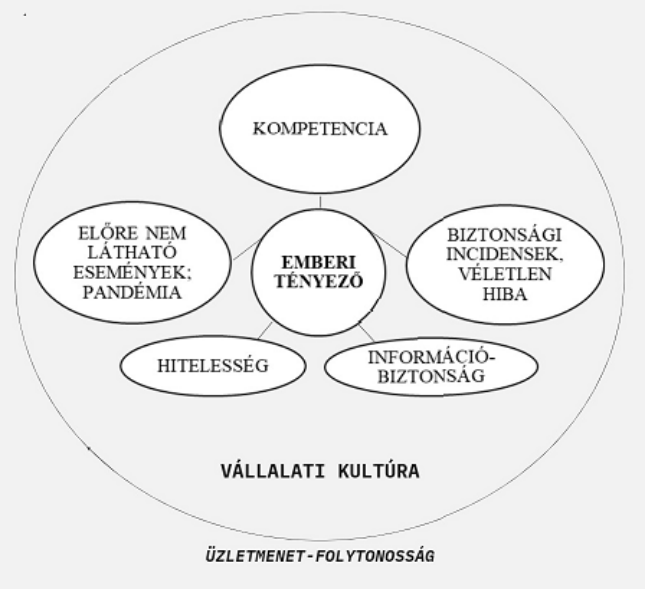
Az autóipari vállalatok esetében a dízelkibocsátási botrány példázza, hogy az esetleges hibák, „rések a pajzson” kontrollhiányosságokra világítanak rá. A vezetőség adekvát válasza, megfelelő javító intézkedések szükségesek az észlelt hiányosságok „orvoslására”, a belső kontrollrendszer korszerűsítésére és fejlesztésére. Egyes esetekben mindez a korábbi hiányosságokon túlmutató rendszerfejlesztéseket, egy komplex tanulási folyamatot, a vállalati kultúra, valamint a kontrolltudatosság fejlesztését is eredményezi. A nem megfelelő cselekedetekkel szembeni tudatosság, az integritás, az etikai elvek követése és a vállalati kultúra a vállalati biztonsági háló „lágy” eleméhez, az emberi tényezőkhöz kötődik.

4.2. Az emberi tényező vizsgálata hálózatkutatási szempontból

A szofisztikált technológiai megoldások mellett az emberi tényezőben rejlő kockázatok kezelésére kiemelt figyelmet kell fordítani. A szakértői kutatásom (5.2. fejezet) és szekunder kutatási eredményeim egyaránt rámutatnak arra, hogy a humán tényezőköz köthető kockázatok meghatározó súllyal bírnak a vállalati biztonság szempontjából. Az emberi tényező a vállalati működés valamennyi szintjén megjelenik. A folyamatlépések és a kontrolltevékenységek végrehajtásához is kapcsolódik emberi tényező. Meghatározó kérdés, hogy a biztonságos szervezeti működés az emberi tényező oldaláról hogyan biztosítható a folyamatosan változó üzleti környezetben, illetve nem várt események, például pandémia esetén.

4.2.1. Az emberi kockázatok átfogó áttekintése

Az emberi kockázatok a szervezetben több szinten vannak jelen. A vállalati kultúra, és ennek részeként a vállalati biztonsági kultúra átfogóan jelen vannak a vállalati folyamatokban. Mindez az operatív folyamatok szintjén jellemzően áttételesen jelenik meg, mindazonáltal a vállalat egészét tekintve meghatározó. Ezekre az áttételes kapcsolatokra és összefüggésekre például egy gyökérok elemzés során azonosított kiváltó okok és összefüggések tudnak rávilágítani. Az alábbiakban a humán kockázatok egy lehetséges taxonómiáját mutatom be. Az emberi kockázatokat átfogóan ismertetem, mert azok jellegükből adódóan hatással lehetnek a vállalati működésre, annak folyamataira stratégiai és operatív szinten is. A 2. ábra az üzletmenet során – a folytonos üzletmenet érdekében – az emberi tényezőhöz kapcsolódó kockázatokat – illusztratív jelleggel, szimbolikusan emberként ábrázolva – szemlélteti.



2. ábra A vállalati biztonsági kultúrát befolyásoló humán kockázatok (Forrás: Saját szerkesztés.)

A 2. ábra áttekintő jelleggel mutatja be a vállalati biztonsági kultúrát befolyásoló emberi kockázati tényezőket, kiemelve a hitelesség és információbiztonsági kockázatokat, melyek stabil, folyamatos kezelése alapvető fontosságú a sikeres biztonsági kultúra szempontjából (lábak), a váratlan események kockázatait (biztonsági incidensek, véletlen hibák, illetve megváltozott körülményekkel kapcsolatos kockázatok, például pandémia) (kezek), melyeket felmerülésük esetén a vállalati kockázatkezelési szabályzatnak megfelelően adekvát válasszal, cselekvési tervvel szükséges kezelni, illetőleg a kompetencia kockázatokat (fej).

Biztonsági incidensek, véletlen hibák: A vállalati működés során bekövetkező biztonsági incidensek jelentős része az emberi tényezőköz köthető [137]. A humán faktorok hatásai biztonsági kockázatot jelentenek, melyek mérsékelhetők, többek között az emberi erőforrás, a munkaerő kellő szakmai felkészültsége és naprakészsége, a szervezeti tudás aktív operatív alkalmazása, a humánerőforrás-menedzsment folyamat integritása, és a szervezeti szinten megfogalmazott és alkalmazott etikai elvek intézményesülése által. Mindezek olyan tényezők, melyek a biztonsági kockázatokat mérsékelni képesek. A Biztonsági incidensek, véletlen hibák kategóriáján belül a kumulált kockázat, fatális hiba esete külön figyelmet érdemel, mely több, látszólag független biztonsági hiba együttes bekövetkezése folytán fokozott problémát tud okozni, ahogy azt a Reason által ismertetett svájci sajt modell példája is illusztrálja [138]. Reason az emberi hibák két fontos jellemzőjére mutat rá, hogy hogyan tud a kontrollok ellenére egy incidens bekövetkezni. Az egyik, hogy a legnagyobb hibát gyakran a legjobb emberek követik el. Másodszor pedig: a szerencsétlenségek messze nem véletlenszerűek, hanem visszatérő problémákat jeleznek és adott körülmények hasonló hibákat idézhetnek elő, függetlenül az érintett személyektől [139].

Hitelességi kockázat: A hitelességi kockázatok, azaz az olyan kockázatok, melyek a felek megbízhatóságával, integritásával, hitelességével kapcsolatosak, a bizalom fogalma köré épülnek. A vállalati bizalmi kultúra elősegíti a folyamatok működését, a folyamatok sebessége nő, a költségek csökkennek [140], melyet a „bízz, de ellenőrizz” szemlélet jegyében kontrollálni kell. A hitelességi kockázatok szorosan összefonódnak az emberi tényezővel, melyek a működési folyamatokban napi szinten megjelennek. A hitelességi kockázat minimalizálása a szervezeti biztonsági kultúra fejlesztéséhez és erős, etikus szervezeti kultúra kialakításához járul hozzá.

A biztonság szintje olyan erős, mint a leggyengébb láncszem a folyamatban [137; 141], így a „hitelességi kockázat” kezelése nagyban elősegíti a biztonsági célok megvalósulását. A támadók is a leggyengébb pontot támadják, vegyük például a pszichológiai manipuláció (social engineering) esetét.

A pszichológiai manipuláció az emberi faktor gyengeségein alapulva képes „rést ütni a pajzson”, azaz a szervezet védelmi rendszerén. A pszichológiai manipuláció az emberi interakciókra támaszkodik, és kihasználja az emberi természet sajátosságait, hogy az emberek alapvetően segítőkészek és konfliktuskerülők [142; 143].

A hitelességi kockázaton belül az emberi tényezőre vonatkozóan kiemelt kockázati területet jelent a csalás kockázata, amikor a munkavállalók egyéni érdekei állnak a csalások (fraud) mögött. A csalás esetek kezelése szintén a vállalat biztonsági rendszerének feladata. Az árulkodó jeleket – személyes figyelemfelhívó jegyek, például anyagi szükséglet, tartozások, életstílus, jövedelem különbözőség, munkafolyamatok izolált végrehajtása – a biztonsági rendszernek fel kell ismernie és kezelnie kell.

Információbiztonsági kockázat: Az információbiztonsági kockázatok súlyos, illetve kritikus következménnyel is járhatnak, például adatbiztonsági kockázatok, adatvesztés, adatszivárgás, GDPR [112] nem megfelelés, IKT kitettségek. Információbiztonsági alapelvek – titoktartás, sértetlenség, hozzáférhetőség (CIA – confidentiality, integrity, availability) – követése szükséges.

Megváltozott körülményekkel kapcsolatos kockázatok, pandémia, előre nem látható természeti jelenség: A vállalatoknak a megváltozott körülményekkel kapcsolatos, illetve az előre nem látható kockázatok kezelésére is fel kell készülniük. A COVID-19 pandémia a kockázati környezetre szignifikáns hatást gyakorolt, és még hangsúlyosabbá tette a biztonság kérdését. A változások mintegy láncreakció jelleggel további változásokat indukáltak.

Az információbiztonság, és kiberbiztonság kérdése még hangsúlyosabbá vált. Az e-kereskedelem térnyerése és vele párhuzamosan az online kereskedelem új kockázatokat hozott. Nőtt a csalással kapcsolatos esetek száma. A munkavállalók mindennapi munkarutinja is érintetté vált. A pandémia esetében nyilvánvaló volt, hogy a biztonság értéket jelent. Változó környezetben a reziliencia, az alkalmazkodóképesség az üzletmenet-folytonosság képességének biztosítását is jelentheti, melynek fontosságát a folyamatos versenyhelyzeteken túl a pandémia is megmutatta.

Az otthoni munkavégzés és a távmunka helyet kapott olyan munkáltatóknál is, ahol korábban az ilyen gyakorlatra nem volt jelen például biztonsági megfontolásokból, illetve jóval kiterjedtebben jelent meg ez a gyakorlat olyan vállalatoknál, ahol a gyakorlat már működött.

Az otthoni munkavégzés gyakorlata kiszakította a munkavállalókat a megszokott életükből, az új helyzet mentális szorongással vagy motivációvesztéssel járhat, ezáltal a munkahelyi mentálhigiéné területe még fontosabbá vált. A dolgozók lelki egészségével foglalkozni kell.

Az új, ismeretlen helyzetek átgondolt változások esetén is kockázatosabbak. A biztonságtudatosság szerepe még inkább meghatározó jelentőségűvé vált. A kockázatkezelés és a kockázattudatos szervezeti kultúra jelentősége még inkább nőtt, melyet a vállalati stratégia részeként lehet hatásosan és eredményesen kezelni.

Kompetenciakockázat: A vállalati stratégia emberi erőforrás oldalát vizsgálva elsődleges, hogy a működéshez szükséges szakértelem és tudás a kellő időben és helyen rendelkezésre álljon. Az emberi erőforrás folyamatokkal – azaz a HR-, az emberek irányítási (people management) és teljesítményértékelési (performance management) folyamatokkal – szemben alapkövetelmény, hogy azok képesek legyenek a kompetenciakockázat kezelésére, ellenkező esetben a felelős személyek nem rendelkeznek megfelelő kompetenciával. A csoportvezetői munkássághoz szaktudás és irányítási képességek szükségesek. A HR stratégia meghatározó jelentőségű, annak vállalati szintű stratégia részeként történő integrált kezelése elősegíti, hogy az emberi erőforrás a szükséges helyen, időben, „mennyiségben" és minőségben rendelkezésre álljon.

Ha a munkatársak nem képesek az irányítási követelmények szerint ellátni feladataikat, annak fő kockázati tényezői között szerepel a szakértelem hiánya; a munkatársak nem ismerik az eljárásokat és a végrehajtási követelményeket, illetve a változó szakmai készségkövetelmények [44]. A kompetencia kérdésköre több szinten jelenik meg a vállalati működés során.

A feladat végrehajtásához szükséges idő függ az operatív feladatot végrehajtó egyén feladatvégzésben megszerzett rutinjától. Azonos szakmai kompetenciával rendelkező egyének kompetencia szintje eltérő lehet, ami azt eredményezi, hogy egy adott feladat végrehajtásának ideje eltérő lehet attól függően ki végzi a feladatot [136]. Ezzel párhuzamosan az elvégzett feladat minősége sem minden esetben sztenderd. Egységes, sztenderd produktumot előállító gyártási folyamat végterméke közelítőleg állandó, míg tanácsadási területen szakértő függvényében más lehet a kimenetel, az output. A minőség és a ráfordított idő fordított arányt mutat, attól függően milyen szinten áll a feladatot végző szakmai tapasztalata, gyakorlata, „rutinja" az adott tevékenység vonatkozásában.

Üzletmenet-folytonosság: Az üzletmenet-folytonosság biztosítása szükséges a humán erőforrás távozása, illetve szabadsága esetén is. A vállalati folyamatok szabályozása és a dokumentumkezelési folyamatok átláthatósága a vállalat rezilienciájának megteremtését segíti. A vállalati folyamatok egy adott egyéntől függetlenül is végbe kell, hogy menjenek. Az üzletmenet-folytonosság biztosításának elve egyetemlegesen jelenik meg a vállalati működés során.

Vállalati biztonsági kultúra: Szorosan kapcsolódik az egyes kockázati tényezőkhöz, azonban jelentősége miatt külön nevesítem. A vállalati biztonsági kultúra szempontjából a szervezet vezetője (tone of the top) elsődleges szerepet tölt be. A vezető felelőssége az adekvát biztonsági kultúra kialakítása, az értékek megfogalmazása, közvetítése, valamint képviselete az alkalmazottak felé. Az információbiztonsági kultúra is része mindennek, és a felsővezetésnek bizonyítania kell vezetői képességét és elkötelezettségét az információbiztonsági irányítási rendszer (IBIR) vonatkozásában. A vezetői akarat és elkötelezettség a szabályozáson keresztül valósul meg [144]. Fejlett biztonsági kultúra esetén a szervezet dolgozói a biztonságot veszélyeztető tényezőkkel kapcsolatban a szükséges ismereteket elsajátítják és felelősen alkalmazzák [145]. A vállalatok komplex biztonsági kihívásokkal és kockázatokkal szembesülnek – ideértve az IKT rendszerekhez és az emberi tényezőhöz köthető kockázatokat, továbbá tágabb értelemben a vállalati működéshez kapcsolódó kockázatokat, mint pénzmosás és terrorizmusfinanszírozás kockázata –, amelyek kezeléséhez sikeres, fejlett biztonsági kultúra szükséges.

4.2.2. Belső kontrollok hálózata

Hálózatkutatási kontextusban lehetnek a csomópontok az emberek, az élek a folyamattevékenységek, egy-egy folyamat egy-egy eleme, mellyel az emberi kapcsolati háló írható le. Értelmezhető a tevékenységek és a tevékenységek közötti logikai kapcsolat által leírt hálózat is. Ez utóbbi esetben a folyamattevékenységek kapcsolati hálózata írható le: az egyes folyamattevékenységek a csomópontok, ahol az emberek és gépek az erőforrások és a tevékenységek közötti logikai kapcsolatok az élek.

A hatásos és biztonságos szinten történő működéshez szükséges többek között a munkafolyamatok összhangja, a vállalati funkciókat képviselő emberek közötti együttműködés és transzparencia. A vállalati folyamatok között összefüggés, „átadás" és visszacsatolás van. A jól tervezett, működtetett és dokumentált folyamatok esetében szinergia érhető el, mert csökken a felesleges és ezáltal kiküszöbölhető átadás-átvételek, azaz kapcsolatok száma, mely csökkenti a felmerülő idő-, pénz- és energiaráfordításokat.

A kívánt biztonsági szint elérése érdekében szükséges a folyamatok hálózatában gondolkodni, és az összefüggéseket holisztikusan szemlélni. A kontrollfunkció működése akkor valósul meg legcélravezetőbben, ha az a munkafolyamatok elválaszthatatlan részeként valósul meg. A munkafolyamatba épített kontrollok a vállalati folyamatok hálózatának szerves részét képezik. A rendszeres ellenőrzés és monitoring a folyamatok tervezett, illetve operatív működéséről adnak visszaigazolást, mely alapján a szükséges preventív, detektív, illetve korrektív tevekénységek meghatározhatók.

Pénzügyi aspektusa valamennyi vállalati folyamatnak van. A kontrolling funkció része a vállalati folyamatoknak. A pénzügyi kontrolling funkció pénzügyi szinten járul hozzá a működési folyamatok tervezéséhez, megvalósulásához, és financiális oldalról validálja a vállalati folyamatokat.

Az IKT rendszerek képet adnak a rendszerbe integrált folyamatokról, és behálózzák a vállalat működését. Analóg módon az emberi tényező is a vállalati működés valamennyi szintjén megjelenik, a felsővezetés és az operatív munkafolyamatokat végző munkavállalók, és munkaerő szintjén is. A vezetőség „hangja" és a képviselt értékrend beépül a vállalat mindennapi működésébe, meghatározza a vállalati kultúrát és a kontrollfolyamatok sikerességét is. A rendszerek biztonsági hálója az emberi tényező kockázatainak egyidejű kezelésével lesz kellőképp erős. A vállalati biztonsági kultúra célkitűzésként is értelmezhető, mely a biztonsági kockázatokat „lefedő", azokat kezelő kontrollokon keresztül valósul meg. A biztonsági kultúra kihat a vállalat külső kapcsolataira, megjelenik többek között a vállalati reputációban és arculatban is.

4.2.3. Folyamatkontrollok modellezése

A vállalati folyamatok közül (Pi) a bevételszerzési folyamat (P1) sikeressége a vállalat sikerességének kulcsa. A következőkben a bevételszerzési folyamat főbb lépéseit és a kapcsolódó kontrollokat (CA) ismertetem egy vállalati jógyakorlat példáján alapulóan [135]. A folyamat gépi és emberi közreműködéssel valósul meg, és változó arányban tartalmaz automatikus, manuális és félig automatikus tevékenységeket.

P11: A bevételszerzési folyamat (P1) a rendelésfelvétellel indul. A rendelésfelvételhez kontrolltevékenységek kapcsolódnak: a rendelési adatok ellenőrzésre kerülnek, nem teljes vagy nem pontos rendelési adatok esetén azokat pótolni szükséges (CA11.1). Rendszer általi ellenőrzés történik a duplikált rendelésfelvétel megakadályozása érdekében (CA11.2). A rendelések feldolgozása jóváhagyott hitelkereten belül történik (CA11.3). Magasabb diszkontráták esetén külön független ellenőrzés történik (CA11.4).

P12: Sikeres rendelésfelvételt követően kerül sor a számlázásra. A számlázáshoz kontrolltevékenységek kapcsolódnak: a szállítmány jóváhagyott kiadása alapján a raktárból, a rendszer automatikusan generálja a számlát azonos dátummal (CA12.1). A szállítási dátum nem módosítható megfelelő szintű vezetői jóváhagyás nélkül (CA12.2).
Rendszerbeállítás alapján a számlaadatok ellenőrzése a törzsadatok és a megrendelésadatok alapján. Nem valid adatok elutasításra kerülnek vagy egy függő tételeket tartalmazó file-ba, mely később korrigálható (CA12.3).

P13: A számlázást követően kerül sor a pénzbeszedési folyamatlépésre. A pénzbeszedéshez kontrolltevékenységek kapcsolódnak: a vezető ellenőrzi a koros követeléseket és összehasonlítja a beérkezett kintlévőségeket a periódus elején nyitott követelésekkel (CA13.1). A beérkező pénz vevőszámlához rendelése a vevőnév, a vevőszám és a számlaszám alapján történik, és csak nyitott számlákkal szemben (CA13.2).

P14: Az értékesítést követően visszaküldésre is sor kerülhet. A visszaküldött áru fizikai ellenőrzése, felülvizsgálata és a visszáru engedély (RMA – return merchandise authorization) jóváhagyása szükséges (CA14.1).

Vállalati folyamatok halmaza i=1,..,n		Folyamat i=1		P1 vállalati folyamat lépései		Kontroll-tevékenységek a folyamatban		Emberi részvétel a kontrolltevékenységben (nem/igen) [0; 1]
				P11		CA11.1		1
						CA11.2		0
						CA11.3		1
						CA11.4		1
Pi		P1		P12		CA12.1		0
						CA12.2		1
						CA12.3		0
				P13		CA13.1		1
						CA13.2		1
				P14		CA14.1		1
					SZUM	10	**SZUM**	7

3. ábra Kontrollok a bevételszerzési folyamatban (Forrás: Saját szerkesztés.)

A 3. ábrán a folyamathoz kapcsolódó kontrollokat modellezem. A 3. ábra a vállalati folyamatok halmazából (Pi) a vállalati bevételszerzési folyamathoz (P1) rendelten jeleníti meg a folyamathoz rendelt kontrollokat, melyek a kockázatok értékelése során beazonosított kockázatok kezelését biztosítják.

A P1 folyamat alfolyamatai (P11, P12, P13 és P14) részben „gépi”, részben manuális, emberi munkaerő segítségével valósulnak meg. Egyes folyamatlépések és hozzájuk kapcsolódó kontrolltevékenységek automatikus, manuális és félig automatikus, félig manuális folyamatlépésekből épülnek fel.

A kontrolltevékenységek jellemzően rendszer által elvégzett kontrolltevékenységek, azonban domináns az emberi tényező részvétele is a kontrolltevékenységekben. A fenti esetben 70%-ban volt jelen emberi részvétel a folyamathoz rendelt kontrolltevékenységekben.

A „gépi” részvétel, a rendszerek által végrehajtott megoldások jellemzők és preferáltak, azonban a humán faktor részvétele a folyamatokban ennek ellenére mégis meghatározó. Mind a „gépi”, mind az emberi tényező részvétele a folyamatokban kockázatokat hordoz, melyek sikeres kezelése a folyamatok biztonságos működéséhez szükséges.

A kockázatkezelés a biztonságos, kellőképp kontrollált vállalat megteremtése érdekében szükséges. Szorosan kapcsolódva a kockázatkezelési feladatokhoz a lehetséges kontrollok közül meg kell határozni, hogy a vállalat mely kontrollokat alkalmazza. A folyamatokhoz rendelt kontrollok hálózata tulajdonképpen a belső kontrollrendszer megvalósulása a vállalati folyamatokban. A vállalat működéséhez kapcsolódóan az összes vállalati folyamatot át kell tekinteni, meghatározni a kockázatokat és kontrolltevékenységeket a vállalat kockázattűrő képességével összhangban. Egyes kontrollok több folyamatlépéshez kapcsolódóan is bizonyosságot nyújthatnak.

A magas fokú kontrolltudatosság esetén a kontrollok számossága magas, mely magas szintű biztonsági kultúrát jelez, ahol a reziduális kockázat – a kockázat, mely a kontrollok működése mellett marad – alacsony. A kontrollfolyamatokat időről időre át kell értékelni, hogy megfelelő védelmet nyújtanak-e, illetve amennyiben változás tapasztalható a kontrollkörnyezetben, például pandémia. A vállalati folyamatokba épített kontrollokon keresztül a vállalat értéket realizál, mely hozzájárul az átlátható, eredményes és hatékony folyamatokhoz, a minőségre vonatkozó célkitűzések megvalósításához, valamint segíti a vállalat alkalmazkodóképességét.

4.2.4. Következtetések

A folyamatlépések és a kontrolltevékenységek végrehajtásához is kapcsolódik emberi tényező. Szükséges az emberi tényezőben rejlő kockázatok azonosítása és kezelése. A humán kockázatok közé tartoznak többek között a biztonsági incidensek, a véletlen hibák, és az információbiztonsági kockázat.

A kockázatkezelés a vállalati folyamat-, illetve a vállalatbiztonság megteremtését segíti. A vállalati folyamatok kockázatokat hordoznak, melyeket adott folyamatlépéshez rendelten kontrollokkal kell kezelni. A vállalati folyamatok hálózatába épített kontrollok a belső kontrollrendszer megvalósulását jelentik a vállalati gyakorlatban. A kontrolltudatos vállalat magasabb biztonsági szintet ér el. A belső kontrollrendszer alkalmas a vállalati „biztonsági kultúra” jellemzésére. Szükséges, hogy a vállalati kultúra és vele együtt a vállalati biztonsági kultúra olyan értékrendet közvetítsen, mely képes a vállalati integritás és kontrollkörnyezet erősítésére.

4.3. A biztonsági háló sajátosságai

A belső kontrollrendszer a vállalatban átfogóan jelen van. A kontrollrendszer szorosan kapcsolódik a vállalati stratégiai célkitűzések megvalósításához, biztosítja a pénzügyi beszámolók megbízhatóságát, a megfelelést, és pragmatikusan megjelenik az operatív mindennapi működésben.

A vállalati belső kontrollrendszer, a biztonsági háló elemző vizsgálata rámutatott a kontrollrendszer összetettségére, és a vállalatot behálózó jellegére. A belső kontrollrendszer egyes elemei a kontroll funkció különféle megnyilvánulási formáin keresztül jelen vannak valamennyi vállalati szinten és folyamatban. A kontrollrendszer vállalati, azaz entitás szintjén a teljes vállalatra vonatkozóan definiált kontrolljai kihatnak a vállalati működés operatív műveleti szintjére is. A vállalat által követett etikai / viselkedési kódex által definiált értékrend egyetemlegesen érvényes. Az operatív működési folyamatokhoz kapcsolódóan definiált kontrollok konkrét folyamatlépések biztonságos működéséhez nyújtanak bizonyosságot.

A felsővezetői szinthez köthető felelősség, döntéshozatal, a külső és belső kapcsolati háló jól reprezentálja a vállalatvezetői szinten végrehajtott feladat egyediségét. Az operatív folyamatokat konkrét részfolyamatok, tevékenységek és műveletek szintjére lebontva azonban egyre inkább az egységesített, standardizált folyamatok felé történő elmozdulás a domináns, ami az egyediség skálájának másik végpontja. Minél inkább szabványosított, leszabályozott egy folyamat, minél kevesebb eltérést enged, annál inkább skálázható, tervezhető. A digitális világban ezek azok a tevékenységek melyek szoftverrobotokkal automatizálhatók. A fenti természetesen két illusztratív véglet, mely rámutat a vállalati belső kontrollrendszer komplexitására.

A hálózati jellemzők egyúttal rávilágítanak a kontrollhálózat erős és gyenge pontjaira egyaránt, mely a hibatűrő képességből és sebezhetőségből származtatható, egyrészt marginális incidens, hiba felmerülése esetén működőképes marad a rendszer, másrészt, amennyiben a kontrollhálózatot meghatározó kulcstényező kiesik, az az egész rendszerre hatással van. A vezetői elkötelezettség döntő jelentőségű a biztonsági háló működése szempontjából. Az információbiztonság sebezhetőségéből kifolyólag szintúgy. Az információbiztonság megvalósítása éppúgy az elkötelezett vezető támogatásának a függvénye.

5. BIZTONSÁGI HÁLÓ

A fejezetben a biztonsági háló meghatározó tényezőinek azonosításához kapcsolódó szekunder kutatási eredményeket (5.1. fejezet), és az elvégzett szakértői kutatásom eredményeit mutatom be (5.2. fejezet).

5.1. A biztonság tényezői

Az értekezés jelen fejezetében az értekezésemhez kapcsolódó szekunder adatokon alapuló főbb eredményeket ismertetem.

5.1.1. Tendenciák a globális kockázati környezetben

Jelen fejezetben tanácsadó cégek globális vállalati kockázatkezelési felmérései [5; 6; 7; 8; 9] alapján készült elemzés eredményeit mutatom be [S7].

Megfigyelhető az a tendencia, hogy a kockázatkezelés a decentralizált irányból egy centralizáltabb irány felé mozdul el. A központosított megközelítés következetesebb kockázati politikát eredményezhet. Ezenfelül a kockázatkezeléshez kapcsolódó felelősség beépül a teljesítménycélok közé a vállalati kockázatkezelés hatékonyságának eszközeként [109]. Az elvégzett elemzés kimutatta, hogy 2006-ról 2020-ra nőtt a kockázatkezelési vezetőt vagy azzal egyenértékű beosztást alkalmazó vállalatok aránya, és a vállalati kockázatkezelési programmal vagy azzal egyenértékű programmal rendelkező vállalatok aránya. Az utóbbi esetében dinamikus növekedés volt megfigyelhető, miszerint 2020-ban 140%-kal volt magasabb 2006-hoz képest [5].

Az integrált kockázatkezelés a jövő kockázatkezelésének tekinthető. Az integrált kockázatkezelési megoldásokat használó vállalatok főként központosított kockázati adattár létrehozására használják, de olyan további funkciókat is igénybe vehetnek, mint a kulcsfontosságú mérőszámok nyomon követése és monitorozása, a kockázatok összesítése és jelentések különféle paraméterek és dimenziók alapján, a munkafolyamatok automatizálása kockázat- és ellenőrzési értékeléshez és pontozáshoz (kockázat és kontroll önértékelés), elemzések használata [6]. A vállalatoknak a 88%-a fontos/nagyon fontos tényezőnek tartja a kockázatok azonosítását és értékelését a kockázatkezelésben, a vállalatok 28%-a pedig erős/nagyon erős tényezőnek a szervezetében [111]. A vállalatok átlagosan 16% kezdetleges szintre értékelte a kockázatkockázatkezelési gyakorlatok megvalósítását a kockázatazonosítás, kockázatértékelés, rangsorolás, kockázatkezelés és monitoring lépésekre vonatkozóan, és mindössze 6-7%-a jelez minden lépésre optimális érettséget [110].

A kockázatkezelési folyamat érettségének mértéke a nagyvállalatoknál általában magasabb, mint a kis- és középvállalatoknál. A komplex környezettel és üzleti modellekkel rendelkező nagyvállalatok nagyobb valószínűséggel használják az integrált kockázatkezelési megoldásokat [6]. A kockázattudatosság korrelál a szolgálati idővel [110]. Az ISACA et al. felmérése szerint az információ / kiberbiztonság a legkritikusabb kockázati terület [110]. A kiberbiztonsági és technológiai kockázat mindamellett magas, hogy a hagyományos kockázati tényezők megmaradnak [110]. A feltörekvő technológiák növelik az olyan fenyegetések és sebezhetőségek szintjét, mint a felhő alapú számítástechnika (cloud computing), az IoT, a gépi tanulás és az mesterséges intelligencia, a blokklánc (és/vagy a kriptovaluta) [110]. A kiberbiztonság köztudottan kulcsfontosságú kockázati terület az ipar 4.0 és 5.0 korszakában.

A COVID-19 világjárvány jelentősen befolyásolta a kockázati környezetet, sőt felerősítette az információbiztonság / kiberbiztonság fontosságát. A COVID-19 világjárvány hangsúlyozta a kockázatkezelés fontosságát, és a Deloitte Insights [5] globális kockázatkezelési felmérése szerint új fókuszterületekre mutatott rá, mint például az operatív reziliencia tervek az otthoni munkavégzéssel kapcsolatban, kiberbiztonság (egyre nagyobb probléma, amely a világjárvány miatt még jelentősebbé vált), magatartási és megfelelési kockázat kezelése (a nem megfelelő magatartás felismerésének kockázata és a szabályozási követelmények be nem tartásának kockázata), kockázattudatos kultúra fenntartása távoli munkavégzési környezetben és nyílt beszélgetések a kockázatokról (a magatartási kockázatok kezelése elengedhetetlen; az új munkavállalók integrációja nehezebb). Megnövekedett a hitelkockázat, és a csalás kockázata, például az ügyféladatokkal való visszaélés. A harmadik felekkel kapcsolatos kockázat kezelése – beleértve az adatvédelmet, a nemteljesítést, az etikátlan magatartást, az üzletmenet- folytonosság elvesztését – kiemelt cél. A három védelmi vonal modell (3.3. fejezet) alkalmazása a felmérés szerint kihívásokkal jár, leginkább az első vonal feladatai és képességei tekintetében. Az adatvédelem / GDPR [112] területét a válaszadók többsége hatásosnak jelölte a felmérés adatai szerint. A kiberbiztonsági kihívások között a szervezeteknek kezelniük kell a következőket: a technológia változásait és fejlődését; a fenyegetések típusának változásait; a túl kevés biztonsági személyzet okozta erőforráskorlátot; a hiányzó készségeket a kiberbiztonsági csapat meglévő személyzetéből; a fenyegetések megnövekedett számát és/vagy a fenyegetés előfordulásának gyakoriságát; a nem megfelelő biztonsági költségvetést; a jogi és/vagy szabályozási kihívásokat; a vezetői támogatás/figyelem hiányát a biztonsági kérdésekben, vagy a kulcsfontosságú biztonsági területekre vonatkozó megfelelő politika hiányát [110].

Magas korreláció figyelhető meg a vállalatoknál jelenleg tapasztalt kiberbiztonsági kihívások rangsora és a következő 12 hónapban várható kihívások rangsora között (Spearman rangkorrelációs együtthatója 0,962) [S7]. Figyelembe véve azt, hogy a vállalatok a jövőben is ugyanazokkal a kiberbiztonsági kihívásokkal számolnak, megállapítható, hogy szükség van a kiberkockázat csökkentését szolgáló módszerekbe és eszközökbe való befektetésre. Ezek megvalósítása ugyanis várhatóan jelentősen csökkenti a kiberkockázatot. Valójában a legtöbb vállalat a kockázatkezelési folyamat eredményeit elsősorban az olyan tevékenységekben látja, mint a mindennapi végrehajtásban dolgozó emberek bevonása a kockázatok kezelésébe, a kockázatkezelők (risk manager) képzése az újonnan megjelenő kockázati területekről és technológiákról, új kockázatkezelési megoldás bevezetése, és integrált megoldás elfogadása a politika, az audit, a kockázat, és a megfelelőség területekre vonatkozóan [110]. A kiberbiztonsági hibák elleni leghatékonyabb hatáscsökkentő kontrollokat a következőképpen rangsorolták: figyelemfelkeltő tréning, katasztrófa utáni helyreállítás, irányítás (governance), titkosítás, harmadik fél által végzett értékelés, biztosítás és egyéb módon [110].

5.1.2. Vállalatok IKT biztonsága az Európai Unió tagállamaiban

A vállalati IKT biztonság területén végzett kutatások ritkán összpontosítanak a megtett intézkedések hatékonyságára. Jelen fejezetben az [S3] kutatási eredményeket ismertetem, mely a vállalati információbiztonság területét a technikai hatékonyság vonatkozásában térben, területi alapon a CCR Date Envelopment Analysis (CCR-DEA) modellel vizsgálta, és következtetéseket fogalmazott meg az Európai Unió (EU) tagországokban működő vállalatokra vonatkozóan. Az IKT biztonsági terület intézkedései az Európai Unió tagállamainak az Eurostat adatbázisból lekért másodlagos adatai alapján kerültek meghatározásra.

Az aktív vállalatok a gazdaságilag fejlett országokban gyakrabban alkalmaznak sokkal fejlettebb technológiákat, mint a kevésbé fejlett országok vállalatai, ami sebezhetőbbé teszi őket a kibertámadásokkal szemben [113; 114; 115]. Következésképpen ezek a vállalatok több biztonsági incidensnek vannak kitéve, ami szükségessé teszi a sokkal nagyobb információbiztonsági kiadások vállalását.

Az IKT-biztonság meghatározott szintjének elérése érdekében a kiadások hatékonyabb tervezési lehetőségeinek feltárása hozzájárulhat a kiépített IKT kockázatkezelési rendszereik fejlesztéséhez. A vállalatok IKT-biztonsági intézkedéseinek hatékonysága kulcsfontosságú vállalatirányítási szempontból. A digitális technológiák terjednek, és a vállalatoknak folyamatosan figyelniük kell az IKT-biztonsági kérdésekre.

Az IKT-technológiák számos új lehetőséget nyitnak meg a vállalatok előtt. A menedzsmentnek azonban összpontosítania kell a hatékony biztonsági eljárások tervezésére és fenntartására a vállalatuk megfelelő védelmének biztosítása érdekében.

5.1.3. Vállalatok ipar 4.0 és 5.0-hoz kapcsolódó szervezeti és kompetencia kihívásai az EU-ban

A digitalizáció, a mesterséges intelligencia megoldásainak elterjedése, és a robotizáció új ipari korszakok – az ipar 4.0, és ipar 5.0 – kereteit formálják. Az ipar 4.0, és ipar 5.0 által leírt ipari forradalmak jelen kockázati környezetben meghatározók, melynek szervezeti és kompetencia kihívásait [S9] alapján mutatom be. Ezek az ipari forradalmak erős hatást gyakorolnak a humánerőforrás-gazdálkodásra, az emberek által végzett munkákra, és komoly biztonsági fenyegetést is jelentenek a vállalatok számára, melyeknek megfelelő kezelése szükséges. Az új munkamódszerek elfogadása stratégiai megfontolásokat, végrehajtási döntéseket, valamint megbízható változásmenedzsment folyamatokat igényel a vállalat minden szintjén, mint például a felső vezetés elkötelezettsége, a projektek megvalósítása (költségvetés tartása stb.), valamint a humán erőforrás, információtechnológiai, illetve vállalatbiztonsági szempontok.

A szekunder adatok alapján elvégzett elemzés a munkavállalói kompetenciákat vizsgálta a digitális átalakulások korszakában az Európai Unió tagállamaiban. Az elemzés rámutatott a számítógépes és digitális készségek jelentős szerepére, különösképp az ipar 4.0 és ipar 5.0 korszakában.

A digitális és számítógépes ismeretek elengedhetetlenek az emberek és az új technológiák közötti teljes együttműködés megvalósításához. A jövő munkavállalóit fel kell szerelni a megfelelő digitális készségekkel ahhoz, hogy robotokkal és gépekkel együtt tudjanak dolgozni [116]. Peng [117] bizonyította, hogy a számítógépes ismeretek befolyásolják a munkavállalók foglalkoztatását, nevezetesen csökkentik az elbocsátást, és megkönnyítik az újrafoglalkoztatást. Emellett a számítógépes ismeretek szükségesek, különösen vezetői és tudásintenzív pozíciók esetén [117]. Falck et al. rámutatott az IKT-ismeretek relevanciájára a mai munkaerőpiacokon [118]. Pedersen et al. kutatásaikat arra összpontosították, hogy rámutassanak az információtechnológiába és a képzett munkaerőbe történő befektetés előnyeire a vállalat számára [119]. Az ipar 4.0 és 5.0 megoldások megvalósítása megköveteli a vállalatoktól, hogy IKT-kompetenciával rendelkező személyzetet vegyenek fel. A digitális átalakulás nyomást gyakorol a képzett munkaerőre [120], különösen azért, mert az ipar 5.0 több képzettséget igénylő munkahely megteremtését segíti elő az ipar 4.0-hoz képest, mivel az embereknek gépekkel kell együtt dolgozniuk [121; 122].

Az Európai Unió különböző országaiban élő lakosság digitális és számítástechnikai ismereteit elemezve megállapítható, hogy ezen országok gazdasági és technológiai fejlettségétől függően hasonlóságok mutatkoznak ezen készségek szintjében. A Nyugat-Európához tartozó országokat az egyének digitális és számítógépes készségei tekintetében hasonló szint jellemzi, mint az észak-európai országokat. Külön klaszterek alkotják Közép- és Kelet-Európa országait.

A vizsgálat eredményei szerint az Európai Unió országai nincsenek megfelelően felkészülve az ipar 4.0 és 5.0 bevezetésére. Ezt fejezi ki az IKT szakértőket alkalmazó vállalatok alacsony százaléka, valamint az IKT-szakismeretet igénylő munkakörökbe toborzott vagy munkaerőt toborozni kívánt vállalatok alacsony százaléka és annak változásai 2020-ban 2012-höz képest. Az IKT-szakértőket alkalmazó vállalatok arányának egyértelmű növekedése volt megfigyelhető az Európai Unió néhány országában, és ezek főként kelet-európai országok voltak. Következésképp az EU országokban a releváns kompetenciák és készségek további fejlesztésére van szükség.

5.1.4. A szabványos irányítási rendszerek elemzése

Az "ISO Survey of Certifications" egy évenkénti felmérés az ISO irányítási rendszer szabványainak megfelelő érvényes tanúsítványok számáról világszerte, melynek az eredményeit [S12]-höz kapcsolódóan dolgoztam fel. Az adatszolgáltatók az IAF MLA tagok – azaz a Nemzetközi Akkreditációs Fórum (IAF) Multilaterális Elismerési Megállapodásokat (MLM) aláírt tagjai – által akkreditált tanúsító testületek [123]. A felmérési adatok alapul szolgáltak a tanúsítási típusok és ágazati felosztásuk saját elemzéséhez az Európai Unió (EU) tagállamaira vonatkozóan. A lefedett Nemzetközi Szabványügyi Szervezet irányítási rendszerekre vonatkozó szabványait a 6. táblázat tartalmazza.

A tanúsítványok típusonként történő elemzése az Európai Unió (EU) tagállamaiban (EU-27) – amely saját feldolgozás az [124] alapján – azt mutatja, hogy az összes tanúsítvány domináns 68% az ISO 9001 minőségirányítási szabványhoz kapcsolódik. Ez nem meglepő, mivel a minőségirányítási rendszer szabványa támogatja a szervezeteket célkitűzései és céljai elérésében, dokumentálja a folyamatokat, irányelveket, szerepköröket és felelősségeket, hogy megfeleljen a vevői elégedettségnek, valamint a szükséges törvényi és szabályozási követelményeknek. Az ISO 9001 szabvány hét alapelvre épül: vevőközpontúság, vezetés, emberek bevonása, folyamatszemlélet, fejlesztés, bizonyítékokon alapuló döntéshozatal és kapcsolatmenedzsment [125; 167].

A második leggyakoribb szabvány az ISO 14001:2015 Környezetirányítási rendszerek szabvány, amely segíti a szervezeteket a megfelelőségi kötelezettségek teljesítésében és a környezetvédelmi célok elérésében, a környezeti teljesítmény fokozásában, a hulladék és a kibocsátás csökkentésében [126; 168]. A harmadik leggyakoribb szabvány az ISO 45001 Munkahelyi egészségvédelmi és biztonsági irányítási rendszerek szabvány. A munkahelyi egészségvédelmi és biztonsági szabvány alapvető és fontos minden ágazatban, mert előmozdítja a biztonságos és egészséges munkahelyeket [182]. Az ágazati felosztás is közel egyenlő megoszlást mutat a megnevezett ágazatokban, az egyetlen kiemelkedő ágazat az építőipar volt. Az építőipar számos kritikus biztonsági kockázatot hordoz magában, ami indokolja a tanúsítások legmagasabb gyakoriságát ebben az ágazatban. Az első három szabvány a vizsgált populáció 94,1%-át fedi le.

A tanúsítványok ágazati felosztása az EU-27-ben 39 gazdasági ágazat szerint történt. Az ágazati elemzés saját feldolgozás a [127] alapján. Az eredmények azt mutatják, hogy a tanúsítványok megoszlása az egyes szabványokhoz kapcsolódóan viszonylag egyenletes volt az egyes ágazatok között, néhány – jellemzően ágazatspecifikus – koncentrációval. A tanúsítványok számának körülbelül a felénél ismeretlen a szektor, mely kategória nem használható elemzési célú információk lekérésére.

Az ISO 9001 tanúsítványok többnyire a nagy- és kiskereskedelemhez, gépjárműjavításhoz tartoznak; motorkerékpárok és személyi és háztartási cikkek; fém termékek; építőipari és egyéb szolgáltatások (gyakoriságonként kb. 5% ágazatonként). Az ISO 14001 tanúsítványok gyakorisága hasonló eredményeket mutat, mint az ISO 9001 tanúsítványok gyakorisága, az építőipar kivételével. Az építőiparban az ISO 14001 szabvány 9,5%-os relatív gyakorisága a környezetirányítási rendszerek kiemelkedő szerepét mutatja az ágazatban. Ráadásul az ISO 45001 tanúsítványok 13%-a az építőiparhoz tartozik, ami megfelel az elvárásoknak és mutatja a munkahelyi egészségvédelem és biztonság jelentős szerepét ebben a szektorban. Az ISO 45001 és az ISO 14001 tanúsítványok eloszlása hasonló.

Az információtechnológiai szektorban a leggyakoribb az ISO/IEC 27001 (35,5%), az ISO / IEC 20000-1 (35,7%) és az ISO 22301 (12,7%) tanúsítvány megszerzése. Az ISO/IEC 27001 tanúsítványok 35,5%-a az információtechnológiai szektorba tartozik, ami jól mutatja az információbiztonsági irányítási rendszerek és az információbiztonsági kockázatok kezelésének központi szerepét az IT szektorban. Az ISO IEC 20000-1 tanúsítványok 35,7%-a és az ISO 22301 tanúsítványok 12,7%-a kapcsolódik az IT szektorhoz. Az említett szabványok az IT-biztonságra [174], az IT-szolgáltatásmenedzsmentre [169] és az üzletmenet-folytonosságra (BCM-re) [170] helyezik a hangsúlyt, amelyek mindegyike kulcsfontosságú az IT szektorban.

Az információtechnológiai szektorban az ISO/IEC 27001 és ISO 9001 szabványok mutatják a legmagasabb számokat az ISO tanúsítványok tényleges számát illetően. Ez mutatja a minőségirányítási rendszerek alapvető szerepét ebben az ágazatban.

Az ISO/IEC 27001 szabvány az információbiztonsági irányítási rendszerekre (IBIR) vonatkozik, és az információbiztonsági célok elérését szolgálják, azaz a titoktartást, az integritást és a rendelkezésre állást és segíti a szervezeteket az információbiztonsági kockázatok szisztematikus kezelésében. Az információbiztonság szerepe a folyamatosan változó világban rendkívül kritikus, ami indokolja a kapcsolódó irányítási rendszer szabványok rangsorolását. A piaci szereplők magas elvárásokat támasztanak az IT szektor vállalataival szemben. Az eloszlások vizsgálata azt mutatja, hogy a vizsgált sokaság IT szektorba tartozó szereplőinek körében jellemző a Nemzetközi Szabványügyi Szervezet kapcsolódó IT biztonságra, IT szolgáltatásmenedzsmentre és üzletmenet-folytonosságra vonatkozó irányítási rendszerszabványainak alkalmazása és megfelelőségük tanúsítványokkal történő igazolása.

5.1.5. Következtetések

A ma vállalata a digitális átalakulás világában működik. A vállalatoknak az információs és kommunikációs technológiákat az üzleti célok szolgálatába kell állítaniuk, megfelelően kell reagálniuk a változásokra, és emellett fel kell készülniük az üzleti és kockázati környezet fenyegetéseire. A digitális transzformáció átalakította a vállalati folyamatokat, az információs és kommunikációs technológiák széleskörű térnyerése következtében fellépő digitális kockázatok naprakész és adekvát kockázatkezelési folyamatokat követelnek meg.

A fejlett technológiák alkalmazása sebezhetőbbé teszi a vállalatokat az IKT incidensekkel, illetve kibertámadásokkal szemben. Ezen vállalatoknak magasabb a kitettsége a biztonsági incidenseknek, következésképp magasabb az információbiztonsággal kapcsolatos költségük és ráfordításuk, melyet a gazdaságilag fejlettebb országok esete példáz. Az IKT-k növekvő dominanciája az IKT biztonsági kérdések kezelését középpontba helyezi. A digitális korban az információbiztonság vállalatbiztonságban betöltött szerepe kulcsfontosságúvá vált.

A digitális forradalmakhoz, az ipar 4.0, és ipar 5.0-hoz köthető változások a kompetenciák és készségek vonatkozásában új kívánalmakat fogalmaznak meg. A digitális transzformáció szükségessé teszi, hogy a vállalati folyamatokban részt vevő emberi tényező az elvárt digitális kompetenciákkal és készségekkel rendelkezzen. A digitális és számítástechnikai készségek és kompetenciák fejlesztése kulcsfontosságú.

A hatékony belső kontrollfolyamatok kialakításának eszköze az integrált kockázatkezelés, a kockázatkezelési rendszer stratégiai célkitűzésekből történő levezetése, és beépülése a működési folyamatokba. A szabványos irányítási rendszerek hozzájárulnak a kapcsolódó vállalati folyamatok megfelelő működéséhez, és elősegítik a vállalati stratégia megvalósítását.

5.2. A biztonsági háló meghatározó elemeit feltáró szakértői kutatás

A biztonsági háló meghatározó tényezőinek azonosításához kapcsolódóan szakértői kutatást végeztem, melyet a megalapozott elmélet módszertana alapján elemeztem. A szakértői kutatás keretei között vizsgáltam a vállalatok nyereségorientált szemlélete és a biztonságos vállalati működés közötti kapcsolatot, azaz hogyan fér össze a profitorientáció, és az elsődlegesen eredménytartalék, illetve működő tőke csökkentő tételek formájában megjelenő biztonság területe. Vizsgáltam azt, hogy hogyan valósítható meg a biztonsági folyamatok, és kontrollok sikeres implementálása az üzleti folyamatokban. Ehhez kapcsolódóan kutattam a digitális átalakulás biztonsági aspektusait, a változások kontrollkörnyezetre gyakorolt hatásának, illetve a megváltozott digitális kompetencia-, és készségkövetelmények oldaláról. A kutatás fontos vetülete volt a biztonsági kultúra intézményesítése, és az adaptív ellenálló képesség, azaz a reziliencia megteremtése vállalati, és munkavállalói oldalról.

A szakértői kutatás eredményei a folyamatos iterálás eredményeképp kerültek meghatározásra. Az összefoglalót a kutatási kérdések vezérfonala mentén készítettem. A főbb összefüggéseket a 4-9. ábrák segítségével mutatom be. Az ábrák a grounded theory kódolási eljárás eredményeképp megalkotott modellek, és irányítatlan hálózatok formájában szemléltetik a kutatás eredményeit.

5.2.1. Biztonság nyereségorientált vállalati szemléletben

Vállalatbiztonság illeszkedése a profitcentrikus üzleti világba

A vállalatbiztonság témájára az üzleti folyamatok zavartalan működéséhez szükséges lételemként kell tekinteni, annak szerves részeként kell kezelni, mely a megfelelő kontrollokon keresztül tud megvalósulni. A profitcentrikus üzleti világban a sikeres, hosszú távú működés érdekében a biztonságra folyamatosan áldozni kell. Fundamentális annak a jelentősége, hogy a vállalatvezetők miként tekintenek a vállalatbiztonsági kérdésekre. A digitalizáció fejlődésével párhuzamosan az információbiztonsági kérdések kezelése egyre nagyobb hangsúlyt kap. Az információbiztonság megteremtése alapvető szükségességű.

Egy vállalat vonatkozásában a biztonságra fordított éves költségvetésben jelenik meg nominálisan a biztonságra fordított összeg. A pénzügyi erőforrásokért folytatott küzdelemben a döntéshozók részéről mindig mérlegelni kell azt, hogy az esetlegesen bekövetkező káresemény mekkora kárt okozhat. A profitorientált vállalatok az eredmény nagyságának maximalizálásában érdekeltek, melyből a hosszú távú sikeres működés érdekében a biztonságra, illetve a biztonsági beruházásokra áldozni kell.

Mindezt láttatni kell a döntéshozókkal az erőforrásokért folyó küzdelem során. Tulajdonosi döntés eredménye, hogy a megtermelt pozitív nyereséget osztalékként kiveszik, eredménytartalékba kerül, és például beruházásokra költik.

A biztonsági megoldások elsődlegesen kockázatot kerülnek, melynek pénzben kifejezhető gazdasági haszna van, mellyel a Biztonsági kérdések gazdálkodói szemszögből szekcióban foglalkozom. A biztonsági szempontok az üzleti kapcsolatokban is érvényesülnek, ebből az aspektusból a biztonsági szempontokra való odafigyelés elősegíti a profitszerzést. Az adatbiztonsági elvárásoknak való megfelelés az vevőszerzés, és - megtartás előfeltételévé is vált. Jól példázza mindezt az a jellemző gyakorlat, melyet a megkeresett HR szolgáltató vállalat vezetője (a továbbiakban: a vizsgált HR szolgáltató vállalat) ismertetett, miszerint a vizsgált HR szolgáltató vállalatnál szinte minden ajánlattétel, illetve szerződéskötés részévé vált az, hogy az üzleti partnerek részére garantálni kell az adatok biztonságos kezelését. A vizsgált HR szolgáltató vállalat Magyarországon első a munkaszerződések és az ahhoz tartozó dokumentumok digitális aláírásában, mely szigorú biztonsági követelményeknek való megfelelést követel meg. Hasonlóan az interjú készítése során megkeresett szoftverfejlesztő vállalat vezetője (a továbbiakban: a vizsgált szoftverfejlesztő vállalat) ismertette, hogy a vizsgált szoftverfejlesztő vállalatnál a biztonsági szempontok már az ajánlat részét képezik, és ha a vevő elégedett a szolgáltatással, és ezzel növelni tudja saját ügyfelei elégedettségét, az újabb megrendeléseket is jelent. Amelyik vállalat a biztonsági szempontokkal csak utólagosan, illetve kérésre foglalkozik, az intő jel. Szoftverfejlesztő vállalatok esetében piaci követelménnyé is vált az, hogy a szolgáltató vállalatok minősítésekkel rendelkezzenek, jelesül a Nemzetközi Szabványügyi Szervezet ISO 9001 [167] és ISO/IEC 27001 [174] tanúsítványaival. A Nemzetközi Szabványügyi Szervezet irányítási rendszer szabványainak való megfelelés azt jelenti a piaci szereplők számára, hogy az adott vállalat egy bizonyos normaszintet követ, mely segíti a biztonságos működés megvalósítását, és ez erősíti az üzleti partnerbe vetett bizalmat. A megfelelő irányítási rendszerek kiépítése beruházást igényel. A kihelyezett szolgáltatásokkal foglalkozó vállalatok (outsourcing) esetében kritikus az adatbiztonság. A szakértői interjúkészítés során megkeresett kihelyezett szolgáltatásokkal foglalkozó, informatikai outsourcing szolgáltatásokat nyújtó vállalat vezetője (a továbbiakban: a vizsgált kihelyezett szolgáltatásokkal foglalkozó vállalat) ismertette, hogy a vállalata az első kihelyezett szolgáltatásokkal foglalkozó vállalat Magyarországon, amelyiknek sikeres információvédelmi auditja volt és megszerezte az ISO/IEC 27001 minősítést. Amelyik vállalat ilyen szintű sztenderdeknek megfelel, azt javallott versenyelőnnyé is formálni a piacon; mindez intézményesül a vállalati biztonsági kultúrában is.

A kockázatkezelésre, biztonsági folyamatokra érdemes olyan módon tekinteni, hogy az hozzájárul a vállalati eredményekhez, azáltal, hogy az incidensekhez kapcsolódó költségek, illetve kockázatok (például reputációs kockázat) nem merülnek fel. Továbbá, a vállalat által reprezentált biztonsági kultúra, illetve egyes biztonsági folyamatok az ügyfelek részéről is elvárásként jelennek meg. A biztonság eredendően nem termel profitot, azonban a biztonságos működésre való odafigyelés eladhatóvá tesz termékeket/szolgáltatásokat, hozzájárul az vevői elégedettség eléréséhez, és az üzletmenet-folytonosság biztosításához.

Biztonsági kérdések gazdálkodói szemszögből

A védelem kockázattal arányos megvalósítása alapvető szemlélet. Az incidens esetén felmerülő költségeket, ráfordításokat, illetve veszteségeket kell szembe állítani a biztonságra fordított költségekkel, illetve ráfordításokkal. A biztonságra fordított kiadások megtérülése incidens esetén válik nyilvánvalóvá. A biztonságra fordított kiadásoknak gazdasági haszna van. A kockázatok és a kockázatokkal arányos védelemmel kapcsolatos költségek kapcsolatát érdemes számszerűsíteni, mellyel előmozdítható a nyereségérdekelt vállalatok döntéshozatali folyamata. A biztonsági beruházások pénzügyi vetülete a hatékonyságszámításhoz vezethető vissza, azaz egy adott cél megvalósítása kevesebb költséggel, vagy egy adott összeg lehető optimális felhasználásával valósuljon meg.

Az információbiztonsági irányítási rendszer szabvány szerinti működtetésével az információbiztonsági kockázatok minimalizálhatók. Az információbiztonsági irányítási rendszer hozzájárul a vállalati biztonsági kultúra intézményesítéséhez, mely a napi működési folyamatok szerves részeként járul hozzá a biztonsági szint növeléséhez. A biztonsági előírások betartására informatikai területen jógyakorlat IT vezető / Chief Information Officer (CIO), illetve vállalatmérettől függően Chief Security Officer (CSO) alkalmazása.

A biztonság értéket jelent a vállalatok számára, gazdasági haszna van, melyet láttatni kell a döntéshozókkal. A biztonság értéke incidens esetén válik igazán láthatóvá. Felelősen gondolkodva a biztonsági kérdéseket az üzleti folyamatok részeként kell kezelni.

5.2.2. Biztonság a digitális korban

Digitális átalakulási projektek biztonsága

A digitalizációs fejlesztés megvalósítását ideális esetben mind a megrendelő mind a fejlesztő sikerként éli meg, mely a vevői elégedettségben (bevétel növelése, kiadás csökkentése, jobb szolgáltatások nyújtása; újabb funkciók kérése, jóhírnév keltése), illetve a sikeres projekt-menedzsment tevékenységen keresztül testesül meg. A projektekhez kapcsolódóan a kockázatelemzés kiemelt szerepű, melynek részeként többek között a jogszabályi megfelelőségre különös figyelmet kell fordítani, ideértve a GDPR [112] megfelelőséget is. A sikeres digitális működéshez megfelelő technológia, technikai elemek / háttér, folyamatok, munkamódszer, és emberi tényezők szükségesek.

A digitális átalakulás sikere érdekében kiemelt vezetői feladat a munkavállalói elkötelezettség megteremtése a változáshoz, a folyamatokban érintett, illetve részt vevő emberek bevonása és megnyerése a projekt sikere érdekében. Az emberi tényező felkészítésének része a megfelelő technikai háttér biztosítása (például hozzáféréskezelés, bizalmasság biztosítása, kontrollált hozzáférés a munkaállomáshoz, virtuális magánhálózat használata távoli munkavégzésnél) és nem utolsó sorban a megfelelő kommunikáció, elfogadtatás a munkavállalókkal. Projektek esetében kritikus, hogy a változásokat az érintett emberek elfogadják-e.

Sokszor triviálisnak tűnő tényezők azok, amin egy átalakulási projekt sikere múlik. A kockázatok sikeres kezelése érdekében IKT fejlesztési projektbe információbiztonsági csoport aktív bevonása már a nulladik lépésben meg kell, hogy történjen. A biztonsági aspektusra a digitális megoldás fejlesztési projektek esetén áldozni kell. A megrendelő részéről a projekt kockázatmenedzsment folyamat részeként ezt kezelni kell. Javasolt olyan szoftverfejlesztő partnerrel szerződni, akinek biztonságos szoftverfejlesztésre minősítése van. Komfortot jelent, ha már az árajánlat részét képezi a biztonsági aspektus.

A digitális átalakulási projektek sikere szempontjából meghatározó, hogy a digitális megoldás fejlesztési folyamat kezdetétől fogva a biztonsági szempontok érvényesüljenek, és az, hogy az emberek a változásokat elfogadják és támogassák.

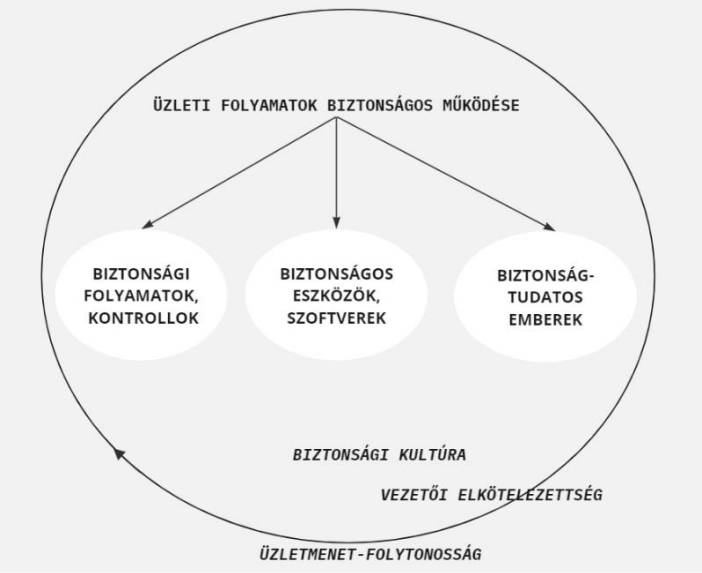
Üzleti folyamatok biztonságos működése

A vezetői elkötelezettség fundamentális eleme az üzleti folyamatok biztonságos működésének. Pragmatikusan elmondható, hogy a biztonsági szabályzatok lefektetése és követése, és az információbiztonsági irányítási rendszer működtetése olyan átfogó követelményrendszert fogalmaz meg, melynek betartása növelheti a működésbiztonság szintjét.

Az üzleti folyamatok biztonságos működése szempontjából a vezetői elkötelezettség kardinális jelentőségű. Az üzleti folyamatok biztonságos működéséhez szükséges komponensek (4. ábra):

- „biztonsági folyamatok”, kontrollok: A folyamatok esetében kontrollált, illetve szabályozott folyamatok szükségesek, például a Nemzetközi Szabványügyi Szervezet információbiztonsági irányítási rendszerekre vonatkozó szabvány szerinti folyamata. A folyamatok folyamatos kontrolljára, és fejlesztésére alkalmas a PDCA ciklus (plan-do-check-act, tervezés, célok meghatározása - tervek megvalósítása – eredmények ellenőrzése - korrigálás), mint módszertani eszköz és fejlesztési szemlélet alkalmazása. A Nemzetközi Szabványügyi Szervezet irányítási rendszerekre vonatkozó szabványaira úgyszintén a folyamatos fejlesztési szemlélet jellemző.
- „biztonságos eszközök”: bevizsgált, lehetőleg tanúsított eszközök, szoftverek, azaz a termék feleljen meg a vonatkozó biztonsági követelményeknek. Biztonságos szoftverfejlesztésre minősítéssel rendelkező vállalatok esetében a fejlesztési folyamat része a biztonsági ellenőrzés, mely követendő jógyakorlat. Informatikai fejlesztésekkel foglalkozó vállalatoknak általában van egy DevOps csapata, mely figyel a biztonságos fejlesztésre. Szoftverfejlesztés esetén javasolt, hogy külsős auditor végezze a biztonsági szabályzatok ellenőrzését, fejlesztés alatt és bevezetés előtt is.
- biztonságtudatos emberek, „biztonsági kultúra”, és a „humán kockázatok kezelése”: A munkavállalók biztonság terén betöltött szerepe kritikus. Az emberi tényezőhöz kapcsolódóan elsődleges a biztonságtudatosság szerepe, melyhez tudatosításra, és a munkavállalók megfelelő támogatására van szükség.

A 4. ábrán szereplő kulcstényezőket a grounded theory módszertan alapján határoztam meg.



4. ábra Üzleti folyamatok biztonságos működése (Forrás: Saját szerkesztés.)

Biztonsági hiányosságok digitális átalakulással összefüggésben, javaslatok

Tipikus biztonsági hiányosságok többek között a szabályzatok megsértéséből fakadó biztonsági hiányosságok; levelezésbe ágyazott támadások véletlen áldozatává válni; jelszavak gondatlan megválasztása; informatikai fejlesztés végén nem az éles környezetbe szánt verzió kerül élesítésre; nem állítanak be kétfaktoros autentikációt egy szoftverben. Bármilyen szofisztikált technológiai megoldást a nem megfelelő emberi interakció sebezhetővé tesz. Ebből eredően a *tudatosítás***,** a kollégák megfelelő támogatása és a kontrollkörnyezet erősítése a biztonsági hiányosságok megelőzése érdekében elengedhetetlen. Tapasztalatból elmondható, hogy a legjobb tanulópénz az incidens maga, ahol sebezhető a folyamat, ott incidens következhet be.

A biztonságos működés megvalósításához *vezetői elkötelezettség* szükséges. A biztonsági szempont intézményesítéséhez alapvető javaslat a kontrollkörnyezet erősítése, ideértve a humán kockázatok kezelését. Továbbá, a védelem kockázatokkal arányos megvalósításához társuljon a biztonsági követelményeknek való megfelelés (például a megfelelés, GDPR), a szabályzat legyen a szervezet minden szintjén érvényes, vonatkozzon mindenkire, és alkalmazása legyen következetes a teljes folyamat során (például a biztonsági szempont legyen a teljes fejlesztési folyamat része). A biztonságról preventív módon előre érdemes gondolkodni, és valamennyi aspektust lefedve teljeskörűen kezelni. Ideális esetben megvalósul a biztonsági szempont mérhetővé tétele is. A biztonságos működés megköveteli az emberi tényező biztonságtudatos, illetve szabálykövető magatartását.

Biztonsági kontrollok digitális átalakulás projekthez kapcsolódóan

A kockázat mértékét az esemény valószínűségének és hatásának a mértéke határozza meg. A kontrollok szerepét demonstrálja az, hogy a biztonsági kontrollok hiánya esetén a legnagyobb hatású incidens is bekövetkezhet helyrehozhatatlan pénzügyi, és reputációs veszteséget okozva. Ebből kifolyólag a kontrollok eredményes működése kardinális jelentőségű. A kontrollok tervezése és működésének tesztelése a későbbi biztonságos működés záloga.

A biztonsági kontrollok eredményes működését egyszerű, könnyen használható szabályzatok mozdítják jól elő, például az üzletmenetfolytonossági terv esetében kritikus a könnyű használhatóság és aktualitás. A folyamatok ellenőrzésével magasabb biztonsági szint érhető el, például szükséges változás azonosításával összeférhetetlenség biztosítása, és feladatok elkülönítése (Segregation of duties) érdekében; a folyamatok formai és tartalmi ellenőrzésével a teljeskörűség érdekében vagy üzleti modellező szoftverek használatával.

A vezetői elkötelezettségen alapulóan kialakított információbiztonsági irányítási rendszer szabvány szerinti folyamatok komfortot jelentenek, biztonságot adnak a folyamatok megfelelőségéről. A folyamatok Nemzetközi Szabványügyi Szervezet minőségirányítási, és információbiztonsági irányítási rendszerekre vonatkozó szabványai szerinti tanúsítása ellenőrzi a szabványban előírt követelményeknek való megfelelést.

Szoftverfejlesztéshez, és élesítéshez kapcsolódóan a fejlesztési projekt minden szakaszánál javasolt, hogy a biztonsági ellenőrzéseket külső auditor végezze, aki teszteli, és ellenőrzi biztonsági szempontból a szoftvert. A külső fél által lefolytatott ellenőrzéssel a folyamatvakság eliminálása biztosítható.

A digitális átalakulás projektekhez kapcsolódóan a kontrollok tervezése és működésük tesztelése a későbbi biztonságos működés záloga.

5.2.3. Eszközök a biztonságos működés intézményesítése érdekében

Digitális kompetencia-, és készségkövetelmények

A digitális naprakészség követelményének való megfelelés a digitális korban elengedhetetlen. Mindezt jól demonstrálja az, hogy a szoftveres megoldások jelen vannak a vállalati folyamatokban, az üzleti folyamatok szerves részét képezik, például bankok, biztosítók esetében. A mai digitális kor sajátossága az is, hogy értékes információ nyerhető az üzleti folyamatok fejlesztéséhez a vállalati döntéshozók számára az adatvédelmi szabályozással összhangban elvégzett adatelemzések révén. A digitális kor vívmányai a munkakörnyezetet is átalakították, jellemzővé vált az otthoni, illetve a távoli munkavégzés. Továbbá, a mesterséges intelligencia robbanásszerű térhódításával is foglalkozni kell. A tipikusan előreprogramozott válaszokat adó Chatbot-ok mellett megjelenő dinamikusan úttörő ChatGPT forradalmasítja a mesterséges intelligencia területét. A vállalatoknak képesnek kell lenniük arra, hogy a digitális kor eszköztárát használják mind technológiai, mind humán erőforrás oldalról egyaránt.

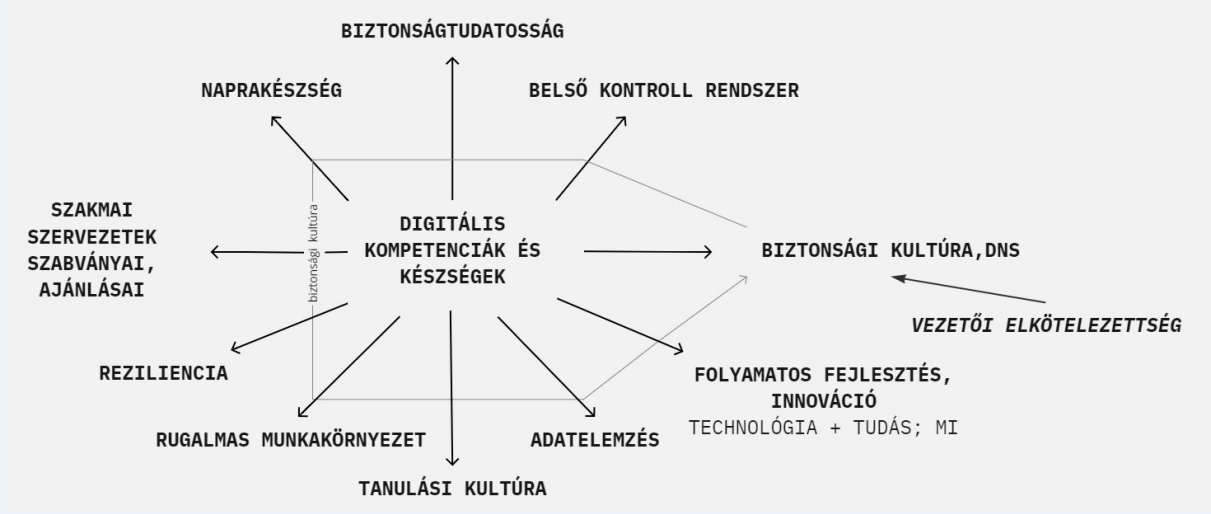
A digitális technológiák felhasználóinak lépést kell tartaniuk az új technológiai megoldásokkal, kompetens tanácsadók bevonásával frissíteni, illetve modernizálni kell a szoftvereket. Az IKT felelősök, az IKT csoport / osztály és partner szerepe meghatározó ebben. Szükséges a digitális tudatosság, és - naprakészség. Ennek elősegítése a munkavállalók folyamatos képzésén és fejlesztésén keresztül tud megvalósulni. Új munkavállalók esetében ezzel már a betanulás részeként foglalkozni kell.

A digitális megoldások fejlesztőinek szintén szisztematikusan folyamatosan tanulniuk, fejlődniük kell, folyamatos tapasztalatcsere, illetve konkrét kitűzött fejlődési célok mentén.

A megszerzett naprakész tudás a későbbi fejlesztésekbe hozzáadott értéket teremtve beépül, például magasabb biztonsági szint, rövidebb fejlesztési idő, hatékonyabb megoldások elérése révén. A folyamatos tapasztalatcsere rámutat a szaktudás, a technikai készségek mellett az interperszonális készségek fontosságára a szoftverfejlesztő csapaton belül, mely a projektmunka esetében is szükséges.

A kompetencia-, és készségkövetelmények biztosításának kulcsa a tudatosítás, a biztonságtudatos viselkedés elsajátítása és gyakorlása. Releváns értékes tudás nyerhető informatikával kapcsolatban az ISO/IEC 27000-es szabványcsaládból [172], az ISACA (Information Systems Audit and Control Association) által létrehozott Control Objectives for Information and Related Technologies (COBIT) keretrendszerből (COBIT 2019 [50]), a Projekt menedzsment Project Management Body of Knowledge-ból (PMBoK) [128], illetve az Adatkezelők Egyesületének / Data Management Association (DAMA) Data Management Body of Knowledge-ból (DMBoK) [129].

A szükséges kompetenciák és készségek a belső kontrollrendszert, és egyúttal a biztonsági kultúrát erősítik, és int. al. hozzájárulnak a reziliens reakciókészség biztosításához. Mindennek gyökere a vezetői elkötelezettség. A digitális kompetencia-, és készségkövetelmények összefüggéseit az 5. ábra tartalmazza, mely a a grounded theory kódolás eredményeképp készült modell.



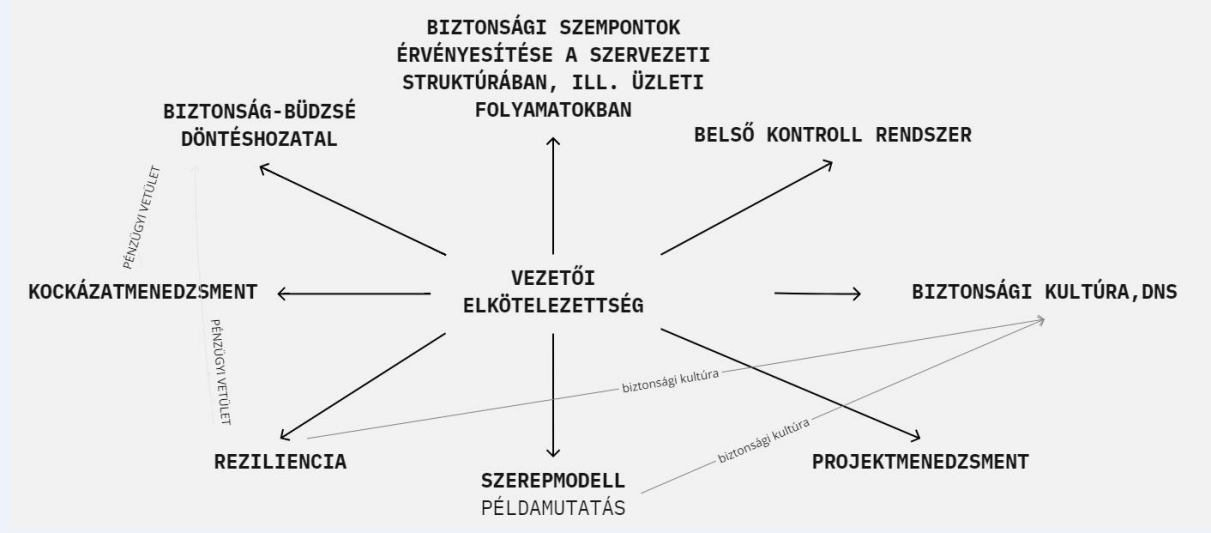
5. ábra Digitális kompetencia- és készségkövetelmények dimenziói (Forrás: Saját szerkesztés.)

A vállalatok digitális naprakészsége megköveteli a digitális technológia megoldások, és a megoldások felhasználóinak és fejlesztőinek naprakészségét egyaránt, mely folyamatos tanulás, és fejlesztés segítségével biztosítható.

Vállalati biztonsági kultúra és Vezetői elkötelezettség

A biztonsági kultúra építőköveit a vezetőség rakja le (6. ábra). Jelentőségteljes biztonsági kultúra kialakításához, mely képes hozzáadott értéket teremteni biztonsági aspektusból a legfontosabb a vezetői elkötelezettség. A vezetői elkötelezettség szerepe, megnyilvánulásai a biztonsági kultúra fejlesztésében, és előmozdításában a szakértői kutatás eredményei alapján:

- biztonsági kérdésekkel kapcsolatos döntéshozatal, megfelelő büdzsé allokálása a biztonság területre,
- folyamatos fejlesztések, új technológiai eszközök alkalmazása, innovációra épülő szervezeti kultúra, gyors és hatékony reakciók a változásokra,
- kockázatmenedzsmentben betöltött szerep, biztonságos működésre való odafigyelés, projekt esetében biztonsági kockázatok mérlegelése már a projekt indításakor,
- kommunikáció és képzés: biztonságtudatosság intézményesítése, tudatosítás, tréningek, jógyakorlatok megosztása, digitális kompetenciák, készségek, digitális érettség erősítése, képesség a kockázatok felismerésére és enyhítésére stb.),
- kontrollkörnyezet erősítése: biztonsági szabályzatok, folyamatok, illetve kontrollok az egyes működési területeken, Nemzetközi Szabványügyi Szervezet ISO/IEC 27001 szabványa szerinti információbiztonsági irányítási rendszer működtetése,
- vállalatvezető aktív érdeklődése a biztonsági kérdések iránt, folyamatos tanulási vágy,
- vállalatvezető szerepmodell is, példát mutat a munkavállalók felé,
- a vállalati arculat (corporate identity) része a biztonság. A vállalat közvetíti a kialakított biztonsági kultúrát a piaci szereplők felé is, akár versenyelőnnyé is tudja konvertálni. Ez segíti a biztonsági kultúra intézményesítését is.
- vállalati biztonsági kultúra nevezhető vállalati biztonsági DNS-ként is, a kialakított biztonsági kultúra jellemzi a vállalatot, illetve a vállalatbiztonságot; hordozza a vállalati biztonsági információkat és a vállalati működés részeként intézményesülve örökítődik.



6. ábra Vezetői elkötelezettség (Forrás: Saját szerkesztés.)

A 6. ábrán szereplő modellt a grounded theory kódolási eljárás alapján állítottam fel. A vállalati biztonságot meghatározó kulcstényezőket a vezetői elkötelezettség centrális jelleggel determinálja. és a kulcstényezői között hálózatszerű összefüggés azonosítható. A vállalati biztonsági háló, a vállalatot behálózó belső kontrollrendszer origója a vezetői elkötelezettség. A vezetői elkötelezettség hálózat jelleggel fogja át a vállalati biztonsági kultúrát. A vállalati biztonsági kultúrának felülről kell jönnie, a mindennapok részévé kell válnia, és nem kampányjelleggel működnie. A jelentőségteljes biztonsági kultúra kialakításához elengedhetetlen a biztonság szerepének tudatosítása. A biztonságtudatosság érdekében hatékony és eredményes eszközt jelentenek a folyamatos tudatosító tréningek, és gyakorlati példák, esettanulmányok megosztása, ahol bemutatják, és jól érzékeltetik, hogy a biztonsági szabályok be nem tartása milyen következményekkel járhat. A tudatosítás eszközeire jógyakorlat a játékos ismeretterjesztés vagy tematikus hírlevél útján történő tudatosító tevékenység[3], mely elősegíti az átadni kívánt tartalom közvetítését és érdemi tudatosítását.

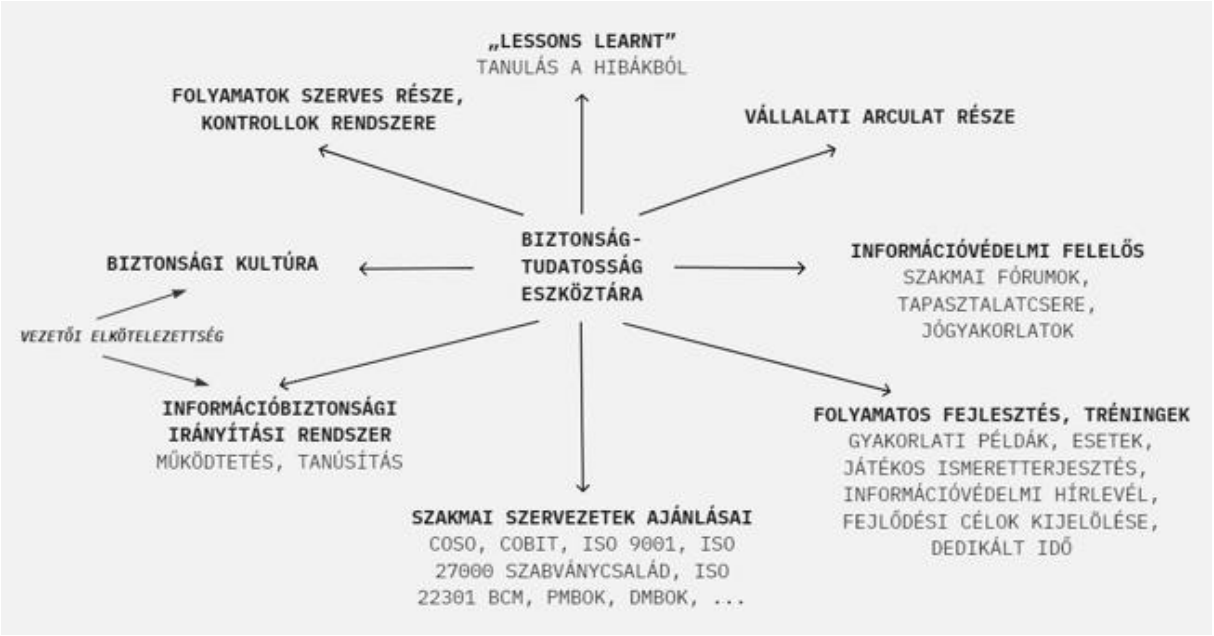
Kontrollok rendszerére, a biztonsági kontrollok vállalati folyamatokat, például HR, pénzügy, jog, IT folyamatokat lefedő hálózatára van szükség, mely együttesen tudja megvalósítani a biztonsági törekvéseket. A kontrollok rendszere, a belső kontrollhálózat a biztonsági kultúra leírása kontroll aspektusból. Az információbiztonsági irányítási rendszer működtetése olyan értéket jelent a szervezet számára, függetlenül attól, hogy tanúsíttatott vagy sem, mely hozzájárul a biztonságos működéshez. Az IBIR működtetése révén az információbiztonsági kockázatok eredményes kezelése megvalósítható. Mindez erőforrásráfordításokkal (pénz; idő) jár, de a működés során mindez megtérül és értéket jelent a vállalat számára.

A jelentőségteljes biztonsági kultúra a vállalat számára versenyelőnnyé is tud válni, a vállalati arculat részeként marketing-eszközként használható. Egy sikeres információbiztonsági auditra például a vállalat legyen büszke, és közvetítse is azt a piaci szereplők felé. Ilyen módon az emberekben a vállalatról kialakult benyomás, azaz a vállalat imázsának része is lesz, hogy a vállalat odafigyel a biztonságos működésre, és érdemes vele üzleti kapcsolatba lépni, például szerződni. Az ilyen elvek mentén kialakított vállalati biztonsági kultúra munkahelyi légkörében az emberek is biztonságban érzik magukat, mernek nyíltan beszélni az esetlegesen ejtett hibáikról, illetve merik tévedéseiket / hibáikat önként jelenteni, mely lehetővé teszi az incidensek / biztonsági esetek mielőbbi korrekcióját. Az incidens kivizsgálási folyamat mielőbbi elkezdése a potenciális veszteségek csökkentését is segíti.

[3] Az információbiztonság-tudatosság növelése érdekében alkalmazott gamifikációval az Óbudai Egyetemről is és a Nemzeti Közszolgálati Egyetemről is többen, például Rubóczki, E. és Oroszi, E. doktori értekezésben foglalkoztak.

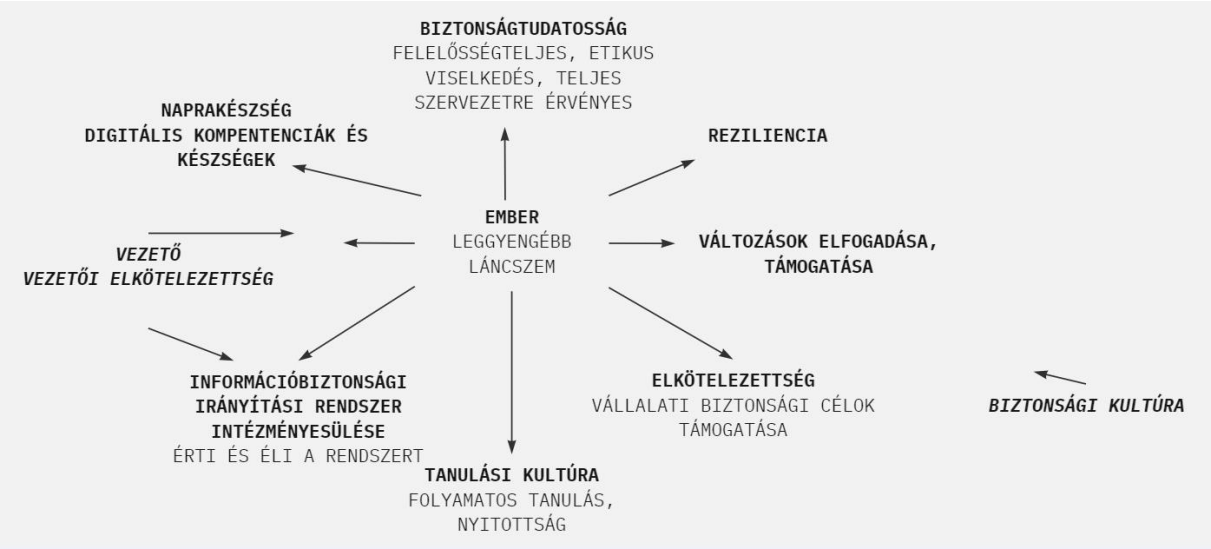
Az incidensek lezárásának részeként fontos elem a szervezeti szintű tanulás az esetből, illetve annak előmozdítása, hogy az incidens újból ne következzen be. Továbbá, a jelentőségteljes biztonsági kultúra légkörében a munkavállalók a folyamatokat javító / fejlesztő kezdeményezéseket is bátrabban mernek tenni.

A 7. ábra a szakértői kutatás során feltárt eszközöket foglalja össze, melyek a biztonságtudatosság intézményesítését szolgálják. Az egyes elemek összefüggenek, hatnak egymásra, egymást erősítik, ezért együttes jelenlétükre van szükség. A 7. ábra a biztonságtudatosság eszköztáráról áttekintő jellegű, egyes jelen pontban nem érintett elemek kifejtése más szakértői kutatási eredmény alszekciókban található. Az ábra a grounded theory kódolási eljárás eredményeképp felállított modellt mutatja be.



7. ábra Biztonságtudatosság eszköztára (Forrás: Saját szerkesztés.)

Az emberi tényező szerepét a biztonságban a 8. ábrán foglaltam össze. Az ábrán megjelenő kulcsszavak a grounded theory kódolás eredményei. Az emberi tényezővel kapcsolatos kockázatok kezelésének eszközei a tudatosítás, a biztonságtudatosság, a vállalati biztonsági kultúra, és kontrollkörnyezet erősítése, melyek biztosításához vezetői elkötelezettség kell. A munkavállalókat meg kell nyerni a változási projektekhez, nagyon fontos a felsővezetés által számukra közvetített üzenet. Egyidejűleg gondoskodni kell a változásokhoz kapcsolódóan a szükséges képzésekről és a készségek fejlesztéséről. A digitális érettség erősödése egyúttal a vállalati biztonsági kultúrát és a felölelő vállalati kultúrát is erősíti. A változások munkavállalókkal való elfogadtatása sikerkritérium. A COBIT 5 is kiemeli ugyanezt emberi viselkedés vonatkozásában [49; p.70].



8. ábra Az Ember szerepe a biztonságban (Forrás: Saját szerkesztés.)

Biztonság – az üzleti folyamatok elválaszthatatlan része

Ahhoz, hogy a biztonsági kérdések az üzleti folyamatok elválaszthatatlan részét képezzék vezetői elkötelezettség szükséges, meghatározó a „vezetőség hangja”, mely a pénzügyi erőforrások biztosítását is magában foglalja. Mindez a vállalati biztonsági kultúra aspektusa. 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.

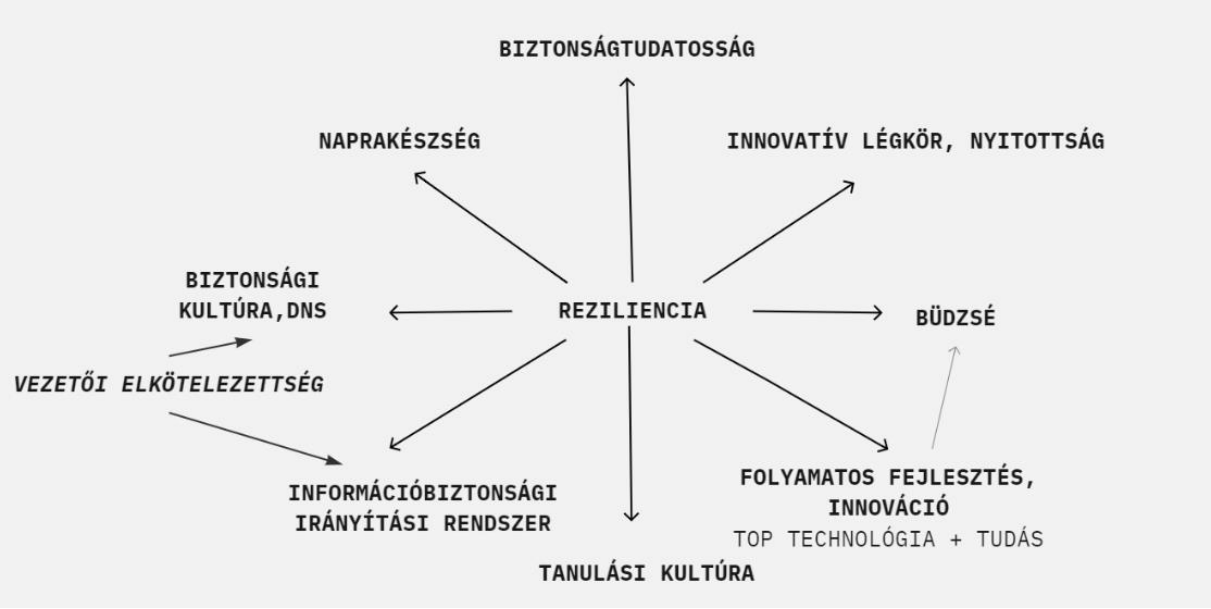
Jógyakorlat, hogy a digitális megoldás fejlesztési folyamatnak kezdetektől része a biztonsági szempont**,** például szoftverfejlesztéskor a vezérfonal (guideline) része a biztonság már ajánlatadáskor. A vevő számára is érték, garancia, ha a biztonságos működés biztosítása a szoftverfejlesztési folyamat szerves része. Fejlesztési projektek sikeressége szempontjából kritikus az információbiztonsági szempontok projekt kezdetén történő mérlegelése és megfelelő kezelése. Ez egyértelműnek tűnik, azonban rendkívül fontos hangsúlyozni, hogy valóban így is történjen, hiszen a tapasztalatok szerint sok esetben ez csak a korábbi tapasztalatokból tanulva, illetve problémákból okulva valósul meg (lessons learnt).

Reziliencia – adaptív ellenálló képesség

Az újonnan megjelenő biztonsági fenyegetéseknek való adaptív ellenállás gyors válaszkészséget, reakciót kíván, mely jellemzően erőforrás függvénye is. Vezetői elkötelezettség kell a reziliencia megteremtéséhez (9. ábra) a folyamatos fejlesztések és tanulás iránt, mely innovatív légkörben, és tanulási kultúrában testesül meg. A reziliens vállalatokat folyamatos biztonsági fejlesztések jellemzik, top technológiával rendelkeznek.

A folyamatos biztonsági fejlesztések finanszírozása kiadással jár, melyhez megfelelő mértékű büdzsé allokálása szükséges a biztonsági területre. Vezetői döntéshozatal kérdése a szükséges erőforrások biztosítása. Reziliens biztonsági folyamatok (biztonsági termékek, szabályrendszer, ellenőrzések, automatizmusok, megfelelő szerepkörök és felelősségek) szükségesek. A reziliens biztonsági törekvéseket ilyen célra létrehozott termék, szoftvermegoldás, illetve olyan szabályrendszer is tudja segíteni, mely a jellemzően jelentőségteljes, erős biztonsági kultúrához társul. A reziliencia érvényesülését segíti az irányítási rendszer intézményesülése a vállalati mindennapi működésben. A kockázatkezelés szerepével valamennyi érintettnek tisztában kell lennie, érteniük kell, hogy a kockázatok kezelése hogyan jelent értéket. Fel kell készülni arra, hogy a támadók egy lépéssel előbbre járnak. Fontos a tapasztalatcsere más szervezetekkel, illetve a jógyakorlatok megosztása, melyet maga az ISO/IEC 27000 szabvány is megfogalmaz jógyakorlatként. Javasolt, hogy a vállalati felelősök a releváns szakmai fórumokat látogassák annak érdekében, hogy az onnan megszerzett tudás birtokában a szükséges biztonsági lépéseket kezdeményezni tudják.

A 9. ábra a rezilienciához kapcsolódó grounded theory kódolási eljárás eredményeképp megalkotott modellt mutatja be.



9. ábra Reziliencia (Forrás: Saját szerkesztés.)

5.2.4. Következtetések

A kutatási eredmények igazolják, hogy a turbulens változások közepette a biztonsági törekvéseket hatékonyan és eredményesen megvalósítani egy olyan biztonságtudatos értékrend mentén lehet, amely a vezetői elkötelezettségen alapul, és a szükséges kontrollok működése biztosított. A kutatás során bizonyítottam, hogy a biztonsági háló sikeres működése mögött meghúzódó elsődleges feltétele a vezetői elkötelezettség. A vezetői elkötelezettség a vállalati biztonsági háló, a vállalatot behálózó belső kontrollrendszer origója.

A digitális átalakulási folyamathoz kapcsolódóan kritikus a biztonsági aspektus kezelése. A biztonsági szempontokról már a nulladik lépésben gondoskodni kell. A változások bevezetése során elsődleges a humán faktor kezelése, az emberek fejében a gondolkodásmód átalakítása, mely vezetői szintről eredeztethető. A szakértői kutatás rámutatott az emberi tényező biztonságban betöltött szerepére a technológiai tényezők mellett.

A szabványok szerint működtetett irányítási rendszerek jó eszközei a biztonságos működés megteremtésének, és alkalmasak a vállalati biztonság szintjének növelésére. Az irányítási rendszerek segítik a biztonsági kultúra intézményesítését, melynek részeként a biztonságtudatos felelős gondolkodás és viselkedés vállalati szinten megvalósul.

6. IRÁNYÍTÁSI RENDSZEREK BIZTONSÁGI JELLEMZŐI

A szakértői kutatás rámutatott a szabványos irányítási rendszerek biztonságban betöltött szerepére. Jelen fejezetben a szabványos irányítási rendszerek biztonsági jellemzőivel foglalkozom. A 6.1. fejezetben az irányítási rendszereket folyamat- és vállalatbiztonság szempontjából jellemzem. A 6.2. fejezetben az irányítási rendszerszabványok kontextusában felállított biztonsági csoportokat ismertetem és részletezem az egyes irányítási rendszerszabványok biztonságban betöltött szerepét.

6.1. Irányítási rendszerek biztonsági szerepe

Jelen fejezetben a szabványos irányítási rendszerek biztonsági szerepének kvalitatív tartalomelemzés módszerével történő vizsgálatát mutatom be [23; 24].

A vizsgálat tárgyát képező irányítási rendszerszabványokat a tanúsított irányítási rendszerekre vonatkozó felmérés [123] tárgyát képező irányítási rendszerszabványok alapján határoztam meg (6. táblázat). A felmérésben elérhető három szabvány a részletes elemzésből kikerült egyedi ágazati jellegük miatt, azaz az ISO 13485 Orvostechnikai eszközök Minőségirányítási rendszerek [184], az ISO 22000 Élelmiszerbiztonsági irányítási rendszer [185], és az ISO 39001 Közúti közlekedésbiztonsági irányítási rendszerek [186] szabványok. Az ISO 31000 kockázatkezelési szabvány irányítási szabvány, és nem irányítási rendszer szabvány [179]. Az ISO 31000 szabvány elősegíti a kockázatkezelés integrálását a vállalatirányítási rendszerbe, és ennek következtében erősíti a rendszert; megfelelő kockázatkezelési folyamatok kialakítását szolgálja, és folyamatbiztonsági szempontból fontos. Az ISO 31000 szabvány nem tanúsítható, ezért nem állnak rendelkezésre tanúsítási adatok, és ezért nem került az elemzés hatálya alá.

A szabványos irányítási rendszerek alkalmazása segíti a vállalatokat célkitűzéseik elérésében. A szabványok meghatározzák az adott irányítási rendszerek követelményeit, és jellemzi őket a biztonságorientáltság, melyet a 6. táblázatban kiemelésekkel szemléltetek. A folyamatok akkor működnek jól, ha teljesülnek a mögöttes biztonsági célok. „A folyamatok biztonsága hozhatja meg a teljes vállalati biztonságot [3]”. Az irányítási rendszerek működése folyamatorientált megközelítésű. Az irányítási rendszerszabványok céljai biztonságorientáltak. A szabványos irányítási rendszerek szisztematikus megközelítése, az átlátható folyamatok és az irányítási rendszer részeként meghatározott folyamatlépések listája a folyamatteljesítmény-menedzsmentet is támogatja.

6. táblázat Nemzetközi Szabványügyi Szervezet irányítási rendszerszabványai (Forrás: Kivonat a vonatkozó szabványokból: [167; 168; 174[4]; 182; 183; 170; 169; 177; 181]

Szabvány	Kivonat a szabvány hatályából
ISO 9001:2015 Minőségirányítási rendszer	… bizonyítani, hogy **képes következetesen olyan termékeket és szolgáltatásokat nyújtani, amelyek a vevők, valamint a vonatkozó törvényi és szabályozási követelményeinek megfelelnek**; *a vevői elégedettség fokozása* **a rendszer hatékony alkalmazásával**, beleértve a *rendszer fejlesztésére szolgáló folyamatokat*, valamint a vevőknek és a vonatkozó törvényi és szabályozási **követelményeknek való megfelelés biztosítását**
ISO 14001:2015 Környezetirányítási rendszer	… **környezetvédelmi teljesítmény** *javítása érdekében …*
ISO/IEC 27001:2022 *Információbiztonság, kiberbiztonság és adatvédelem* Információbiztonsági irányítási rendszerek*	… az információbiztonsági irányítási rendszer *folyamatos fejlesztése* a szervezeten belül; tartalmazza az **információbiztonság**i kockázatok felmérésére és kezelésére vonatkozó követelményeket a szervezet igényeihez igazítva
ISO 45001:2018 Munkahelyi egészségvédelem és biztonságirányítási rendszer	… lehetővé teszi a szervezetek számára, hogy **biztonságos** és egészséges munkahelyeket biztosítsanak a munkával összefüggő sérülések és rossz egészségi állapot megelőzésével, valamint a munkahelyi egészség és biztonság teljesítményük *proaktív javításával*
ISO 50001:2018 Energiagazdálkodási rendszerek	... lehetővé teszi egy szervezet számára, hogy *szisztematikus megközelítést* kövessen az energia*teljesítmény* és az energiagazdálkodási rendszerek (EnMS) *folyamatos javítása* érdekében
ISO 22301:2019 **Biztonság** és reziliencia – Üzletmenet-folytonossági irányítási rendszer (BCM)	**...** olyan irányítási rendszer *fejlesztése*, amely a fennakadások ellen **védelmet** nyújt, csökkenti azok előfordulásának valószínűségét, felkészül, reagál azokra és helyreállítja azokat, amikor felmerülnek.
ISO/IEC 20000-1:2018 Információtechnológia – Szolgáltatásmenedzsment – 1. rész: Szolgáltatásirányítási-rendszer	**...** a szolgáltatásmenedzsment rendszer (SMS) *folyamatos fejlesztése*. A jelen dokumentumban meghatározott követelmények magukban foglalják a szolgáltatások tervezését, létesítését és változtatását, nyújtását és fejlesztését, hogy **megfeleljenek a szolgáltatási követelményeknek és értéket nyújtsanak**
ISO 28000:2022 **Biztonság** és reziliencia - Biztonságirányítási rendszerek	… **biztonsági irányítási rendszer**rel szemben támasztott követelményeket határoz meg, … biztonsági irányítási rendszert kíván létrehozni, megvalósítani, fenntartani és *fejleszteni*
ISO 37001:2016 Antikorrupciós irányítási rendszer	… *antikorrupciós*, *megvesztegetés elleni* irányítási rendszer *fejlesztése.* A rendszer lehet önálló vagy integrálható egy átfogó irányítási rendszerbe

A szabványok a folyamatos fejlesztési szemléletmódhoz kapcsolódnak. Nagy hangsúly kerül bennük a fejlesztésre és a képzésre. Az irányítási rendszerek működése definíció szerint a Plan-Do-Check-Act (PDCA) cikluson alapul és folyamatorientált megközelítésű. Minden szabványban megtalálható a folyamatos fejlesztési gondolkodásmód beépített komponense, például a PDCA ciklus Korrigálás (Act) fázisában, amely az Ellenőrzési ciklus teljesítményértékelését követi, melyet a 6. táblázatban dőlt betűs kiemelésekkel szemléltetek. Ezek a tényezők hozzájárulnak a folyamatteljesítmény, és a folyamatbiztonság növeléséhez.

[4] Az ISO/IEC 27001:2013 Információtechnológia - Biztonsági technikák - Információbiztonsági menedzsment rendszerek, Technikai korrigendum 2014, & 2015 szabványt az ISO/IEC 27001:2022 Információbiztonság, kiberbiztonság és adatvédelem – Információbiztonsági irányítási rendszerek – Követelményszabvány módosította. A szabványok hatályára vonatkozó megfogalmazás azonos.

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 növeli a folyamatbiztonság szintjét. Az irányítási rendszerek tanúsítása bizonyítékul szolgál az irányítási rendszerek megfelelő működéséről, mely az üzleti kapcsolatokhoz is szükséges lehet.

Ami az információbiztonságot illeti, az ISO/IEC 27000 információbiztonság irányítási rendszerszabványok és irányelvek családja világszerte közös nyelvként szolgál a biztonságos üzleti tevékenységhez [162]. Az ISO/IEC 27000 szabványcsomagban a többi irányítási rendszer szabványhoz képest egyedülálló módon egy saját, információbiztonsággal foglalkozó kockázatkezelési szabvány is található (ISO/IEC 27005 [176]), mely mutatja a kockázatkezelés fontosságát az információbiztonság területén. Az ISO/IEC 27001 tanúsítvánnyal rendelkező vállalatnak minden biztonsági intézkedést be kell vezetnie, amelyet a szabvány előír [35]. Ezenkívül az ISO/IEC 27001 sikeres végrehajtása megköveteli, hogy az alkalmazottak teljes körű támogatását és hozzájárulását [35]. Tekintettel arra, hogy jelentős a vállalaton belülről származó kockázati kitettség [137; 164; 165], az információbiztonsági irányítási rendszer hozzájárul az emberi tényezőhöz kapcsolódó kockázatok csökkentéséhez.

Az információbiztonsági irányítási rendszer tanúsítása a szabványban előírt követelményeknek megfelelőnek minősíti a rendszert, segíti a bizalom építését a szervezetek kapacitásába, valamint csökkenti a kockázatokat, beleértve az üzleti veszteséget, a bírság kockázatát, illetve a jogi viták miatti kártérítési kifizetések, és segít megelőzni a biztonsági sérüléseket [29; 163].

6.2. Biztonsági csoportok

Az irányítási rendszerszabványokon alapulóan biztonsági csoportokat határoztam meg. Az egyes biztonsági csoportok különböző biztonsági szempontokat fednek le, melyeket jelen fejezetben ismertetek. A nyolc biztonsági csoport lefedi a vállalatok fontos és kritikus ellenőrzési területeit.

I. **Minőségirányítás** ISO 9001-re alapulóan: Az ISO 9001 minőségirányítási szabványnak megfelelően a szervezetek fenntartják, frissítik és felülvizsgálják a minőségi politikát, a szabványos működési eljárásokat, beleértve az üzleti folyamatokhoz kapcsolódó ellenőrzési tevékenységeket, hogy rendelkezzenek int. al. egyértelmű szerepkörökkel és felelősségekkel, dokumentumkezelő rendszerrel, aktuális szervezeti diagrammal és minden munkakörhöz/szerepkörhöz kapcsolódó munkaköri leírásokkal. Mindez segíti a szervezeteket abban, hogy olyan jól strukturált folyamatokat tartsanak fenn, amelyek ellenállóak a változások esetén, például kulcsfontosságú alkalmazottak távozása esetén; amelyek transzparensek és folyamatteljesítmény-mérőkkel mérhetők, és amelyek eszközként szolgálhatnak a folyamatos fejlesztési lehetőségek azonosításához. A minőségirányítási rendszer célja a vevői elégedettség biztosítása, amelyet mérni kell, hogy megkapjuk a szükséges visszajelzéseket a vevőktől (külső intézkedés), valamint rendszeres minőségirányítási auditokkal kell alátámasztani (belső intézkedés).

II. **Folyamatmenedzsment (belső)** ISO 22301, & 33001-re alapulóan: a belső üzleti folyamatok az vevőigények folyamatos kiszolgálásához szükségesek; megbízható és biztonságos üzleti működést kell biztosítaniuk. Az üzletmenet folytonosságát váratlan körülmények esetén is fenn kell tartani. A belső folyamatokat folyamatértékelésnek kell alávetni annak érdekében, hogy elérjék a kívánt minőséget, és azonosítani tudják a fejlesztési lehetőségeket.

III. **Információs technológiai - és információbiztonság** ISO/IEC 20000-1, & 27001-re alapulóan: az információtechnológiai szolgáltatások és az információbiztonsági irányítási rendszerek (IBIR) a bizalmassági, integritási és rendelkezésre állási célok biztosítását szolgálják. Az információs technológia mélyen beágyazott a vállalati folyamatokba, következésképpen a humán erőforrásokkal együtt szükséges a zavartalan üzleti működéshez. Az információbiztonság kulcsfontosságú a szervezetek számára.

Az információ- és IKT-biztonság megsértése súlyos következményekkel járhat, beleértve a közvetlen pénzügyi veszteséget, a rendszerek elérhetetlensége miatt az üzletmenet fennakadását, a titoktartási kötelezettség megsértését, az általános adatvédelmi rendelet megsértésével kapcsolatos bírságokat, a hírnévkockázatot. Információ-, és kiberbiztonsági kontrollokra, ellenőrzésekre van szükség a bizalmasság, a rendelkezésre állás és az integritás biztosításához. A biztonság megfelelő folyamatok és eljárások eredménye, amelyet támogatni kell technológiával, azaz különféle kockázatok kezelésére szolgáló biztonsági tevékenységekhez szükséges szoftvermegoldásokkal és emberekkel, akiknek rendelkezniük kell a megfelelő készségekkel, ismeretekkel, kompetenciákkal, például a social engineering támadások azonosításához.

IV. Humán erőforrás ISO 45001-re alapulóan: a humán erőforrás a megvalósuló üzleti folyamatok szerves része. A munkahelyi egészség és biztonság mindenkor alapvető fontosságú. Bármilyen biztonsági veszélyt, bármilyen kapcsolódó problémát, sérülést és eseményt komolyan kell venni, és utána kell járni, hogy a jövőbeni megismétlődés elkerülhető legyen.
Ezek az incidensek nemcsak az emberek biztonságát veszélyeztetik, hanem tényleges anyagi veszteséggé is válhatnak az időveszteség és a kapcsolódó üzleti folyamatokban elveszett termelés/értékteremtés miatt, következésképpen közvetlenül befolyásolják az üzleti eredményeket, és reputációs problémákat is okozhatnak. A munkahelyi egészség és biztonság esetek gondos nyomon követése kulcsfontosságú.

V. Ellátási lánc biztonsága ISO 28001-re alapulóan: az ellátási lánc biztonsága a termékek és szolgáltatások stabil szállítását eredményezi a vevők számára, és elengedhetetlen a rövid és hosszú távú üzleti sikerhez. Célszerű tanúsított minőségirányítási rendszerrel rendelkező partnerekkel történő üzleti kapcsolatok kialakítására törekedni.

VI. Energetikai és egyéb infrastruktúrák ISO 50001-re alapulóan: Az energetikai és egyéb infrastruktúrák legmegfelelőbb teljesítménymutatói elsősorban az üzleti profiltól függenek. A megfelelő teljesítménymutatók meghatározása érdekében a kapcsolódó folyamatokat részletesen elemezni kell. Napjaink energiaválsága a jól átgondolt energiafogyasztás szükségességét hangsúlyozza. A hatékony energiafelhasználás végső soron hozzájárul a működési költségek csökkentéséhez; így a termékek és szolgáltatások ára alacsonyabb maradhat, ami a vásárlói elégedettség szempontjából meghatározó jelentőségű. Továbbá elősegíti a környezettudatos fenntartható működést.

VII. Környezetirányítás ISO 14001-re alapulóan: a vállalati működés környezeti hatásainak minimalizálása A sikeres környezetirányítási folyamat fontos lépései a működés környezeti hatásainak tisztázása, a környezeti kockázatok és fejlesztési területek azonosítása.

VIII. Antikorrupció, vesztegetés elleni küzdelem ISO 37001-re alapulóan: A vesztegetés és a terrorizmus finanszírozása elleni küzdelem a vállalatok számára komoly témát jelent; szilárd alapokon nyugvó antikorrupciós ellenőrzésekre van szükség. A megvesztegetés elleni ellenőrzéseknek jelen kell lennie minden olyan környezetben, ahol a kockázat felmerülhet, például alkalmazottak, vevők, szállítók és bármely szerződő fél esetében.

6.3. Következtetések

A grounded theory módszertan alapján elvégzett szakértői kutatás (5.2. fejezet) igazolta az információbiztonsági irányítási rendszerek szerepét a biztonságos folyamatok és vállalati biztonság elérésében.

A szakértői kutatás igazolta, hogy a szabványos információbiztonsági irányítási rendszer működtetése hozzájárul a biztonságos működéshez és alkalmas a vállalati biztonsági szint növelésére. Továbbá, hogy a folyamatok ellenőrzésével magasabb biztonsági szint érhető el.
A szakértői kutatás megerősítette a tanúsított irányítási rendszerek szerepét az információtechnológiai szektorban a minőségirányítási és információbiztonsági irányítási rendszerek vonatkozásában, melyekre szükség és igény is van ebben a szektorban.

A szakértői kutatás mellett a szekunder adatelemzés eredménye is visszaadta a minőségirányítási és információbiztonsági irányítási rendszerek tanúsításának jelentőségét a szektorban. A szekunder adatelemzés szerint az információtechnológiai szektorban a Nemzetközi Szabványügyi Szervezet ISO/IEC 27001 és ISO 9001 szabványai mutatják a legmagasabb számokat a tanúsítványok tényleges számát illetően.

A szabványos irányítási rendszerekhez kapcsolva biztonsági területeket (kontrolling területeket) definiáltam, azaz olyan ellenőrzési területeket, mint a minőségirányítás, a folyamatmenedzsment, az információ technológia- és információbiztonság, az emberi erőforrások, az ellátási lánc biztonsága, az energia- és egyéb infrastruktúrák, a környezetgazdálkodás vagy a megvesztegetés elleni küzdelem.

7. A BIZTONSÁG TELJESÍTMÉNYMÉRÉSE

A fejezetben a vállalatbiztonság teljesítménymérésére alkalmas eszközt mutatok be (7.1. fejezet), és a vállalatbiztonság meghatározó területeit (6.2. fejezet) lefedő rendszert (7.2. fejezet) állítok fel. Az eszköz a biztonság értékét segít láthatóvá tenni.

7.1. Teljesítménymutatók alkalmazása

A folyamatok teljesítménymérésén keresztül a vezetőség rendszeres tájékoztatást kap arról, hogy a vállalat, egyes egységei és folyamatai hogyan teljesítenek, keretet ad az eltérések nyomon követésére, és segít a fejlesztési lehetőségek azonosításában. A teljesítménymérés során a teljesítmény PDCA ciklus szerinti kezelése a folyamatos fejlesztés lehetőségét építi be a teljesítménymérési folyamatba. A biztonsági teljesítménymutatók definiálásakor célszerű megtalálni a megfelelő egyensúlyt a mutatók proaktív módon történő meghatározásához, és nemcsak azokra az intézkedésekre koncentrálni, amelyek azt mutatják, hogy mi romlott el, mi nem működött megfelelően, hanem a biztonsági folyamat eredményeire is.

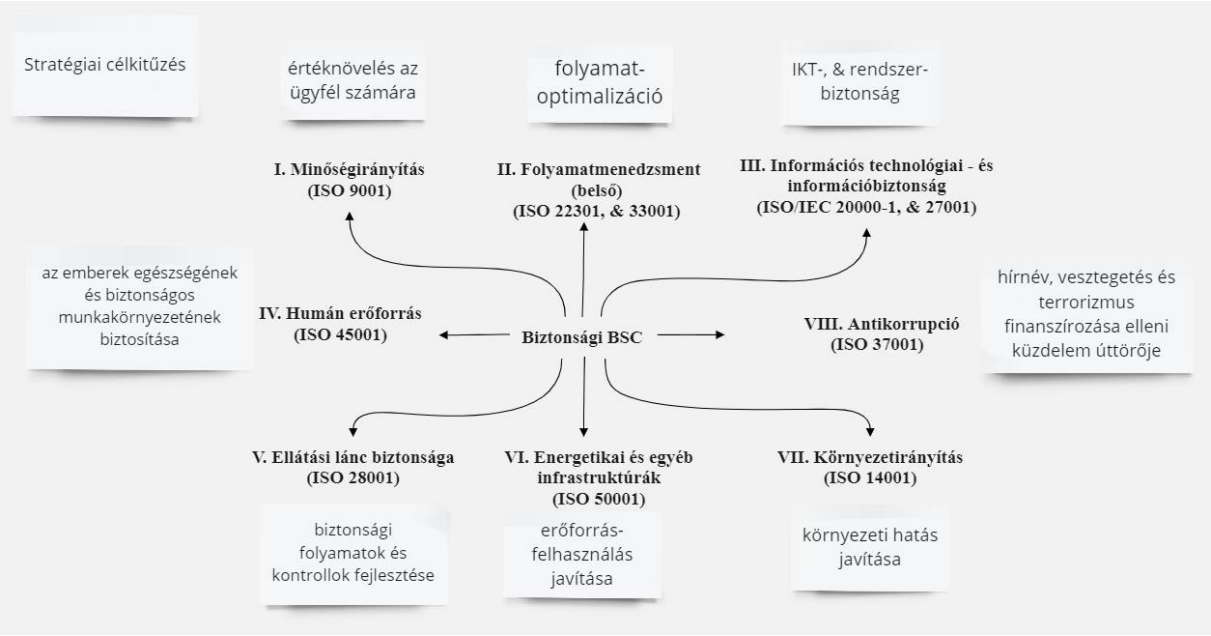
A BSC-t az egyik legbefolyásosabb stratégia-végrehajtási és ellenőrzési eszköznek tekintik, de a vállalati teljesítményre gyakorolt hatásáról vegyes adatok állnak rendelkezésre [147]. A BSC-t kritikus perspektívából lehet tekinteni, például abból a szempontból, hogy a BSC egy menedzsment eszköz, melynek alapfeltevése, hogy a szervezetek racionális, felülről lefelé irányuló folyamatban valósítják meg a stratégiát, vagy hogy az erős szervezeti kontroll elképzelésére épül [148]. A kritikák ellenére a BSC felhasználható a vállalati célkitűzések támogatására. A kulcs teljesítménymutatóknak (angolul KPI – key performanace indicator) összhangban kell lenniük a vállalat stratégiai célkitűzéseivel, és célértékekhez kell kapcsolódniuk. A KPI-k teljesítését elősegíti a folyamatok fejlesztése, egy jobb folyamat jobban hozzá tud járulni a stratégiai célkitűzések eléréséhez. A KPI-k képesek mérni a fejlesztések szintjét. Egyes KPI-kat könnyű, míg másokat nehezebb és időigényesebb összegyűjteni [149]. A teljesítménymutatók a folyamatok teljesítményét tükrözik. Az alkalmazott KPI-készlet kialakítása a megfelelő folyamatteljesítmény-mérés előfeltétele. A rögzített adatoknak pontosnak és megbízhatónak kell lenniük. A felsővezetésnek és a közvetlen feletteseknek rendszeresen figyelemmel kell kísérniük a KPI-kat, és szükség esetén meg kell határozniuk a szükséges intézkedéseket. A kiegyensúlyozott mutatószámrendszert számos különböző szervezet sikeresen alkalmazta a teljesítmény mérésére és értékelésére [146]. Számos tanulmány bizonyítja a BSC sikeres alkalmazhatóságát nagyvállalatoknál és szervezeteknél.

A BSC alkalmasnak tűnik minden típusú és méretű vállalat számára, mind a nagy, mind a kisvállalatok számára, de például az Egyesült Királyságban és Cipruson 500 vállalat kutatási adatai alapján nagyon kevés kisvállalat használja a BSC-t, különösen az Egyesült Királyságban [150]. Vannak jó példák az üzleti szektoron kívül is – például a felsőoktatás [146], vagy az egészségügyi szolgáltatások egészségügye [151; 152] – ahol a BSC bizonyítottan helytáll hatékony stratégiai menedzsment eszközként. Vannak olyan tanulmányok, amelyek a BSC-vel a biztonság kontextusában foglalkoznak, mint például a BSC adaptációja a szervezeti biztonsági kultúra mérésére [153], a munkahelyi egészségvédelem és biztonság [154], egészség-, biztonság- és környezetirányítási rendszerek [155; 156], az iskolai biztonsági teljesítmény [157], a tengeri biztonság javítása a tengeri folyamatirányítás javításával [158] stb. A BSC-t biztonsági szemszögből is kutatják például az információbiztonság [159; 160]; vagy az információbiztonsági befektetési döntések [161]. Következésképp, a BSC koncepciója alkalmas eszközként használható a folyamatteljesítmény mérésének támogatására, és a biztonsági folyamatmérési célokra való továbbfejlesztésre. Az új biztonsági BSC-modell a vállalati biztonságot holisztikusan közelíti meg, és egy modellen keresztül különféle biztonsági területeket fed le a stratégiai célkitűzésekből származtatva.

7.2. Biztonsági kiegyensúlyozott mutatószámrendszer

A biztonsági célkitűzések és célok a vállalati stratégia részhalmazai, és a változó üzleti és kockázati környezetben szerepük egyre fontosabbá válik. Az integrált kockázatkezelési megközelítés elősegíti, hogy a biztonságkezelési folyamatokat a megfelelő üzleti folyamatok szerves részeként kezeljék. A Biztonsági BSC szintúgy a stratégiai célkitűzéseken alapul.

A 10. ábrán kontrolling területekre bontva, azaz biztonsági csoportonként szemléltetem a Biztonsági BSC-hez kapcsolódó stratégiai célkitűzéseket.



10. ábra A Biztonsági Balanced scorecard pillérei a stratégiai célkitűzésekkel (Forrás: Saját szerkesztés.)

A 7. táblázat biztonsági csoportonként (I.-VIII.) tartalmazza az általános teljesítménycélokat és mérési mutatókat a megfelelő Nemzetközi Szabványügyi Szervezet irányítási rendszerekre vonatkozó szabványokkal együtt. Mindez jó gyakorlatként szolgálhat, ezért modellként ajánlott egy átfogó biztonságmenedzsment rendszer egészének vagy egy részének megvalósítása során.

7. táblázat Teljesítménycélok és mérésük biztonsági csoportok szerint (Forrás: Saját szerkesztés.)

Biztonsági csoport	Célkitűzés	Mérés - Teljesítményindikátorok
I. ISO 9001 minőségirányítási rendszer	- Folyamatok folyamatos fejlesztése (CI), beleértve a megfelelő dokumentációt - KPI-ok, pl. az vevőelégedettségi mérőszámok, vagy az elsőre jó arány (first time through rate) összhangban vannak az üzleti folyamatokkal, rendszeresen figyelik és szükség szerint intézkedés történik - Nincs lejárt intézkedés - Nincs lejárt audit/ellenőrzési intézkedés - Az alkalmazottak ismerik a Minőségpolitikát, a Minőségcélokat és a QMS kötelezettségeiket/hozzájárulásaikat - A “minőség” kultúrájának népszerűsítése	- CI-projektek (nyitott, befejezett) száma és az elért hatékonyság - A menedzsment és a felső vezetés számára a KPI-jelentés megtörtént és a szükséges intézkedések meghatározásra kerültek - Nyitott/megkésett intézkedések száma - Nyitott/megkésett audit során meghatározott intézkedések száma - Rendszeres QM tréningek vizsgatesszteléssel tréningterv szerint, tréning-jegyzőkönyvek megőrzésével; Részvételi arány - Rendszeres kommunikáció a minőségirányítással kapcsolatban, például e-mail, vagy személyes formában QMS témájú ismeretterjesztés, QMS foglalkozások
II. Folyamatmenedzsment (belső) ISO 22301, & 33001 Üzletmenet-folytonossági irányítási rendszer (BCM), & Informatika - Folyamatértékelés	- Üzletmenet folytonosságának fenntartása - Megbízható IKT szolgáltatásnyújtás a szolgáltatási szint megállapodásoknak (Service Level Agreements, SLA) megfelelően; IKT és információbiztonsági politika meghatározása, működtetése és rendszeres felülvizsgálata; a folyamat teljesítményét ellenőrzik; - Információbiztonsági folyamatok és eljárások hiányosságainak és fejlesztési területeinek azonosítása annak biztosítása érdekében, hogy az információ- és kiberbiztonsági kontrollok működjenek, és szükség szerint frissítésre kerüljenek a titkosság, a rendelkezésre állás és az integritás biztosítása érdekében. - Az alkalmazottak ismerik a BCM-mel kapcsolatos kötelezettségeiket	- BCM tesztelés szám - Hatékony BCM-tesztek száma - Elvégzett IKT felülvizsgálatok / auditok száma, Audit intézkedések száma / Audit hiányosságokhoz kapcsolódó intézkedések száma, CI-intézkedések száma és határidőben történő befejezésük, illetve határidőn túli intézkedések száma - Rendszeres képzések vizsgatesszteléssel tréningterv szerint, tréning-jegyzőkönyvek megőrzésével; Részvételi arány
III. ISO/IEC 20000-1, & 27001 Informatika - Szolgáltatások kezelése, & Információbiztonság	- A vállalat nem tapasztal problémát IKT és/vagy információbiztonsági incidens miatt, pl. az IKT szolgáltatások elérhetetlensége, adatsérülés, bizalmas adatok nyilvánosságra hozatala; - Az alkalmazottak tisztában vannak az IKT-biztonsággal kapcsolatos kötelezettségeikkel	- IKT-incidensek száma (cél: nulla) és az SLA szerint megoldott IKT-incidensek száma (megfelelőségi arány) - IKT-val kapcsolatos kérelmek és az SLA szerint végrehajtott kérelmek száma - Incidensek átlagos megoldási ideje - Feladatok elkülönítésével (segregation of duties, SoD) kapcsolatos konfliktusuk száma (cél: nulla) - IKT biztonsággal kapcsolatos képzések és a résztvevők száma; Részvételi arány

Biztonsági csoport	Célkitűzés	Mérés - Teljesítményindikátorok
IV. ISO 45001 Munkahelyi egészségvédelmi és biztonsági irányítási rendszerek	- Balesetmentes munkanapok - Munkával kapcsolatos incidensek, balesetek/sérülések/balesetközeli események elkerülése - Munkahelyi egészségügy és munkahelyi biztonság képzéseken való részvétel biztosítása	- Munkával kapcsolatos incidensek száma (cél: nulla); Munkahelyi egészségvédelmi és biztonsági problémák miatt elveszített idő - Biztonságos (azaz: balesetmentes, munkahelyi egészségvédelmi és biztonsági eseménymentes, sérülésmentes) munkanapok száma - Munkahelyi egészségügy és munkahelyi biztonság képzések száma és résztvevők száma, Részvételi arány
V. ISO 28001 Biztonsági irányítási rendszerek az ellátási lánchoz	- Az ellátási lánc biztonsági értékelése, és a hiányosságok és a fejlesztési lehetőségek meghatározása	- Szállítási idő csökkenése - Preferált szállítói vásárlások számának növelése
VI. ISO 50001 Energia irányítási rendszer; Energia és egyéb infrastruktúra	- Az energiaelnyelő folyamatok áttekintése (pl. termelési egységek vagy irodaház) és energiaoptimalizálási megoldások keresése - Energiateljesítmény mérése, energiaadatok nyomon követése és elemzése - v%-kal javítani az energiahatékonyságot	- Energiafogyasztási mutatók - Az azonosított optimalizációs megoldások száma - Az elért hatékonyság pénzbeli összegben kifejezve
VII. ISO 14001 Környezetirányítási rendszerek	- Minimalizálja a működés környezeti hatását: - Károsanyag-kibocsátás csökkentése az ellátási értékláncban x%-kal - Megújuló energiatermelés növelése y%-kal a fosszilis energiaigény csökkentése érdekében - Újrafelhasznált anyagfelhasználás növelése z%-kal - Fejlesztési területek azonosítása - Az alkalmazottak tisztában vannak a környezetgazdálkodással kapcsolatos kötelezettségeikkel	- A befejezettség százalékos aránya a célértékekhez képest (x;y;z) - CI-projektek száma (nyitott, befejezett) és az elért hatékonyság - Környezetvédelmi tréningek és résztvevők száma; Részvételi arány
VIII. ISO 37001 Antikorrupciós irányítási rendszerek	- A vesztegetés és a terrorizmus finanszírozása elleni küzdelem	- A vesztegetés és a terrorizmus finanszírozásával kapcsolatos jogsértések, incidensek száma (cél: nulla)

A 8. táblázatban a Biztonsági BSC-hoz kapcsolódó teljesítménycélokat és mérőszámokat mutatok be a biztonsági csoportokhoz rendelten a pénzügyi, vevő, belső folyamat, valamint innovációs és tanulási szempontok szerint.

Biztonsági Balanced Scorecard					
Biztonsági csoport	**Pénzügyi perspektíva**		**Biztonsági csoport**	**Vevői perspektíva**	
	cél	**mérőszám**		**cél**	**mérőszám**
I. QMS	Nyereségesség - folyamatos működés	Cash flow; Jövedelem; Költségek	I. QMS	Vevőelégedettség	Vevőelégedettségi index (ár, minőség, termékek és szolgáltatások megbízhatósága, elérhetőség-szállítási idő)
I. QMS	Pénzügyi beszámoló megbízhatósága	Megfelelő belső folyamatok; belső kontroll felülvizsgálatok; audit megállapítások (belső; külső)	I. QMS	Piaci részesedés	Kiemelt vevőmenedzsment; vevőszerzés és -megtartás
I. QMS; II. Folyamatmenedzsment; III. IKT biztonság; IV. Munkahelyi egészségvédelem és biztonság	Stabil működés	A folyamat meghibásodásával, incidenssel kapcsolatos időkieséssel eltöltött idő; visszaküldött termék/panasz; a vásárlói megrendelések időben feldolgozásra kerülnek			
III. IKT / adatokkal kapcsolatos megfelelés (bizalmasság, GDPR etc.); IV. Munkahelyi egészségvédelem és biztonság; V. Ellátási lánc; VII. Környezet; VIII. Antikorrupció	Jogszabályoknak való megfelelés	Az előírások be nem tartása miatt nincs bírság			
V. Ellátási lánc; VI. Energia	Költségszerkezet javítása, optimalizálási megoldások	Költségcsökkentés, kiadások csökkenése			
I. QMS; II. Folyamatmenedzsment; III. IKT biztonság	Project menedzsment	Büdzsé és megvalósult eredmények (teljeskörű nyomonkövetés)			
Biztonsági csoport	**Belső folyamatok/működés perspektívája**		**Biztonsági csoport**	**Innováció és tanulás perspektívája**	
	cél	**mérőszám**		**cél**	**mérőszám**
II. Folyamatmenedzsment (BCM, IT szolgáltatások)	Gyors reagálás váratlan eseményekre	BCM készenlét hatékonysága; SLA - szolgáltatás minősége	I-VIII.	IKT- és a rendszerbiztonsági szint javítása	Hiányelemzés; fejlesztési projektek/akciók; Folyamatos fejlesztési projektek (nyitott, zárt)
II. Folyamatmenedzsment (BCM, IT szolgáltatások)	Folyamatok egyszerűsítése, a lehetséges problémák minimalizálása	Biztonsági incidensek, közeli balesetek	I-VIII.	Vállalati biztonsági kultúra	Alkalmazottak biztonsági attitűd felmérése; fejlesztő tréningek (munka közben; tantermi; online)
I. QMS	Elsőre jó arány	Átdolgozás, reklamáció	I-VIII.	Alkalmazottak kompetenciái	Tréning
IV. Munkahelyi egészségvédelem és biztonság	Munkavállalók egészségének és biztonságának megőrzése	Biztonságos munkanapok	I-VIII.	Alkalmazottak elkötelezettsége	Munkavállalói elégedettségi index; Munkavállalói megtartási index
V. Ellátási lánc biztonság	Időben történő szállítás	Csökkentett átfutási idő			

8. táblázat Biztonsági Balanced Scorecard: teljesítménycélok és mérőszámok (Forrás: Saját szerkesztés.)

7.3. Következtetések

A kiegyensúlyozott mutatószámrendszer megközelítést szakirodalmi elaboráció alapján kutattam. A biztonsági csoportokhoz (6.2. fejezet) kapcsolódóan kidolgoztam az új Biztonsági Balanced Scorecard modellt. A Biztonsági BSC átveszi az eredeti BSC struktúráját, és azt vállalati biztonsági szempontokra alkalmazza.

A Biztonsági BSC keretként szolgál a folyamatbiztonság teljesítményének vállalati szintű mérésére. A Biztonsági BSC integrált megközelítésű, és modellként ajánlott egy átfogó biztonsági irányítási rendszer egészének vagy egy részének megvalósítása során. A Biztonsági BSC általános biztonsági teljesítménycélokat és intézkedéseket tartalmaz, amelyek testre szabhatók és felhasználhatók bármely vállalat számára. A modellel kapcsolatban beválás-vizsgálatot végeztem, melynek keretei között a modellt egy nagyvállalatnál ismertettem. A visszajelzés alapján a modell teljes mértékben alkalmazhatónak nevezhető. A visszajelzés megerősíti a teljesítménymérés szerepét, a vállalati célok elérését segítő megfelelő mérőszámok meghatározásának jelentőségét, illetőleg a működtetés kapcsán kulcs tényezőnek nevezi a kommunikációt, a munkatársak támogató hozzáállását a rendszerhez.

8. ÖSSZEGZETT KÖVETKEZTETÉSEK

A fejezetben az értekezéshez kapcsolódó záró gondolataimat fogalmazom meg (8.1. fejezet), ezt követően a kutatási eredményeim hasznosítási lehetőségeit (8.2. fejezet), majd az értekezésem elején megfogalmazott hipotéziseim értékelését (8.3. fejezet), és a kutatómunkám új tudományos eredményeit, a felállított téziseimet (8.4. fejezet) mutatom be.

8.1. Záró gondolatok

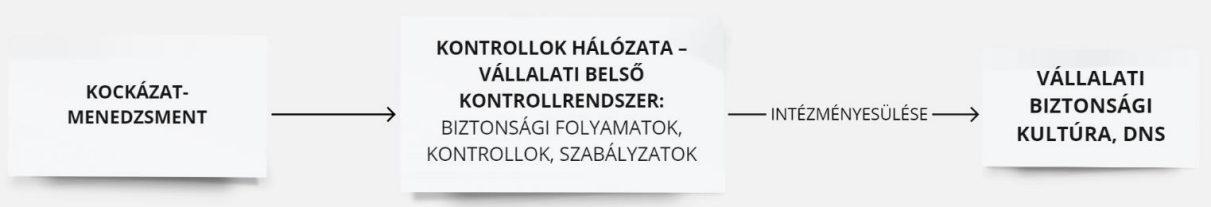
Az értekezésben a vállalatbiztonság kérdéskörének vizsgálatára került sor. A digitális kor kihívásaira adekvát válaszok szükségesek, melyhez szorosan kapcsolódik az információbiztonság területe. A reziliencia, az adaptív ellenálló képesség érdekében megfelelő biztonsági folyamatok szükségesek. A vállalati biztonság hálózatszerű összefüggései meghatározóak. A belső kontrollrendszer hálózatként leírható. A vállalati biztonsági hálónak meg kell felelnie a mai kor követelményeinek. A belső kontrollrendszerre, a kockázatkezelésre, a szabványos irányítási rendszerekre és a kiegyensúlyozott mutatószámrendszerre együttesen igaz, hogy közös a csomópontjuk, a vállalati stratégia. A vállalatbiztonsági kérdéseknek együtt kell járniuk a stratégiai kezdeményezésekkel. A vállalati biztonság összekapcsolódik a vállalati stratégiai célkitűzésekkel és pragmatikusan az üzleti folyamatok részeként valósul meg.

A biztonsági szempontok érvényesülését a *vezetői elkötelezettség* tudja előmozdítani. A vállalati *biztonság háló* erőssége, eredményes és sikeres működése szempontjából a vezetői elkötelezettség a fő húzóerő. A pozitív vezetői hozzáállás a biztonsági szempontok vonatkozásában maga után vonja az alkalmazottak pozitív hozzáállását, mely nemcsak a belső, hanem a külső érintettek, ideértve ügyfelek számára is értéket tud generálni. A vállalatok a többi piaci szereplővel való együttműködés révén tudnak működni, fennmaradni, és növekedni, ezek a kapcsolatok határozzák meg működési környezetüket, és alkotják a vállalat külső kapcsolati hálóját. Ez a kapcsolati háló kihat a belső folyamatokra is: megfogalmazott ügyféligények formájában, termékeket/ szolgáltatást illetően, melynek részét képezik a biztonságos működésre, és folyamatokra való igény is. A nyereségorientált vállalatok piacon maradásának feltétele a vevő*igény* kielégítése. A biztonsági folyamatok, kontrollok mögöttes célja a vevői elégedettség biztosítása, a vállalati célkitűzések megvalósítása, melyhez jellegéből adódóan jellemzően indirekt módon járulnak hozzá, ugyanakkor direkt kapcsolódási pontok is azonosíthatók. Már a szerződéses kapcsolat kezdetekor követelmény, hogy a megfelelő védelmi szint biztosított a kapcsolat során, például a GDPR adatvédelmi megfelelőség, információbiztonság vagy a biztonsági szempontok érvényesülése a megvásárolt termék / szolgáltatás használata során.

Az erős biztonsági kultúra az ügyfélkapcsolatok kialakítása, és fenntartása során értéket jelent, mely eladhatóvá teszi a termékeket / szolgáltatásokat.

A *vállalat kontrollrendszerét meghatározó kontrollok*nak a vállalati működés minden szintjén jelen kell lenniük, például IT, HR, Jog, pénzügy. A vállalati biztonsági háló, illetve vele együtt a kívánt biztonsági szint a kockázatkezelési tevékenység eredménye.

A *vállalat kontrollhálózata, a biztonsági háló* kontrollokból épül fel. A biztonsági folyamatok és kontrollok az *üzleti folyamatok részét* képezve tudnak eredményesen és hatékonyan működni, ezért az üzleti folyamatok részeként a biztonsági aspektusra is gondolni kell. A biztonsági kultúra intézményesítése szempontjából elsődleges a vezetőség elkötelezettsége, melyhez a szolid kockázatmenedzsment tevékenység eredményeként definiált belső kontrollrendszernek kell társulnia (11. ábra). A biztonsági szabályzatokat nemcsak lefektetni kell, hanem élni is kell azt a rendszert, és egy idő után a biztonságtudatosság a vállalati biztonsági kultúra intézményesülése révén a mindennapok részévé válik, melyet a „vállalati DNS", a vállalati kultúra, és értékrend hordozni fog.



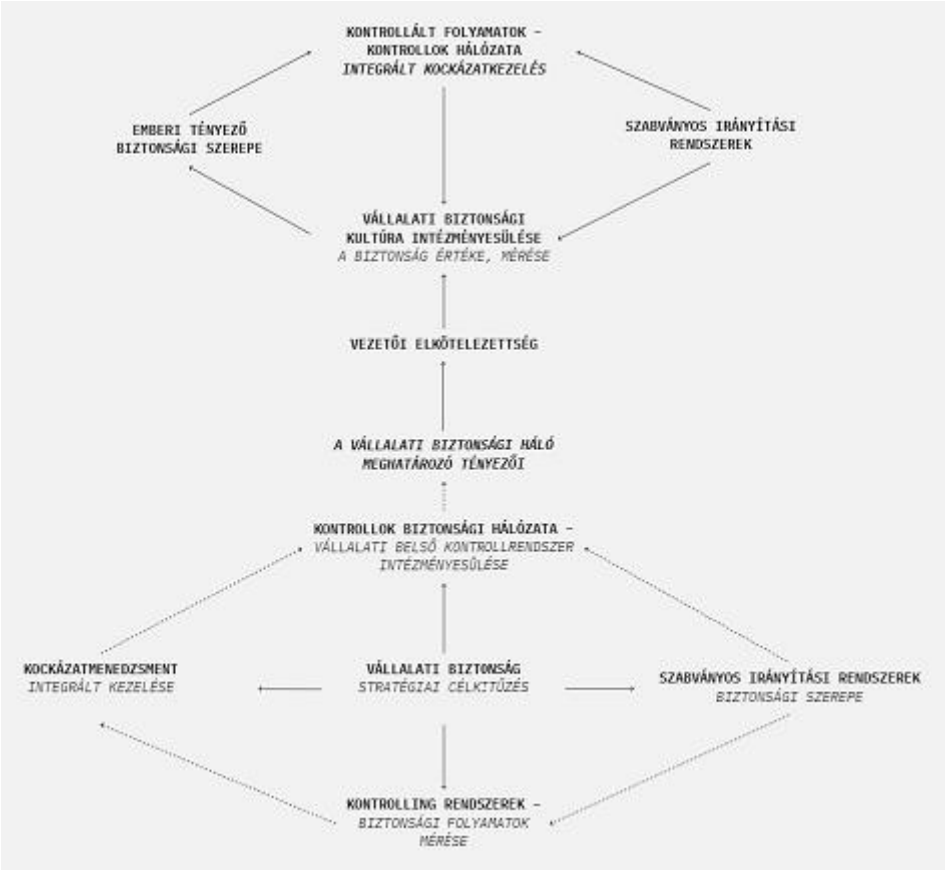
11. ábra A kontrollhálózat intézményesülése (Forrás: Saját szerkesztés.)

A *vállalatbiztonság* intézményesítése szempontjából az *információbiztonság* szerepe a digitális kor kontextusában meghatározóvá vált. Az információbiztonság kérdését információbiztonsági irányítási rendszer mentén kialakítva a kritikus szerepű információvédelmi elvek megvalósítása mellett a vállalati biztonsági kultúra intézményesítése is megvalósul. Az információ különféle formáiban a vállalati folyamatok szerves részét képezi, ebből eredően az információbiztonsági irányítási rendszer a vállalati folyamatok részeként valósul meg. A szabvány szerinti irányítási rendszer segíti a biztonsági követelményeknek való megfelelést, és intézményesülése révén hozzá tud járulni *a reziliens fellépés*hez biztonsági fenyegetések esetén. Az irányítási rendszerszabvány szerint kialakított *információbiztonsági irányítási rendszer* – annak tanúsításától függetlenül – értéket jelent, a megfogalmazott elvárások lefektetik egy olyan rendszer alapjait, mely hosszú távon képes a vállalati biztonsági célkitűzések támogatására, és pozitív módon hatnak a vállalati működésre a jelentőségteljes biztonsági kultúra intézményesítése révén.

Egy jól működő információbiztonsági irányítási rendszer alkalmas a folyamatbiztonság növelésére, mely egyúttal a felölelő vállalatbiztonságot és biztonsági kultúrát is erősíti. Az irányítási rendszerek független tanúsító testület általi tanúsítása a folyamatbiztonság szempontjából további komfortot jelent. A tanúsított irányítási rendszerek bizonyosságot jelentenek a folyamatbiztonság vonatkozásában. A tanúsítás többek között erősítheti az üzleti bizalmat is, mely a vállalati profittermelő képesség szempontjából kritikus. Mindez egy válaszkész, agilis rendszer működését tudja szolgálni, mely a digitális korban elvárássá nőtt *reziliencia* képességének letéteményese.

Az irányítási rendszerszabványok céljai biztonságorientáltak. A szabványos irányítási rendszerek alapján a vállalati biztonságot meghatározó biztonsági csoportok határozhatóak meg, többek között a fundamentális minőségirányításra, a folyamatmenedzsmentre, az információbiztonságra, a humán erőforrás biztonságára, az ellátási lánc biztonságára, az energetikai és egyéb infrastruktúrákra, a környezetirányításra, és a megvesztegetés, korrupció elleni védelemre kiterjedően.

A folyamatok teljesítményének mérése a vállalati célkitűzések megvalósítását támogatja. A biztonsági folyamatok teljesítményének mérése egyaránt szükséges. A teljesítménymérés kapcsán a kiegyensúlyozott mutatószámrendszer alkalmazása megalapozott eszköznek tekinthető. A kiegyensúlyozott mutatószámrendszer és a szabványos irányítási rendszerek alapján definiált biztonsági csoportok integrálása révén egy új modellt állítottam fel, mely a biztonsági folyamatok teljesítménymérésére alkalmas. A biztonsági folyamatok teljesítményének mérése eszköz arra, hogy a döntéshozók és az érintettek számára a biztonsági folyamatok hozzáadott értéke meg tudjon mutatkozni.



12. ábra Az értekezés áttekintése

A vállalati kontrollhálózat eredményeként „értéket” (value) realizálhatunk. A vállalatbiztonság elérésében a definiált és működtetett kontrollok hálózata több aspektusból is értéket jelent, int. al.: az eredm**é**nyesség szintjén, a tervezett eredmények megvalósulnak, az érintettek elégedettek. A **r**eziliencia, azaz az adaptív ellenálló képesség, a változó környezethez való alkalmazkodás, a megbirkózás, megküzdés képességében, amely a mai üzleti és gazdasági környezetben kiemelkedően fontos. A **t**ranszparencia révén, a folyamatok átlátható működésében, mely a belső vállalati folyamatok integritása miatt kiemelkedő jelentőségű, támogatja a döntéshozatali folyamatokat, a pénzügyi kimutatások hitelességét, és csökkenthetők általa az audittal kapcsolatos vállalati „terhek” a gyorsabban lezajló külső audit folyamat révén. A hat**é**konyság révén a vállalat az erőforrásait gazdaságosan használja fel. A **k**valitás, azaz minőség egy következő szinergiahatás, mely a jól tervezett és működtetett folyamatok esetében megjelenhet, hozzájárulva a vevői elégedettség magas szintjéhez és versenypiaci előnyökhöz.

8.2. 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.

8.3. Hipotézisek értékelése

A kutatási célkitűzések érdekében négy hipotézist fogalmaztam meg. A hipotézisek igazolása érdekében a szakirodalmi áttekintést követően a kutatási eredményeimet a disszertációban a 4. – 7. főfejezetekben mutattam be. A fejezetek logikai sorrendje a hipotézisek sorrendjét követi elsődlegesen. A részkutatási eredmények adott részkutatásonként egy helyen kerültek bemutatásra, azonban azok egyes esetben több hipotézis alátámasztását is szolgálták.

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.

8.4. Új tudományos eredmények

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]

IRODALOMJEGYZÉK

Hivatkozott irodalom

[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.

ISO szabványok

[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

Saját publikációk

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*, *2021*(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 Journal megjelenés alatt*

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, EMPAS Journal*, *16*(1), 114-133. https://doi.org/10.2478/emj-2024-0009

RÖVIDÍTÉSJEGYZÉK

AML	Anti-money laundering, pénzmosás elleni küzdelem
BCM	Business Continuity Management, üzletmenet-folytonosság
BSC	Balanced Scorecard, kiegyensúlyozott mutatószámrendszer
CDPSE	Certified Data Privacy Solutions Engineer
CI	Continuous improvement, folyamatos fejlesztés
CIA	Confidentiality, integrity, availability
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CSO	Chief Security Officer
COSO	Committee of Sponsoring Organizations'
COBIT	Control Objectives for Information and Related Technologies
DMBoK	Data Management Body of Knowledge
DevOps	Development (fejlesztés) és Operations (üzemeltetés)
ERM	Enterprise Risk Management, Vállalati Kockázatkezelés
GDPR	General Data Protection Regulation
GT	Grounded theory, megalapozott elmélet
IBIR	Információbiztonsági irányítási rendszer
ICFR	Internal Control over Financial Reporting
IKT	Információs és kommunikációs technológia
ISACA	Information Systems Audit and Control Association
IIA	The Institute of Internal Auditors
ISO	International Organization for Standardization, Nemzetközi Szabványügyi Szervezet
KPI	Key performance indicator
PDCA	Plan-Do-Check-Act, tervezés-végrehajtás-ellenőrzés, és beavatkozás ciklus
PMBoK	Project Management Body of Knowledge

ÁBRAJEGYZÉK

TÁBLÁZATJEGYZÉK

MELLÉKLET

1. SZ. MELLÉKLET: A SZAKÉRTŐI KUTATÁSHOZ KAPCSOLÓDÓ KÉRDÉSEK

1. Ön szerint hogyan illeszkedik a proficentrikus üzleti világba a vállalatbiztonság kérdése?
2. Ön szerint hogyan lehet a biztonsági kérdéseket gazdálkodói szemszögből hatékonyan kezelni?
3. Ön szerint melyek a digitális átalakulási projektek sikertényezői? Hogyan lehet ezeknek a projekteknek a kockázatait csökkenteni és kezelni?
4. Ön szerint mi szükséges az üzleti folyamatok biztonságos működéséhez a) rendszerhez, technológiához, és b) emberi erőforráshoz köthetően a digitális korban?
5. Ön szerint melyek a leggyakoribb biztonsági hiányosságok a vállalati folyamatokban a digitális átalakulással összefüggésben? Mi az Ön javaslata azok kezelésére?
6. Ön szerint milyen következményei vannak, ha egy digitális átalakulás projekthez kapcsolódóan szükséges biztonsági kontrollok hiányoznak vagy nem hatásosak? Ön szerint hogyan biztosítható, hogy a biztonsági kontrollok tervezése eredményesen megtörténjen?
7. Mit javasolna Ön a vállalatoknak, hogy a modern digitális kor kompetencia- és készségkövetelményeinek képesek legyenek megfelelni?
8. Ön szerint hogyan lehet egy jelentőségteljes vállalati biztonsági kultúrát kialakítani, mely képes a vállalati biztonsági célok eredményes támogatására?
9. Ön szerint mik a feltételei annak, hogy a biztonsági kérdések az üzleti folyamatok elválaszthatatlan részét képezzék?
10. Ön szerint mi jellemzi azokat a vállalatokat, melyek képesek rugalmasan ellenállni a folyamatosan változó biztonsági fenyegetéseknek (reziliencia képessége)?

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném megköszönni témavezetőmnek, Prof. Dr. Michelberger Pálnak, hogy tanulmányaim során végig támogatott. Szeretnék köszönetet mondani a Doktori Iskola oktatóinak, és munkatársainak. Dr. habil. Velencei Jolán tanulmányaimat végigkísérő iránymutatásaiért különösképp hálás vagyok. Külön köszönettel tartozom a primer kutatásomban részt vevő interjúalanyaimnak. Utoljára, de nem utolsó sorban köszönöm szeretett Családomnak, hogy végig mellettem álltak és segítettek abban, hogy a kutatásomra tudjak összpontosítani.