ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

**DOKTORI (PHD) ÉRTEKEZÉS**

**DOMBORA SÁNDOR**

# Eredményes információbiztonsági rendszerek kialakítása és bevezetése

Témavezető: Prof. Dr. Michelberger Pál PhD

**BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA**

Budapest, 2022.01.27.

## Szigorlati Bizottság:

Elnök:

Prof. Em. Dr. Berek Lajos professor emeritus, ÓE

Tagok:

Dr. habil. Kerti András, egyetemi docens, külső – NKE

Prof. Dr. Rajnai Zoltán, egyetemi tanár, ÓE

## Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Rajnai Zoltán, egyetemi tanár, ÓE

Titkár:

Dr. Pető Richárd adjunktus, ÓE

Tagok:

Dr. Krasznay Csaba egyetemi docens; külső – NKE

Dr. habil. Tick Andrea egyetemi docens; ÓE

Dr. habil. Velencei Jolán egyetemi docens

Bírálók:

Dr. habil. Szádeczky Tamás egyetemi docens ÓE

Dr. Honfi Vid Sebestyén főiskolai tanár; külső – MFE

## Nyilvános védés időpontja

2022.06.30.

**NYILATKOZAT**
**A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL**

Alulírott Dombora Sándor kijelentem, hogy az

Eredményes információbiztonsági rendszerek kialakítása és bevezetése

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, 2022.01.27.....

..... (aláírás)

# TARTALOMJEGYZÉK

# BEVEZETÉS

Az információs társadalom kialakulása során bekövetkezett digitalizációs robbanás következtében nemcsak a gazdaság különböző szektoraiban, hanem az élet minden területén fontossá vált az információ azonnali hozzáférhetősége. A digitalizáció kezdetén a munkafolyamatok támogatására szakterületenként készültek szigetszerű megoldások. Ezeket később felváltották a hálózatba kötött informatikai rendszerek, amelyek integrált vállalatirányítási rendszerekké fejlődtek. Ezzel párhuzamosan robbanásszerűen terjedt el az Internet, behálózva a világot, lehetővé téve a digitális kommunikáció és vele együtt a szociális média elterjedését és mindennapi használatát. Gondoljunk itt arra, hogy szinte mindenki zsebében ott lapul az okostelefon, amely segítségével üzenhetünk, de akár videóhívás formájában is beszélhetünk egymással. Ezzel együtt megnőtt az szervezetek informatikától és infokommunikációs rendszerektől (a továbbiakban röviden IT) való függősége. Egyre fontosabbá vált az informatikai rendszerek rendelkezésre állása, a szolgáltatott adatok megbízhatósága és bizalmasságának megvédése. Ez elkerülhetetlenné teszi, hogy a szervezetek egyre nagyobb hangsúlyt fektessenek a 21. században az információ és informatikai biztonságra. Ahogy az informatikai rendszerek egyre fejlettebb és integráltabb megoldásokká álltak össze, behálózva a világot, a cégek egyre nagyobb biztonságfokú, moduláris és integrált információbiztonsági rendszerek létrehozására törekednek. Az információbiztonság kialakítása és fenntartása a technológia fejlődésével egyre bonyolultabbá vált, folyamatosan frissülő szabványok és keretrendszerek jelentek meg amelyek bevezetése elősegíti a szervezet számára szükséges információ és informatikai biztonsági szint elérését. Ezek közül a legfontosabbak: a folyamatosan bővülő több mint 40 szabványból álló ISO/IEC 27000 szabványcsalád, ISO 31000, ITIL (IT Infrastructure Library) és COBIT (Control Objectives for IT and Related Technology). A tématerület fontosságát jelzi, hogy egyre több jogszabály jelenik meg amelyek kiterjednek a személyes adatok védelmére és az állami és önkormányzati szervek információbiztonságára is. Ilyen többek között: a 2013 évi L. törvény (továbbiakban Ibtv) és végrehajtási rendeletei, Az Európai Parlament és Tanács (EU) 2016/679 rendelete (továbbiakban GDPR) a személyes adatok védelméről. Emellett folyamatosan frissítik a gazdasági szektorokra vonatkozó információbiztonságot is előíró jogszabályokat. Ahhoz, hogy a szervezetek által felépített információbiztonsági rendszer eredményesen, hatékonyan és megfelelően működjön illeszkednie kell a vállalat működéséhez, informatikai rendszereinek és infrastruktúrájának kialakításához, de önmagában a rendszerben kialakított és működő megoldások egymáshoz való harmonizációja is szükséges.

## A tudományos probléma megfogalmazása

A szabványok követelményrendszert állítanak, azaz a „MINEK kell megfelelni?” kérdésre adnak választ. Az információbiztonságra való törekvés térhódítása és az egyre szigorúbb jogszabályi környezet, a követelmények megfogalmazásán túl szükségessé teszi a követelmények gyors bevezetésének lehetőségét. Ez felveti az átlátható, moduláris, rugalmas és könnyen módosítható információbiztonság irányítási megoldások kialakításának kérdését, azaz a „HOGYAN feleljünk meg?” kérdés megválaszolását. A szabványokat bevezető szervezetek az esetek többségében rendelkeznek információvédelmi szabályzatokkal és intézkedésekkel. Ezek már a bevezetés pillanatában is lefedik valamilyen mértékben a szervezet információbiztonsággal kapcsolatos igényeit, a helyi és globális jogszabályi környezet előírásait, de sok esetben csak adott cél megvalósítását szolgálják, nem teljes körűek és nem teljesítik az egyenszilárdság elvét. Az is előfordulhat, hogy a szabályzatok jogszabályoknak és a szabványoknak való megfelelése teljesül, de a szabályzatok által előírt védelmi követelmények nem valósulnak meg a gyakorlatban. Az így kiépített rendszerek nem biztosítják az információ biztonságát a szervezet számára.

Fontos megemlíteni, hogy a nagy tanácsadó cégek és nemzetközi szervezetek is végeznek információbiztonsággal kapcsolatos felméréseket. Ezek a felmérések jellemzően a szervezetek Információbiztonság Irányítási Rendszerével (továbbiakban IBIR), szabályzataival és szervezeti struktúrájával kapcsolatban fogalmaznak meg kérdéseket. Jó példa erre az ISACA Budapest Chapter 2011 óta rendszeresen készített „Információbiztonsági helyzetkép” [1] [2] [3] [4] [5] címet viselő felmérése, amely a szabványok szabályozási, szervezeti és általános követelményeire kérdez rá, de nem vizsgálja az információbiztonság megvalósulását, a bevezetett IBIR szerkezetét, hatékonyságát és eredményességét ezáltal egy részeredményt tálal, ami hamis biztonságérzetet kelthet – azaz a szervezet jobbnak ítélheti meg az információbiztonságát mint ami megvalósul a gyakorlatban. Ahhoz, hogy valós képet kapjunk az információbiztonság állapotáról nem elég csak az egyes intézkedések létezését vizsgálni, hanem érdemes rákérdezni azok működőképességére is, habár az utóbbi kérdésekre nem valószínű, hogy valós válaszokat kapunk a megkérdezettektől. Ilyen az információbiztonság megvalósulására irányuló főbb kérdések:

- Mi akadályozza a szervezetekben az információbiztonsági szabályzatok betarthatóságát?
- Szervezetükben milyen mértékben segítik vagy hátráltatják a munkavégzést az információbiztonsági szabályzatok?
- Milyen változások szükségesek ahhoz, hogy a dolgozók ne kerüljék meg az információbiztonsági szabályzatokat a munka felgyorsítása érdekében?

Az információbiztonság megvalósításához olyan irányítási rendszert – szabályzatokat és eljárásrendeket - kell kialakítani, figyelembe véve a szervezet infrastruktúráját és gazdasági lehetőségeit, amelyek megfelelő szinten biztosítják a szervezet által kezelt információ elvárt és jogszabályi környezetnek megfelelő védelmét. Az így kialakított irányítási rendszer követelményei megvalósíthatók kell legyenek a gyakorlatban, olyan biztonsági intézkedések formájában, amelyek biztosítják a munkafolyamatok zavartalan működését az elvárt biztonsági szint mellett. Központi irányítás alá tartozó szervezetekben megvalósítandó információbiztonság esetében további kérdéseket vet fel, az egyes szervezetek szabályozási, méretbeli és technológiai heterogenitása.

## A témaválasztás indoklása

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

## Célkitűzés(ek)

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

1. meghatározzam az információbiztonsági rendszerek problémáit és feltárjam azok forrását;
2. kidolgozzak egy olyan IBIR modellt, amelynek bevezetése biztosítja a szervezetek jogszabályi és szabvány követelményeknek megfelelő információbiztonságát;
3. meghatározzam az IBIR követelményeinek olyan minimális mennyiségű szabályzatra és eljárásrendre bontásának módját, amely biztosítja a szervezet struktúrájához való illeszkedést;
4. meghatározzam azt a bevezetési módot, amelynek alkalmazásával az általam kidolgozott IBIR modell megvalósítása elősegíti a munkafolyamatok zavartalan végrehajtását, a tervezett biztonsági szint elérése mellett;
5. kidolgozzak egy integrált incidenskezelési munkafolyamatot, amely hatékonyan kezeli az IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági események kezelését.

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

## A téma kutatásának hipotézisei

Előfordul, hogy az IBIR szabályzatai és eljárásrendjei megfelelnek a jogszabályi és szabvány követelményeknek, de megvalósításuk nem biztosítja megfelelően a szervezet által kezelt információ biztonságát. Kutatásomban meghatározom azokat a tényezőket, amelyek befolyásolják az IBIR által megvalósított információbiztonság eredményességét.

H1. A szervezetek információbiztonsági állapotát befolyásoló tényezők függetlenek a szervezet tevékenységétől és méretétől.

A szervezetek információbiztonságának megvalósítását sok esetben több jogszabály és szabvány is befolyásolja. A szervezetek üzleti szolgáltatásait IT szolgáltatások támogatják, amelyek megvalósításához az ITIL alapú IT szolgáltatásmenedzsment bevezetése nyújt segítséget. Az információbiztonság eredményes megvalósításához olyan integrált IBIR modell megvalósítására van szükség, amely kiküszöböli annak állapotát befolyásoló tényezők negatív hatásait.

H2. Az ITIL munkafolyamatainak, a jogszabályok és szabványok követelményeinek integrálásával építhető olyan IBIR modell, amely a feltárt problémák kiküszöbölésével biztosítja a szervezetek számára a szükséges szintű információbiztonságot.

Előfordulnak esetek, amikor az IBIR bevezetését akadályozzák a szabályzatokban és eljárásrendekben szereplő a szervezetben felismerhetetlen szerepkörök. A követelmények

megfelelő csoportosításával, szabályzatokra bontásával azonosíthatóvá válnak az IBIR bevezetéséhez szükséges szervezeti egységek és szerepkörök.

H3. Csoportosíthatók úgy az IBIR követelmények, hogy a csoportok mentén létrehozott szabályzatok és eljárásrendek illeszkedjenek a szervezet struktúrájához megkönnyítve ezzel az IBIR bevezetését.

A szervezetek munkafolyamatainak végrehajtását gyakran ellehetetlenítik az IBIR követelményei. Ahhoz, hogy a munkafolyamatok végrehajthatók legyenek az érintetteknek meg kell szegniük az IBIR előírásait. Az IBIR munkafolyamatokra kiterjedő elemzésével létrehozható olyan bevezetési mód, amely integrálja az IBIR követelményeit a munkafolyamatokba és ezáltal kiküszöböli az ellentmondásokat.

H4. Létezik olyan IBIR bevezetési mód, amelynek alkalmazásával megvalósítható a munkafolyamatok zavartalan végrehajtása a szükséges biztonsági szint elérése mellett.

A IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági incidenskezelési munkafolyamatok silószerű végrehajtása során információbiztonságra való hivatkozás akadályozza az incidensek gyors kivizsgálását és elhárítását. Az incidensek kivizsgálásának és elhárításának akadálymentesítéséhez és felgyorsításához elengedhetetlen az incidenskezelési munkafolyamatok közötti gyors információáramlás megvalósítása.

H5. Definiálható olyan integrált incidenskezelési munkafolyamat modell, amely összehangoltan irányítja az IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági eseményeket.

## Kutatási módszertanok kiválasztása

Az információbiztonság szervezetekben való működőképességének kutatása több szakterületre bontható. A szakterületek követelményeinek összehangolása meghatározza a kialakított rendszer hatékonyságát és hatásosságát. Az alkalmazott védelmi intézkedések által nyújtott biztonsági szint nyilvánosságra hozatala hatással lehet a szervezetek megítélésére, így a szervezetek igyekeznek bizonyítani a külvilág felé, hogy profi módon védik az általuk kezelt információt. Az információbiztonságra vonatkozó kérdőíves adatgyűjtések és elemzések sok esetben torzulnak, mivel a szervezetek nem minden kérdésre válaszolnak, illetve adnak valós válaszokat. Ennek oka részben arra vezethető vissza, hogy sok esetben a szervezetek statisztikai alapon is beazonosíthatók az adatok anonimizálását követően is. Ennek következtében kizárom a nagy mintán elvégzett statisztikai módszerek alkalmazását.

Ahhoz, hogy közelebbről megismerhessem az információbiztonság megvalósításának eredményességét, csak olyan módszertan kiválasztása jöhetett szóba, amely részletes információt szolgáltat az egyes szervezetekben kialakított megoldásokról és azok hatékonyságáról. Az elvégzendő vizsgálatok részletessége miatt nincs lehetőség nagy elemszámú minták statisztikai elemzésére. Ez a megállapítás a kvalitatív módszertanok irányába terelte figyelmemet, mivel a kvalitatív kutatási módszertanok célja a probléma okainak és miértjeinek megértése, eredménye pedig a kiinduló probléma megértése. A kvalitatív kutatási módszertanok jellegzetessége, hogy feltáró jellegük miatt mélyebb elemzést és árnyaltabb ismeretek megszerzését, sajátosságok megértését teszik lehetővé. A kvalitatív kutatások elvégzése, jellemzően nem szolgáltat statisztikailag alátámasztható, számszerűsíthető eredményt, mert részletezettsége miatt csak kisebb elemszámú mintán végezhető el.

Mint a projektek aktív résztvevője adta magát, az akciókutatás módszertana, amelynek célja nemcsak elmélet létrehozása, hanem annak alkalmazása is a gyakorlatban. Coghlan és Barnnick szerint azokban az esetekben alkalmazható sikeresen, amikor a kutatási kérdések egy adott célcsoportban, közösségben vagy szervezetben egy sor időben kibontakozó esemény leírásához kapcsolódnak, a kutató a csoport tagjaként a megérti, hogy a csoport viselkedése miért és hogyan változik vagy hogyan fejlődik bizonyos szempontból egy rendszer [6]. Paul és David Coghlan szerint az akciókutatás keretében a létrehozott tudás típusa egy adott helyzetbeli gyakorlat, ellenőrzése pedig kontextusba ágyazott kísérlet, a kutató pedig részese a létrehozott változásoknak. Az eredmény az elméleten túl a gyakorlatban alkalmazott tudás, minőségi eredményeket pedig akkor lehet elérni, ha a kutatónak globális rálátása van a kutatott problémákra, amelynek a kutatási ciklusok megtervezésében is szerepe van [7]. Jól illeszkedik a kutatási területemhez az akciókutatás az a Lewin által megfogalmazott célja, hogy együttműködéssel pozitívan járuljon hozzá, mind az emberek valós gondjaihoz egy azonnali problémás szituációban, mind a társadalomtudomány céljaihoz egy mindkét fél által kölcsönösen elfogadható etikai keretben [8]. Reason és Breadbury szerint az akciókutatás egy keretet biztosít sokféle lehetősséggel a kutatóknak, amelyek között megtalálhatják a számukra megfelelőt kutatásaik elvégzéséhez [9].

Mivel kutatásaim az információbiztonsági szakértői munkámra épülnek, végrehajtásuk során esettanulmányokat kellett készíteni, amelyek elvégzett feladatok tapasztalatait írják le és foglalják össze az adott ügyfél számára. Az esettanulmány fogalmát, mint kutatási módszertant több szerző is megfogalmazta, de a legtöbb szakirodalom amikor az esettanulmány fogalmát megfogalmazza Yin R. K. definícióját idézi, Yin szerint az esettanulmány leírás egy egyedülálló, érdekes vagy

különleges dologról. Az esettanulmány szólhat személyről, szervezetről, folyamatról, tervről, térségről, intézményről vagy eseményről [10]. Mitev szerint a kutatónak jó nyomozónak kell lennie, aki képes a különböző helyeken és formákban fellelhető információ gyűjtésére és előállítására, majd a tudás és megértés alapján a megfelelő elemek összeillesztésére [11]. Az esettanulmányok elkészítésekor találkozhatunk általános esettel, amelynek kutatott tulajdonságai a kutató szerint sok esetre érvényesek, és extrém esettel, amikor a kutatott tulajdonságok alapján az eset egyedinek, kivételesnek mondható. Eisenhardt szerint az esettanulmányok alkalmasak szervezeti és menedzsment tanulmányok elkészítéséhez [12].

Ugyan Zainal megkérdőjelezi az esettanulmány, mint kutatási módszertan megbízhatóságát a nehéz átláthatósága és egyedisége miatt [13], de az esettanulmányról mint kutatási módszerről végzett irodalomkutatásaim alátámasztatottak, hogy az esettanulmányok készítése, köztes eredményként szolgál a kutatási céljaim eléréséhez, az egyediséget és az átláthatóságot pedig a projekteken átívelő struktúra egységesítésével, bevezető magyarázattal tudom ellensúlyozni.

A kutatásaim céljai között szerepel egy IBIR modell és bevezetési irányelvek kidolgozása, amelyek eredményes információbiztonsági rendszer bevezetéshez vezetnek. Ehhez szükségem van egy elméletalkotási módszertanra. A kvalitatív kutatási módszertanok irodalmát áttekintve találkoztam a Glaser és Strauss [14] által megalkotott megalapozott elmélettel (grounded theory), amelynek célja, hogy empirikus kutatómunka segítségével elméletet hozzon létre. Ez az elmélet a kutatás során gyűjtött adatokból fejlődik ki, ráilleszthető az adott kutatási környezetre. A módszertan alkalmazása folyamatos iteratív munkát jelent, amely adatgyűjtés, kódolás, elemzés és elméletalkotás lépésekből áll, ahol a lépések nem feltétlenül követik sorban egymást, hanem tetszőleges sorrendben egymással párhuzamosan is történhetnek. A kutató részese a folyamat minden lépésének. Az elméletalkotás fontos eleme az elméletet alkotó fogalmak meghatározása és a magasabb szintet képviselő kategóriák azonosítása. Kucsera szerint a kutatás addig zajlik, amíg a kategóriák megtelítődnek, ami alatt azt érti, hogy a tulajdonságai nem bővíthetők további adatgyűjtéssel [15]. A módszertan kulcseleme a folyamatos összehasonlítás, amelyben adatot adattal, fogalmat fogalommal kell összehasonlítani. Az elméletalkotás során szubsztantív és formális elmélet jön létre. A szubsztantív elmélet a kutatás kontextusában érvényes, amely tovább fejleszthető formális elméletté [15]. A módszertan megalapítói között a későbbiek során vita alakult ki a kutatási módszer alkalmazásában. Strauss szerint a kutatás előre megtervezett, induktív és deduktív logika kombinációját alkalmazza, a kódolásnál a szakirodalomban már létező kategóriák is használhatók és az ellenőrzés lényeges szempont. Glaser szerint a kutatás menet közben alakul, kizárólag az adatok elemzése során kialakuló kategóriák és induktív logika használható, az

ellenőrzésnek nincs relevanciája. A kutatók sok esetben nem pontosan követik a módszertanokat, pedig az elméletek megalapozása szempontjából fontos, főleg a kódolás és a kutatás menetének leírása [11].

A megalapozott elmélet szakirodalmának áttekintését követően körvonalazódott, hogy az információbiztonság speciális esetére, ahol fontos az adatok bizalmassága, az adatgyűjtés nem mindig tervezhető előre és sok esetben az adatok összegyűjtésének lehetőségei is korlátozottak mivel a szervezetek védik az információbiztonságra vonatkozó dokumentumaikat, adataikat, tanulmányaikat, így a Glaser féle kutatási vonal az, amely alkalmazható az én esetemben.

A megalapozott elmélet és az esettanulmány jól kiegészíti egymást. A bemenetet az interjúk és esettanulmányok képezik, az elméletalkotásba pedig beépítem Dörfler és Velencei tudásrendezés [16] valamint a szerzők Baracskaival közösen bemutatott fogalom feltérképezési technikáit [17], amely a fogalmak csoportosításának folyamatát mutatják be elősegítve ezzel az elmélet kikristályosítását.

A kutatás során végzett interjúk és adatgyűjtések a szakterület bizalmasságára vonatkozó sajátosságaira való tekintettel titkosak, emiatt nem közölhetők, csak a menet közben elvégzett kódolás, az adatok kategorizálása és az elmélet alkotás.

## A kutatások elvégzése

Kutatásaimat a 2012 és 2019 közötti időszakban végrehajtott IBIR kialakítási projektek ihlették. Ez idő alatt többek között 9 szervezetben 12 információbiztonsági projekt megvalósításában vettem részt, mint vezető információbiztonsági szakértő. Minden elvégzett projekt újabb és újabb gazdasági szektor információbiztonsági kérdéseit hozta magával, lehetőséget nyújtva egy átfogó elemzés elvégzéséhez. Minden projekt során esettanulmányok készültek, továbbá mint a projektben részt vevő szakember közelről szemlélhettem a szervezetek szabályozási környezetét, szabályzatait és azok követelményeinek megvalósulását a gyakorlatban. Mint a projektek résztvevője minden esetben részletes információ állt rendelkezésemre, a szervezet működéséről és az információbiztonság aktuális állapotáról, ahonnan elindulva új, hatékony és hatásos információbiztonsági rendszer megvalósításában vehettem részt. Ez lehetőséget nyújtott a szervezetek működésének és információbiztonsági szabályozásának részletes elemzésére.

A vizsgálatokat projektenként hajtottam végre. Alkalmaztam a tartalomelemzést, megfigyelést, félig strukturált interjút és esettanulmány készítést. Az egyes projektek eredményeit konszolidáltam.

Minden egyes projekt befejezésével, összefoglaltam a tanulságokat, amelyeket beépítettem a következő projektbe.

Kutatásaim a munkám során elvégzett feladatok tapasztalataira, a szakirodalom feltárására és elemzésére épül. Interjút készítettem az érintett szervezetek IT és biztonsági vezetőivel, felhasználtam az informatikai és információbiztonsági rendszerek tervezése, vizsgálata, aktualizálása és bevezetése során gyűjtött tapasztalataimat. Elemeztem, hogy a szervezetekben kialakított információbiztonsági rendszer milyen mértékben működik együtt a szervezet feladatainak ellátásával, mennyire akadályozza a munkafolyamatok végrehajtását, milyen többlet terhet ró a szervezetre és mennyire tölti be szerepét az információ védelmének megvalósításában. A rendszerbiztonság tervezési projektek esetében a szervezetek üzleti vezetőinek hozzáállását vizsgáltam a biztonság megfelelő szintjének kialakításához. Az így összegyűjtött adatokat elemeztem és szintetizáltam egy működőképes információbiztonság irányítási rendszer szempontrendszerének kialakításához.

Ahhoz, hogy az elvégzett kutatás eleget tegyen a tudományosság szempontjainak, követtem az empirikus kutatások Molnár Dániel által megfogalmazott alapvető szempontjait [18], amelyek:

- a kutatási terv meghatározása;
- kutatási terv végrehajtása és az eltérések dokumentálása;
- adatgyűjtési hibák és téves eredmények kiszűrése;
- a tanulmány korlátjainak bemutatása
- és az eljárások bemutatása megismétléshez.

Az esettanulmányok elkészítése a munkám részeként zajlott, az adatokat meglévő dokumentumokból, vezetőkkel, szakértőkkel és a projektekben érintett részvevőkkel folytatott egyeztetések során és félig strukturált interjúk keretében gyűjtöttem, figyelve arra, hogy az érintett szervezetek érdekei ne sérülhessenek.

A kutatás során ötvöztem az akciókutatást az esettanulmánnyal és a megalapozott elmélettel. Minden elvégzett projekt egy-egy újabb adathalmazt jelentett, amelyek eredményei forrásként szolgáltak a soron következő projekt végrehajtásához.

## Az értekezés felépítése

Az **első fejezetben** bemutatom az információbiztonság szükségességét, szakirodalomban legyakrabban előforduló és a kutatómunkám során alkalmazott definícióját. Áttekintem az információbiztonságot befolyásoló legfontosabb nemzetközi és hazai szabványokat,

keretrendszereket és jogszabályokat. Feltérképezem az általam ismert gazdasági szektorokban előforduló leggyakoribb adatelemeket és elemzem azok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit.

A **második fejezetben** feltárom az információbiztonságot és kapcsolatait tárgyaló tudományos szakirodalmat, kitérek az információbiztonság állapotát és fejlesztését befolyásoló tényezőkre. Elemzem az információbiztonság és a szorosan kapcsolódó szakterületek: minőségirányítás és IT szolgáltatásmenedzsment kapcsolatát. Elemzem az információbiztonság munkafolyamatokra és a szervezet versenyképességére gyakorolt hatását. Kidolgozom az IBIR folyamatszemléletű bevezetési módját és összehasonlítom a szakirodalomban fellelhető bevezetési módokkal.

A **harmadik fejezetben** a kutatási projektjeim során interjúk keretében gyűjtött információ és elkészített esettanulmányok alapján a tudásrendezés módszertanát követve feltárom az információbiztonság megvalósításának problémáit. Kitérek az információbiztonság irányítási rendszerek hiányosságaira, amelyeket problémacsoportokba rendezek. Elemzem a feltárt problémák előfordulásának gyakoriságát és okait, majd kimutatom függetlenségüket a szervezet tevékenységétől és méretétől.

A **negyedik** fejezetben akciókutatás keretében gyűjtött információ alapján megalapozott elmélet segítségével kialakítom az eredményes IBIR modellt, amely integrálja a minőség- és IT szolgáltatásmenedzsmentet és kiküszöböli a harmadik fejezetben feltárt problémákat. Az modell tartalmazza a bevezetés sikerességének elérése érdekében elvégzendő munkafolyamatokat és betartandó szabályokat.

Az **ötödik** fejezetben létrehozom az integrált incidenskezelési modellt, amelynek bevezetésével megszüntethető a szervezetekben jellemzően egymástól függetlenül és átfedésben végrehajtott IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági incidenskezelés. Az integrált incidenskezelési folyamat nagy előnye a párhuzamosságok megszüntetésén túl, a folyamat végrehajtásának felgyorsítása az egyes szakterületek közötti azonnali információmegosztással.

# 1 INFORMÁCIÓBIZTONSÁG

Az ipar, kereskedelem és a közszolgáltatások működése is elképzelhetetlen infokommunikációs szolgáltatások nélkül. A hiteles és aktuális információ kulcsfontosságú a szervezetek működtetésének fenntartásában. Az információs rendszerek és a bennük kezelt információ biztonsága kritikus a szervezetek üzleti és ügyviteli folyamatainak fenntartásában. Ezáltal az információbiztonság egyre nagyobb szerepet kap a szervezetek életében, elérése nem öncélú, hanem a megbízható működés biztosításának kulcsfontosságú eleme [19].

Az a tény, hogy információbiztonságról beszélünk, magában hordozza, hogy annak kialakítása nem pusztán technológiai kérdés. Kiépítése során figyelembe kell venni az információ előfordulásának minden lehetséges formáját a szervezetben és komplex védelmi intézkedéshalmazt kell megvalósítani, amely kiterjed a szervezet minden munkatársára, partnerére, eszközére és folyamatára függetlenül attól, hogy azt támogatja vagy sem informatikai szolgáltatás. A védelmi intézkedések a veszélyforrásoknak megfelelően lehetnek fizikai, logikai, szervezet szervezési, valamint informatikai rendszerek életciklusához kapcsolódók. Az informatikai rendszerekhez kapcsolódó veszélyforrások és védelmi intézkedések részben megjelennek a fizikai, logikai és szervezet szervezési veszélyforrások között is.

Az információ előfordulása az informatikai rendszerekben tárolt és feldolgozott adatokon túl lehet papír alapú vagy szóbeli. Így az informatikai veszélyforrásokon túl további jelentős veszélyforrások fenyegetik az információ biztonságát. Az információt nem csak az informatikai rendszerekben kell védeni, hanem minden előfordulási formájában.

Az egyik legjelentősebb veszélyforrás, amely független az alkalmazott technológiától az úgynevezett social engineering típusú támadás, amely a felhasználói jóhiszeműséget, tudatlanságot, oda nem figyelést, hanyagságot stb. használja ki. Az E&Y, PwC, és Forst&Sullivan tanulmányai is foglalkoznak a témával, hogy információbiztonság szempontjából a leggyengébb láncszem az ember [20] [21] [22]. Ugyanerre utal Jeimy J. Cano is amikor arra hivatkozik, hogy a szervezet legértékesebb információjának biztonsága a hozzáférő felhasználók általi korrekt feldolgozástól függ [23]. Egyetértek ugyan ezekkel a megállapításokkal, ugyanakkor felhívom a figyelmet arra, hogyha nincs hatályban lévő megfelelő színvonalú és minőségű szabályozás, nincs mihez igazodniuk a dolgozóknak és felhasználóknak.

Egy másik gyakori veszélyforrás a hamis biztonságtudatosság, ami azt jelenti, hogy a szervezet és annak vezetői abban a tudatban vannak, hogy a szervezet információbiztonsága teljes körű és nem

fenyegeti semmilyen veszélyforrás, miközben hiányosságok vannak a védelmi intézkedésekben vagy a védelmi intézkedések során használt eszközökben. Megítélésem szerint ezt a hamis biztonságtudatot erősítik a rosszul vagy hiányosan összeállított információbiztonsági kérdőívek, amelyek félreértelmezhetők.

**Az információbiztonság fogalmára számos definíció létezik, de a legelterjedtebb az ISO/IEC 27001 szabvány szerinti** [24]**,** kutatásaim során is ezt a definíciót tekintettem alapnak. A definíciót az ISO/IEC 27000 szabvány - a szabványcsalád közös áttekintő dokumentuma - fogalomtára tartalmazza:

**Információbiztonság:** „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése" [25, p. 4];

**Bizalmasság:** „tulajdonság, miszerint az információkat nem teszik elérhetővé vagy nem adják ki jogosulatlan személyek, szervezetek vagy folyamatok számára" [25, p. 2]

**Sértetlenség:** „a pontosság és a teljesség tulajdonsága" [25, p. 5];

**Rendelkezésre állás:** „szükség szerint hozzáférhető és használható az arra felhatalmazottak által" [25, p. 2].

Az információbiztonságot gyakran keverik össze az informatikai biztonsággal, ami csak az elektronikus információs rendszerekben tárolt adatokra vonatkozik. Haig az információ és az informatikai - köztük a hálózat és az IoT - eszközök hadműveleti szempontú felhasználását és biztonságának fontosságát hangsúlyozza [26]. Meglátásom szerint ez a terület egyre nagyobb fontossággal bír, hiszen az IoT eszközök nem csak a hadviselésben, de az iparban és a magánszférában is egyre nagyobb szerepet kapnak. Emellett megjelenik még a kiberbiztonság fogalma, amelynek definíciója nem annyira egyértelmű. Kovács definiálja a kiberbiztonság fogalmát, amely nézőpontja szerint tartalmazza az információbiztonságot, de kevés a különbség az információbiztonság tágabban vett értelmezése és a kiberbiztonság között. A kiberteret gazdaság, társadalom és magánszféra struktúrára bontva elemzi. Vizsgálja a kibertér veszélyeit és a kiberbiztonság megvalósítását a kibertér különböző területeire, a bontás, az elemzéseket területi és szakterületi bontásban mutatja be [27]. Hasznosnak tartok egy-egy ilyen elemzést, de ne feledkezzünk meg arról, hogy a szakterületek átfedésben és szimbiózisban vannak egymással.

## 1.1 Jogszabályi háttér

Az információbiztonság egyre nagyobb hangsúlyt kap, egyre több és szigorúbb jogszabály írja elő az információ védelmét a szervezetek számára. Szádeczki Tamás „Szabályozott biztonság” című PhD értekezésében [28] részletesen kielemezte az érvényben lévő információbiztonságot érintő jogszabályokat. Azóta a jogi szabályozás jelentős átalakuláson ment át, új az egész társadalmat érintő jogszabályok jelentek meg. Jelen munkámnak nem célja újra feldolgozni a jogszabályi hátteret, de fontosnak tartom bemutatni az érvényben lévő legfontosabb jogszabályokat.

**General Data Protection Regulation (GDPR): AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE** (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) [29]. Európai szinten egységesíti a személyes adat fogalmát, meghatározza a személyes adatok kezelésének követelményeit és irányelveit, továbbá magas összegben határozza meg a megsértése esetén fizetendő minimális bírság mértékét.

**Federal Information Security Management Act (FISMA)** [30], megköveteli, hogy az Egyesült Államok szövetségi ügynökségei implementáljanak információbiztonsági programot információs rendszereik számára.

**Social Security Number Protection Act of 2011** [31], előírja az Amerikai Egészségügyi és Humán Szolgáltatások minisztere számára, hogy olyan eljárásokat dolgozzon ki amelyek kiküszöbölik a Medicare kedvezményezettek társadalombiztosítási számlaszámainak szükségtelen gyűjtését, használatát és megjelenítését a Medicare azonosító kártyákon és kommunikációban.

**Children's Online Privacy Protection Act of 2010: (COPPA)** [32], a 13 évnél fiatalabb amerikai gyermekek védelmére fogalmaz meg követelményeket a weboldalak és online szolgáltatások üzemeltetőivel szemben az érintettek személyes adatainak gyűjtésének és nyilvánosságra hozatalának korlátozására.

**2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv)** [33] és technológiai végrehajtási rendelete a **41/2015 BM rendelet (BMr)** [34], az állami és önkormányzati szervek információbiztonságának megteremtése és fenntartása érdekében. Kötelezővé teszi az informatikai rendszerek biztonsági szintbe sorolását

előre definiált skála alapján és kötelező kontrollokat ír elő az egyes biztonsági osztályokba sorolt rendszerek védelmének érdekében.

**2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól** [35], amely korszerűbb elektronikus ügyintézést tesz lehetővé a lakosság számára. Célja az elektronikus ügyintézés széles körű elterjesztése, az eljárások felgyorsítása és az adminisztrációs terhek csökkentése.

**910/2016 EU rendelet: eIDAS: eIDAS (electronic IDentification, Authentication and trust Services) AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.)** [36], amely szerint a gazdasági és szociális fejlődés fontos feltétele az online elektronikus környezetekbe vetett bizalom kiépítése. A rendelet célja az elektronikus tranzakciókba vetett bizalom közös alapokra helyezése az állampolgárok, gazdasági szereplők és közszféra számára növelve ezáltal az online szolgáltatások hatékonyságát.

**Információbiztonsági előírásokat tartalmazó ágazati jogszabályok a teljesség igénye nélkül:**

**Sarbanes-Oxley (SOX) Act of 2002** [37], védi a befektetőket és a nyilvánosságot a vállalati közzétételek pontosságának és megbízhatóságának növelésével, információbiztonsági követelményeket tartalmaz az informatikai rendszerek ellenőrzési követelményeihez;

**Gramm-Leach-Bliley Act (GLBA) of 1999** [38], USA jogszabály, amely a Pénzügyi Szolgáltatások Modernizációs Jogszabálya néven is ismert, követelményeket tartalmaz a fogyasztók pénzügyi információinak védelméhez;

**Health Insurance Portability and Accountability Act (HIPAA)** [39], az egészségbiztosítási hordozhatóságról és elszámoltathatóságról szóló törvény, amely biztonsági és adatvédelmi követelményeket is megfogalmaz;

**Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 - 16 CFR Part 681** [40], megköveteli a pénzügyi intézményektől és a hitelezőktől, hogy hajtsanak végre személyazonosság-lopási megelőzési programot a személyazonosság-lopások felderítésére, megelőzésére és enyhítésére.

## 1.2 Szabványok és keretrendszerek

A szabványok implementálása opcionális. A szervezetek jellemzően a saját működésük javítása érdekében vezetik be. Bevezetésük által a szervezetek jobb produktivitást, minőséget és biztonságot érhetnek el. A szabványok szerinti tanúsítás versenyelőnyt jelent, mivel egy független

3. fél végzi el a szabvány követelményeinek teljesülését, amelynek jogosultsága van tanúsítványt kiállítani. Bizonyos körülmények között előfordulhat, hogy bizonyos szabványok bevezetése kötelezővé válik a szervezetek számára. Ilyen esetek lehetnek: tanúsítvány meglétének elvárása beszállítók felé vagy pályázaton való indulás feltétele. Tapasztalataim alapján a leggyakrabban implementált információbiztonságot érintő szabványok [41]:

**MSZ ISO/IEC 27001** Informatika. Biztonságtechnika. Az információbiztonság irányítás rendszerei. Követelménye [24], általános információbiztonsági szabvány, amely teljeskörűen tárgyalja a szervezetek információbiztonságát és lehetővé teszi annak tanúsítását;

**MSZ ISO/20000-1:2013** Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei [42], IT szolgáltatásmenedzsment szabvány, amely támogatja ITIL alapú IT szolgáltatási folyamatok bevezetését és tanúsítását;

**PCI-DSS (Payment Card Industry Data Security Standard)** [43], folyamatosan fejlődő szabvány a fizetések biztonsága és a bankkártya tranzakciókkal kapcsolatos információk védelme érdekében, kötelező a fizetési és bankkártya adatokat kezelő szervezetek számára;

**NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations** [44], folyamatosan fejlődő USA szabvány, biztonsági és adatvédelmi kontroll katalógust biztosít a szervezeti műveletek és vagyon, az egyének, más szervezetek és a nemzet védelme a különféle fenyegetések és kockázatok ellen, ideértve az ellenséges támadásokat, az emberi hibákat, a természeti katasztrófákat, a strukturális kudarcokat, a külföldi hírszerző egységeket és az adatvédelmi kockázatokat;

**NIST SP 800-61 Computer Security Incident Handling Guide** [45], segíti a szervezeteket reagálási képességek kialakításában a számítógépes biztonsági eseményekre, valamint az események hatékony és eredményes kezelésében.

**Információbiztonság szempontjából leggyakrabban alkalmazott keretrendszerek:**

**COBIT (Control Objectives for IT and Related Technology)** az ISACA folyamatosan fejlődő keretrendszere. A 4.1 verzió a keretrendszert, kontroll célkitűzéseket, vezetői útmutatókat és érettségi modelleket tartalmaz [46]. Az 5-ös verzió kiegészült kockázatelemzés és IT irányítási fejezetekkel és „A vállalati IT irányítás és menedzsment üzleti keretrendszere” címet kapta [47]. A COBIT 2019 az 5-ös verzió továbbfejlesztése, szervezetre szabott dinamikus irányítási rendszerrel.

**ITIL (IT Infrastructure Library)** az IT szolgáltatásmenedzsment legjobb gyakorlata. Az első fontos verziója az **ITIL V2** amelynek két alapkönyve a **Service Support** [48] és a **Service Delivery** [49] melyek az IT szolgáltatás támogatás és nyújtás munkafolyamatainak legjobb gyakorlatát mutatják be. Ezt bővíti ki a V3 az IT szolgáltatások életciklus modelljére, amelyet 5 szakaszra bont. Az **ITIL Service Strategy** az IT szolgáltatási stratégia meghatározásához szükséges témaköröket tárgyalja többek között a piac és üzleti stratégiával való összehangolást helyezi fókuszba [50]. Az **ITIL Service Design** a szolgáltatások tervezésének munkafolyamatait mutatja be, kitér az IT szolgáltatás folytonosság és rendelkezésre állás, valamint az Információbiztonság menedzsmentre [51]. Az **ITIL Service Transition** a szolgáltatások bevetésével és változtatásával járó munkafolyamatokat tartalmazza beleértve a változások tesztelését, kiértékelését, az eszköz és konfigurációkezelést, valamint a tudásmenedzsmentet [52]. Az **ITIL Service Operation** a szolgáltatások üzemeltetési munkafolyamatait írja le: eseménykezelés, incidenskezelés, kérésteljesítés, problémakezelés, és hozzáférés menedzsment [53]. Az **ITIL Continual Service Improvement** a szolgáltatások folyamatos javításának hét lépéses folyamatát írja le [54]. Az **ITIL V4** az értekezés írásának időpontjában még kidolgozás alatt áll, amely az életciklus szemlélet helyett az értékteremtést és az értékláncokat helyezi fő fókuszba.

A vonatkozó jogszabályok, szabványok és keretrendszerek listája megtalálható a Muha és Krasznay által 2014-ben összeállított, 2018-ban frissített: Az elektronikus információs rendszerek biztonságának menedzselése című tananyagban [55].

## 1.3 Információbiztonság különböző gazdasági szektorokban

Az információbiztonsági követelmények az egyes szervezetek esetében más és más szempontból válnak fontossá. Áttekintve az iparágakat, az információbiztonság más-más jellemzői kerülnek előtérbe. A szervezetek méretüktől, működési területüktől és fejlettségüktől függően más-más informatikai technológiát használnak. Az informatikai eszközöket és általuk feldolgozott adatokat fenyegető veszélyforrások függenek a kiépített technológiától, így azok elhárítására más-más védelmi intézkedésekre van szükség.

### 1.3.1 Információbiztonság az államigazgatásban

Állami szervek felelősek számos kritikus fontosságú, legmagasabb biztonsági szintet igénylő tevékenység végrehajtásáért. A teljesség igénye nélkül ide tartoznak a személyes okmányok igénylése és előállítása, az egészségbiztosítási szolgáltatások nyújtása, a nyugdíjbiztosítási és folyósítási szolgáltatások biztosítása, a bűnüldözés és bűnmegelőzés, a közoktatással, honvédelemmel, a nemzetbiztonsággal kapcsolatos tevékenységek. E szolgáltatások nyújtása

során az állami intézmények nagy mennyiségű személyes és kiemelten védett adatot kezelnek. Ezen adatok kezelése során kiemelt szerepet játszik az adatok bizalmasságának és sértetlenségének megőrzése továbbá rendelkezésre állásának biztosítása. Az Ibtv megjelenését megelőzően - a szerző tapasztalatai szerint - az állami és önkormányzati szektor vezetői csak részben ismerték fel az információbiztonság fontosságát, a szakirányítást végző szervek pedig nem minden esetben biztosították a szükséges emberi és anyagi erőforrásokat.

A fenti cél megvalósításának érdekében Magyarország Országgyűlése megalkotta az állami és önkormányzati szervezetekre vonatkozó Ibtv és annak végrehajtási rendeleteit. A védelmi intézkedéseket tartalmazó végrehajtási rendelete a NIST SP 800-53 szabványra épül, gyakorlatilag annak kivonatolt és módosított magyar változata. Végrehajtási rendeletei a technológiai 77/2013. (XII. 19.) NFM rendelet [56], majd az ezt kiváltó BMr [34] részleteiben kitér az informatikai rendszerek biztonsági osztályba sorolására és az egyes osztályok esetében megvalósítandó védelmi intézkedésekre. A 26/2013. (X. 21.) KIM rendelet [57], az információbiztonsági szerepkörökkel rendelkező személyek oktatását írja elő. A 42/2015. (VII. 15) BM rendelet [58], a jogszabály hatálya alá tartozó szervezetek hatósági nyilvántartásba vételét írja elő. A 187/2015 (VII.13.) Kormányrendelet [59], pedig az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok feladatait és hatáskörét szabályozza, valamint a zárt célú elektronikus információs rendszerek meghatározását támogatja.

Kutatási projektekben szerzett tapasztalataim alapján a jogszabály első kihirdetésekor még nem állt rendelkezésre a jogszabály által előírt megfelelő számú és képesítésű szakember. Az állami és önkormányzati szervek sok esetben saját erőből képesítés nélküli munkatársakkal próbálták megoldani a hiányzó szakemberek munkáját, mások pedig külső partnerekre bízták az IBIR kialakítását miközben nem vettek részt annak megalkotásában és nem gyakoroltak megfelelő kontrollt az elkészült szabályozási rendszer felett. Így az elkészült szabályzatok ugyan teljesítették a jogszabály előírásait, de sok esetben nem illeszkedtek a szervezet munkafolyamataihoz és nem állt rendelkezésre az elméletben megfogalmazott kontrollok kiépítéséhez szükséges anyagi erőforrás. Másrészről a jogszabály alkotója az előírt követelmények mellé nem rendelt megfelelő szintű anyagi erőforrást és a felügyeleti szerveknek sem volt megfelelő számú és képesítésű szakemberük az ellenőrzéshez, így az első években az eredmény elmaradt az elvárttól.

A minél jobb információbiztonsági környezetek kialakításának érdekében a jogalkotók és a jogszabály végrehajtását felügyelő szerv: a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), mely 2015. október 1-től a Nemzeti Kibervédelmi Intézet részévé vált, folyamatosan nyomon követi a jogszabályok alkalmazásának módját, betarthatóságát és szükség esetén

javaslatot tesznek ezek módosítására, használhatóbbá tételére, hozzájárulva ez által az információvédelem megvalósításához.

Az Ibtv-t 2015 első felében vizsgálták felül amikor több jelentős módosításon esett át. A rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolásának változásával az elektronikus információs rendszert üzemeltető szervezetekkel szembeni elvárások szigorodtak, és az új rendszerek bevezetését érintő követelmények teljesítésének halasztott teljesítési lehetősége megszűnt, azokat már az éles induláskor teljesíteni kell.

Az új technológiai rendelet a BMr felépítése több témakörben is szakított az eredeti NIST SP-800-53 szabvány struktúráját követő felépítéssel és logikájával. Kontrollokat csoportosítottak át a fejezetek között, és kivettek belőle több menedzsment jellegű követelményt: az informatikai biztonsági politikát, az informatikai biztonsági stratégiát, a szervezet szintű architektúrát, a kockázatkezelési stratégiát és a pénzügyi erőforrások biztosításának követelményeit.

A jogszabály első megjelenésekor sok kritikát kapott a technológiai végrehajtási rendelet a szakma részéről, de egyetértés volt abban, hogy szükség van rá. Ez a rendelet jelentős módosításon esett át, a kontrollok átcsoportosítása és a szükségtelen előírások eltávolítása megítélésem szerint sokat javított a végrehajthatóságán és megítélésén is.

Az információbiztonság fontosságára hívja fel a figyelmet Horváth a Közérthetően nemcsak az IT biztonságról című közszférában dolgozóknak szánt tájékoztató kiadványa is [60], amely az információbiztonság tudatosság növelését célozta meg.

Az elmúlt években - a jogszabályok kereteinek megfelelően - felerősödött az állami és önkormányzati szervek információbiztonsági átvilágítása, hiányosságainak meghatározása és tervezetek készültek a feltárt hiányosságok kockázatainak megszüntetésére vagy csökkentésére. Az információbiztonsági felmérések rámutattak a legfőbb hiányosságokra. A kutatási projektekben szerzett tapasztalataim alapján ezek kezelhetők, ha a szervezet szisztematikusan felépített programként tekint az információbiztonság megvalósítására. A program fontos elemei, amelyeket minden szervezet esetében priorizálni kell: a biztonságtudatosság növelése, szabályzatok létrehozása és megerősítése, eljárásrendek kialakítása és megújítása, ügyviteli és informatikai folyamatok biztonságát támogató megoldások bevezetése, rendszerfelügyeleti megoldások implementálása, konfigurációkezelés bevezetése, formalizált változáskezelés kialakítása, az információbiztonság követelményeinek beépítése a munkafolyamatokba stb.

Az BMr strukturálja és részletezi az Ibtv követelményeit. Az egyes követelménypontokban meghatározott elvárások esetenként több tevékenységet is megfogalmaznak, ami nehezíti a követelmények érthetőséget, gátolja azok értelmezését és ezáltal azok alkalmazását is.

### 1.3.2 Információbiztonság a különböző iparágakban

Az ipari automatizálás korát éljük. Az Európai Parlament 2016-ban fogalmazta meg álláspontját az Ipar 4.0-val kapcsolatban: „Az ipar 4.0 a termelési folyamatok olyan szervezését írja le, melynek keretében az eszközök önállóan kommunikálnak egymással az értéklánc mentén: a jövő egy olyan „okos" gyárát hozva létre ezzel, amelyben a számítógép-vezérelt rendszerek nyomon követik a fizikai folyamatokat, létrehozzák a fizikai valóság virtuális mását és decentralizált döntéseket hoznak önszervező mechanizmusok alapján." [61]. Az ipar 4.0-ban megfogalmazott követelményeknek megfelelően az ipari termelési folyamatok végrehajtása: a gyártás előkészítése, tervezésére és a legyártott termékek minőségbiztosítása során folyamatosan támaszkodik a feladatok automatizált elvégzéséhez szükséges információra. Elengedhetetlenné vált a gyártást támogató rendszerek folyamatos működése, az általuk biztosított információ sértetlensége és rendelkezésre állása.

A gyártósorokon a megrendeléseknek megfelelő termékeket állítják elő. Mivel ugyanazokon a gyártósorokon különböző termékek előállítása folyik, a gyártástervezésnél fontos szerepet játszik a termékek gyártásának sorrendje, a gyártandó termékek mennyiségének meghatározása és a minimum mennyiség, amelyet egy termékből a gyártás során elő kell állítani a gazdaságosság megteremtéséhez. A gyártási folyamatok működésének biztosításához elengedhetetlen a termékek gyártásához szükséges információk eljuttatása a gyártósori berendezésekhez. A gyártósori infokommunikációs szolgáltatások leállása, termeléskiesést okoz, ez által csökken az előállított termékek mennyisége és gazdasági kár keletkezik elmaradt termelés formájában. A másik fontos szempont a gyártott termékek minőségének biztosítása. Ennek érdekében a gyártás utolsó fázisában tesztelik az elkészült termékeket. A tesztelés lehet manuális vagy automatizált. A tesztelési eredmények gyűjtése, a kész termékek minőségi paramétereinek tárolása fontos szerepet játszik a gyártási technológiák fejlesztésében és a legyártott termékek továbbfejlesztésében. Az így összegyűjtött információból meghatározható a hibásan gyártott termékek aránya, az egyedi termékek minőségi mutatói, a gyártósor és technológia alkalmassága az egyes termékek gyártásához.

Az így összegyűjtött gyártástervezési és minőségbiztosítási adatok nemcsak a termék gyártójának jelentenek hasznos információt, hanem a konkurencia számára is. Mivel sok termék gyártása

bérgyártás keretében zajlik, fontos megemlíteni, hogy egy gyártósoron több gyártó termékeit is előállíthatják. A bérgyártóknak kiemelt figyelmet kell fordítaniuk arra, hogy az előállított termékekhez köthető információ csak az adott termék megrendelőjéhez juthasson el.

Egyre fontosabb az információbiztonság az autóiparban is. A gyártók különböző, részben átfedő információbiztonsági elvárásokat támasztottak a beszállítókkal szemben, ami jelentős terhet rótt rájuk a megfeleléshez való felkészülésben. Emiatt 2017-ben a VDA egy új egységes követelmény és értékelési rendszert dolgozott ki TISAX (Trusted Information Security Assessment Exchange) néven, ami az ISO/IEC 27001 szabványra épül [62].

A tervezési munkák végrehajtása általában számítógéppel támogatott folyamat. A munka során értékes információk keletkeznek, amelyek lehetnek eredeti ötletek, megvalósítási tanulmányok, kivitelezéshez szükséges számítások stb. Ezen információk meghatározzák a végtermék megjelenését, alakját, minőségét, használhatóságát. Az így keletkezett adatok sok esetben üzleti titoknak minősülnek. Mivel más szervezetek is dolgoznak hasonló terveken, így a tervinformációk kiszivárgása előnyhöz juttattathatja a konkurenciát.

### 1.3.3 Információbiztonság a kereskedelemben és a szolgáltató iparban

Az 1990-es évek végén és a 2000-es évek elején a dotcom cégek megjelenésével fellendült az internetes kereskedelem, amely lehetővé tette a különböző termékek értékesítését és megrendelését egyrészt Business-to-Business (B2B) illetve Business-to-Consumer (B2C) internetes kereskedelmi megoldások kialakításával. Az e-kereskedelem elterjedésével fontossá vált az árukészletek mennyiségének azonnali lekérdezhetősége, az áruk körforgásának optimalizálása érdekében. Kiemelt fontosságúvá vált a beszerzési árak elérhetősége és pontossága, a pénztárak árazási információval való ellátása, a beszerzett és eladatott áruk mennyiségének folyamatos nyomon követése. Ez magával hozta a kereskedelem lebonyolításához szükséges adatok rendelkezésre állásának és pontosságának követelményét. Fontos megemlíteni, hogy a beszerzési árak és az eladási árak képzése bizalmas információ, hiszen a konkurencia ezek megismerése esetén versenyelőnyre tehet szert.

A szolgáltató iparban egyre fontosabb szerepet kap az ügyfelekkel folytatott kommunikáció. A közműszolgáltatók esetében a mérőóra állásának telefonos diktálását felváltotta a kényelmesebb és barátságosabb internetes beküldés, a papír alapú számlákat és fizetési utalványokat pedig az elektronikus számlázás és online fizetés. Egyre több gyártó döntött a garanciális ügyek online formában történő lebonyolítása mellett, ami kényelmes, megbízható és visszakereshető ügyintézést tesz lehetővé az ügyfelek számára. Emellett egyre több olyan szolgáltató jelenik meg

a piacon beleértve az egészségügyi szolgáltatókat is, amelyek szolgáltatásait teljes mértékben vagy részben online formában is igénybe lehet venni, szolgáltatásaik díjáról pedig elektronikus számlát állítanak ki.

Az internetes ügyintézés során fontos szerepe van a személyes adatok pontosságának és bizalmasságának. A személyes adatok bizalmasságának megőrzése és személyiséglopás megakadályozása érdében jogszabályok születtek, a teljesség igénye nélkül a legfontosabbak az Európai Unióban a GDPR az Amerikai Egyesült Államokban pedig a GLBA és a HIPPA.

Az internetes fizetés elterjedésével megszaporodtak a bankkártya és hitelkártya csalások ezáltal fontossá vált a bankkártya tranzakciók és a kapcsolódó adatok védelme. A bankkártya és hitelkártya adatok biztonságos kezeléséhez a PCI (Payment Card Industry) Security Standards Council kiadta a DSS (Data Security Standard) szabványt [43], amely betartását a kártyatársaságok kötelezővé tették minden bankkártya információt feldolgozó szervezet számára.

### 1.3.4 Információbiztonság a pénzügyi szektorban

Banki környezetben nemcsak személyes adatok fordulnak elő, hanem személyekhez köthető további bizalmas információk, például a bankszámla adatai beleértve a bankszámlák egyenlegét, a telefonbankhoz kapcsolódó felhasználói azonosítót és jelszót, a bankszámlához tartozó bankkártyák adatait, az internetbanki hozzáféréshez szükséges felhasználónevet és jelszót, a kétfaktoros azonosításhoz szükséges telefonszámot stb. A banki működést szabályozó jogszabályok kitérnek a bankok által kezelt adatok információbiztonságára. Ezek részben üzleti és ügyviteli síkon határozzák meg az általuk kezelt információk biztonsági paramétereit, másrészt pedig informatikai rendszerekre érvényes szabályozással. Ugyanakkor a bankbiztonsági követelményeknek való megfelelés szükségessé teszi az információbiztonság teljes körű megvalósítását mind az írott vagy elhangzott információ mind pedig az informatikai rendszerekben fellelhető adatok szempontjából. A bankok működésének biztonsági feltételeit a lokális és globális jogszabályi környezet írja elő. Ahhoz, hogy a bankok teljesíteni tudják a biztonsági követelményeket szabványokra és működéstámogató keretrendszerekre támaszkodnak, ezek közül a legismertebbek a COBIT és az ITIL.

A bankszektorban az információbiztonság megteremtésének és fenntartásának érdekében alkalmazott szabványok az MSZ ISO/IEC 27001:2015 [24], PCI DSS [43] és MSZ EN ISO 9001:2015. Az ISO/IEC szabványokkal ellentétben a PCI DSS szabvány ingyenesen elérhető és alkalmazása kötelező a bankkártyával végzett tranzakciós adatok védelmének érdekében a bankkártya tranzakciókat végrehajtó szervezetek számára [43]. Az ITIL és MSZ ISO/IEC 20000-

1:2013 szabvány szerinti működés nem előírás, de alkalmazása hozzájárul az informatikai és ezáltal az üzleti szolgáltatások megfelelő szintű és költséghatékony nyújtásához. Az információbiztonság egyre szigorúbb szabályozása és a szabványok fejlődése egyre inkább előtérbe helyezi a NIST SP 800-53 szabvány alkalmazását banki területen.

## 1.4 Összegzés

Az informatika és az infokommunikációs hálózatok társadalmunk minden területét átszövő elterjedése és robbanásszerű fejlődése, lehetővé tette az információ azonnali elérhetőségét a világ bármely pontjáról. A vállalatok tevékenységeinek végrehajtása függővé vált a rendelkezésre álló információtól és annak minőségétől. Az információ bizalmasságának megőrzése kiemelt szerepet kapott gazdasági szektortól függetlenül. Ez szükségessé tette az információbiztonság fogalmának definiálását. **Áttekintettem az információbiztonságra vonatkozó, jogszabályokat, szabványokat és keretrendszereket. Megállapítottam, hogy információbiztonság alatt többségük az információ bizalmasságát, sértetlenséget és rendelkezésre állását érti, ami az ISO/IEC 27001 szabvány szeinti definíciója. Kutatásaim során és értekezésemben én is ezt a definíciót alkalmazom.**

Elemeztem az információbiztonság jellemzőivel szembeni elvárásokat az egyes gazdasági szektorokban. Megállapítottam, hogy a különböző gazdasági szektorok esetén (közigazgatás, gyártás, tervezés, pénzügy, kereskedelem és szolgáltatás) más-más információ fordul elő és ezek bizalmasság, sértetlenség és rendelkezésre állás követelményei eltérnek egymástól. Az 1-es táblázatban a teljesség igénye nélkül láthatók, hogy az egyes iparágakban előforduló legyakoribb adatkörök esetében az információ mely tulajdonságai vannak fókuszban.

| Iparág | Érintett adatok | Bizalmasság | Sértetlenség | Rendelkezésre állás |
|---|---|---|---|---|
| **Közigazgatás** | személyes adatok | X | X | |
| | nemzeti adatvagyon | | X | |
| | minősített adatok | X | X | |
| **Gyártás** | termék előállítás | | X | X |
| | termék tesztelés | X | X | |
| **Tervezés** | tervek és tervezés | X | X | |
| **Kereskedelem és szolgáltatás** | árazás, beszerzés, megrendelés és értékesítés | X | X | X |
| | személyes adatok | X | | |
| | logisztikai információk | X | X | X |
| **Pénzügyi szektor** | személyes adatok | X | X | X |
| | pénzügyi tranzakciók | X | X | |
| | számla, egyenleg, bankkártya | X | X | X |

*1. táblázat Az iparágak információbiztonságának legfontosabb jellemzői (saját szerkesztés)*

# 2 AZ INFORMÁCIÓBIZTONSÁG MEGVALÓSÍTÁSA

Az információbiztonság kiterjed minden szervezeti egységre és mint az 1-es fejezetben láttuk, fontos szerepet játszik a szervezetek életében. Megvalósításának minősége hatással van a szervezet működésére, azaz a munkafolyamatok végrehajtására, az elkészült termékek és nyújtott szolgáltatások minőségére és nem utolsó sorban az IT szolgáltatási folyamatok kialakítására és fenntartására.

## 2.1 Az információbiztonság kapcsolatai

A hatékonyan működő gyártási folyamatok, valamint az ügyfeleknek nyújtott minőségi és megbízható szolgáltatások megvalósítása és fenntartása érdekében a szervezetek IT szolgáltatásokat üzemeltetnek vagy vesznek igénybe és minőségirányítási rendszert működtetnek. Emellett a jogszabályok megkövetelik a személyes adatok védelmét, amelyek illetéktelen vagy rosszindulatú felhasználása károkat okozhat az érintetteknek. Ez szükségessé teszi az információbiztonság, minőségmenedzsment, IT szolgáltatásmenedzsment és adatvédelem összefüggéseinek vizsgálatát.

### 2.1.1 Információbiztonság és adatvédelem

Az adatvédelem kifejezés, mint a személyes adatok védelme került be a jogszabályokba és a köztudatba. A GDPR, amelynek hatályba lépési ideje 2018. május.25. kimondja: „A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése, a GDPR I. (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy „Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.” [29, p. 1] [63, p. 55]. A személyes adat fogalmát a GDPR a következőképpen definiálja: „azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható” [29, p. 33]. A rendelet felülírja az Európai Unió (EU) országainak adatvédelmi törvényeit és összehangolást igényel velük.

A személyes adatok védelmét Magyarországon a 2011. évi CXII. törvény (továbbiakban Infotv.) [64] írja elő, amely összehangolásra került az EU általános adatvédelmi rendeletével. Célja, hogy a természetes személyek magánszféráját a szervezetek tiszteletben tartsák, de emellett

érvényesüljön a közügyek átláthatóságának elve is, azaz a közérdekű adatok nyilvánossága. A jogszabály előírja a személyes adatok kezelésének feltételeit és ezáltal biztosítja azok bizalmasságának megőrzését. A jogszabály érvényes minden olyan szervezetre iparágtól függetlenül, amely működése során személyes adatokat kezel.

A célok betartásának érdekében a 2011. évi CXII. törvény (Infotv.) előírja, hogy a szervezeteknek hozzájárulást kell kérniük az érintettektől az adatok adott célra való felhasználáshoz, be kell jelenteniük az adatkezelést a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH), adatkezelési és adattovábbítási naplót kell vezetniük, az érintettek kérésére információt kell szolgáltatniuk az adatok kezeléséről és továbbításáról, biztosítaniuk kell, hogy az adatok nem férhetők hozzá illetéktelenek számára [64].

Mint láthatjuk, az adatvédelem kimeríti az információ bizalmasságának elvét, így szorosan összefügg az információbiztonsággal. Ez egyben azt is jelenti, hogy a szervezeteknek minden lehetséges eszközzel védeniük kell a személyes adatok bizalmasságát. Az állami és önkormányzati szervek esetében az információbiztonság megvalósítását az Ibtv és annak technológiai végrehajtási rendelete a BMr írja elő, amely kiemelten veszik figyelembe a személyes adatok védelmét az informatikai rendszerek besorolása során [34].

### 2.1.2 Az információbiztonság és IT szolgáltatásmenedzsment kapcsolata

Nagyobb szervezetek esetében a fontos üzleti szolgáltatásokat jelentős számú és méretű informatikai rendszer támogatja. Az üzleti folyamatok támogatását biztosító informatikai szolgáltatások - funkciók, infrastruktúra és folyamatok - megtervezése, beszerzése, implementálása, üzemeltetése, folyamatos fejlesztése és szakszerű megszüntetése fontos szerepet jártszik a minőségi, vállalt szolgáltatási szintnek megfelelő üzleti szolgáltatások nyújtásában.

Az ITIL a brit kormányzat által kidolgozott, nemzetközileg elfogadott ajánlásgyűjtemény, amely informatikai szolgáltatások nyújtásának optimalizálását célozza meg, azaz minőségi szolgáltatások nyújtását a lehető legkedvezőbb áron. Az MSZ ISO/IEC 20000:2013 az ITIL-re épülő IT szolgáltatásmenedzsment szabvány. Az MSZ ISO/IEC 20000-1:2013 azokat a követelményeket tartalmazza, amelyek támogatják az informatikai szolgáltatások tervezését, bevezetést, fejlesztést, nyújtást és ez által támogatja mind a szolgáltatókat mind pedig az ügyfeleket [42]. Az ISO/IEC 20000-2:2012 támogatást nyújt az MSZ ISO/IEC 20000-1:2013 szolgáltatásmenedzsment rendszer alkalmazásához [65]. A minőségi, optimalizált és költséghatékony informatikai

szolgáltatások megvalósításához elengedhetetlen az ITIL alapokra helyezett informatikai működési modell, adott esetben MSZ ISO/IEC 20000-1:2013 szabvány szerinti tanúsítással.

Az ITIL a szabványokkal és a COBIT keretrendszerrel ellentétben, amelyek követelményeket – minek kell megfelelni – fogalmaznak meg, ajánlásokat – hogyan valósítsuk meg – tartalmaz legjobb gyakorlatok formájában az üzleti folyamatokat támogató informatikai szolgáltatások kialakításához, üzemeltetéséhez és folyamatos fejlesztéséhez. A szervezet méretétől, a nyújtott informatikai szolgáltatások és informatikai eszközök számosságától függően bevezetése és működtetése IT szolgáltatásmenedzsment eszközzel is támogatható. Számos gyártói és nyílt forráskódú informatikai rendszer áll rendelkezésre, amelyek különböző szintű támogatást nyújtanak az IT üzemeltetési folyamatok végrehajtásában. Ezek alapját általában konfigurációs adatbázis képezi, amely tartalmazza az informatikai eszközöket és azok kapcsolatait.

A minőségi üzleti szolgáltatások folyamatos nyújtásának fontos feltétele az információ és annak rendelkezésre állását támogató IT szolgáltatások biztosítása. Az IT szervezet ITIL alapú működése adott esetben MSZ ISO/IEC 20000-1:2013 szabvány szerinti tanúsítása nagymértékben hozzájárul az informatikai rendszerek működtetésének és üzemeltetésének optimalizálásához. Ez elősegíti az informatikai rendszerek és a rendszerekben létrehozott, tárolt és feldolgozott információk rendelkezésre állásának biztosítását, de nem terjed ki az informatikai rendszereken kívül működő üzleti és támogató munkafolyamatok által kezelt információkra.

Az információs rendszerekben tárolt és kezelt információ védelmének érdekében az ITIL V3 a szolgáltatás életciklus tervezési fázisában definiálja az információbiztonság menedzsment folyamatot. Ennek a folyamatnak a célját a következőképpen határozza meg: „Az információbiztonság menedzsment célja az, hogy megvédje az információt, a felhasználók érdekeit, az információs és kommunikációs rendszereket, amelyek az információt szolgáltatják azoktól az ártalmaktól, amelyeket a bizalmasság, sértetlenség és rendelkezésre állás sérülése okoz.” [51, p. 197]. Ez a definíció nagyon közel áll az MSZ ISO/IEC 27001 szabvány definíciójához, az információbiztonság bizalmasság, sértetlenség és rendelkezésre állás fogalmakra építésén túl kitér az információt használó személyek és szervezetek érdekeinek védelmére is.

Az ITIL V3 az Információbiztonság menedzsment folyamatának tevékenységeit a jól ismert PDCA (Plan, Do, Check, Act) ciklusra alapozza.

**Tervezés:** A tevékenység célja a megfelelő biztonsági intézkedések kidolgozása és ajánlása, a szervezet követelményeinek megértése alapján. Ebben a szakaszban az információbiztonság

menedzsment együttműködik a szolgáltatási szint menedzsmenttel a szolgáltatási szint megállapodásban meghatározott biztonsági követelmények megértése érdekében.

**Implementálás:** Ez a feladat biztosítja, hogy megfelelő eljárások, eszközök és ellenőrzések legyenek érvényben az információbiztonság menedzsment szabályzatának végrehajtásához. Biztosítja továbbá, hogy a biztonsági intézkedéseket a meghatározott terv szerint hajtsák végre.

**Kiértékelés:** Ez a feladat biztosítja a biztonsági megvalósítás sikerének mérését. Ennek érdekében rendszeresen elvégzi az informatikai rendszerek műszaki és biztonsági auditjait. Ellenőrzi, hogy a biztonság megvalósítása megfelel-e a szolgáltatási és üzemeltetési szint megállapodásokban meghatározott informatikai biztonsági irányelveknek és biztonsági követelményeknek.

**Karbantartás:** Ebben a fázisban megtörténik a biztonsági értékelés eredményeinek kiértékelése. Ez alapján készül javaslattétel biztonsági javításokra és biztonsági megállapodások javítására.

Nem szabad elfelejteni, hogy ezek nem egyszeri tevékenységek, hanem ciklikusan ismétlődnek. Az ITIL V3 szerint az információbiztonság menedzsment folyamat 4 részfolyamatból áll, ezek a következők.

**Biztonsági kontrollok tervezése:** Felel a megfelelő technikai és adminisztratív intézkedések megtervezéséért a szervezet eszközei, információi, adatai és szolgáltatásai bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében. A kontrollokat adminisztratív, logikai és fizikai csoportokba sorolja.

**Biztonság ellenőrzés és tesztelés:** Felel a biztonsági kontrollok és biztonsági tevékenységek megvalósításának rendszeres teszteléséért és kiértékeléséért,

**Biztonsági incidensek kezelése:** Célja a támadások és behatolások felderítése és leküzdése, valamint a biztonsági szabályok megsértése által okozott károk minimalizálása.

**Biztonsági felülvizsgálatok:** Rendszeresen vizsgálni kell, hogy a biztonsági intézkedések és eljárások összhangban vannak-e az üzleti kockázatokkal, továbbá, hogy az intézkedéseket és eljárásokat rendszeresen karbantartják-e és tesztelik-e.

Az ITIL az IT szolgáltatások biztonságos és költséghatékony nyújtásának érdekében sok ponton kapcsolódik az információbiztonság témaköréhez [66].

### 2.1.3 Az információbiztonság és minőségbiztosítás kapcsolata

Figyelembe véve, hogy mára minden szervezet számára előnyös, követendő, de adott esetekben kötelező is az MSZ EN ISO 9001:2015 [67] vagy AQAP (Allied Quality Assurance Publications - Szövetségi Minőségbiztosítási Kiadványok) minőségbiztosítási szabványok szerinti működés vagy tanúsítás, számolni kell azzal, hogy a szervezetek már rendelkeznek bevezetett minőségirányítási rendszerrel. A NATO (North Atlantic Treaty Organization) beszállítók esetében szerződéses követelményként jelenik meg az AQAP, amely ráépül az ISO szabványokra és amelyeket további követelményekkel egészít ki.

A bevezetett minőségirányítási rendszer szerinti működés nem csak az üzleti, hanem a szervezet működését támogató folyamatokra is kiterjed, beleértve az informatikai rendszerek életciklusának menedzsmentjét a stratégiától elindulva a tervezésen, bevezetésen és üzemeltetésen túl a folyamatos fejlesztési eljárásokig. Ez magával hozza az adatok sértetlenségnek biztosítását, amely az információbiztonság egyik lényeges összetevője.

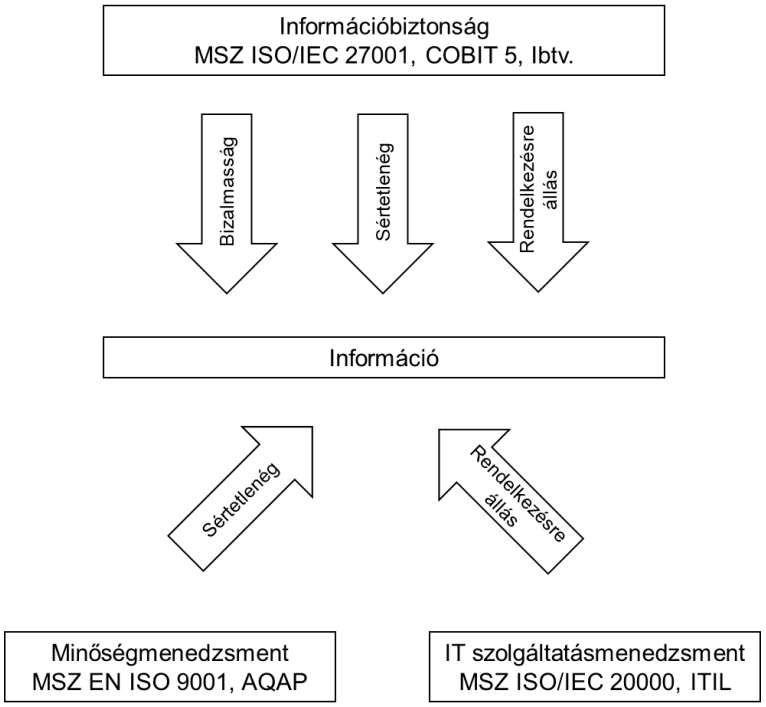
### 2.1.4 Az információbiztonság, minőségirányítás és IT szolgáltatásmenedzsment összefüggései

A gyakorlatban egyre többször találkozunk azzal a ténnyel, hogy jogszabályok írják elő az információbiztonság megvalósítását, de az MSZ ISO/IEC 27001:2014 szabvány szerinti tanúsításra is szükség van egy-egy szervezet életében. Ugyanakkor fontos az informatikai szolgáltatások általi értékteremtés, a költséghatékony IT szolgáltatásmenedzsment kialakítása, amelyet az ITIL ajánlások, valamint a COBIT érettségi modell és kontrollrendszer támogatnak.

A bemutatott szabványok és ajánlások más-más területek működését támogatják. Kiegészítik egymást, de ugyanakkor átfedésben is vannak egymással, emiatt fontos a bevezetésük összehangolása.

A nemzetközi szabványügyi testület felismerve azt a tényt, hogy adott esetben a szervezeteknek több menedzsment szabványnak is meg kell felelniük, elkezdték egységesíteni a menedzsment szabványok struktúráját. Az ISO szabványügyi testület az ISO/IEC Directives, Part 1, Consolidated ISO Supplement 2015. évi 6. kiadásában megújította a menedzsment szabványok kidolgozásának irányelveit és javaslatot tett az egységes struktúrára, tartalomjegyzékre, közös terminológiára és a szervezeti kontextusra érvényes közös szövegezésre [68], hogy megkönnyítse azok integrált bevezetését.

Az információbiztonság megvalósítása szempontjából az 1-es ábrán látható összefüggéseket állapítottam meg a minőségirányítási (MSZ EN ISO 9001, AQAP), az IT szolgáltatásmenedzsment (MSZ ISO/IEC 20000, ITIL) és az információbiztonság menedzsment (MSZ ISO/IEC 27001, COBIT 5, Ibtv) rendszerek között [69].




*1. ábra Az információbiztonság, minőségmenedzsment és IT szolgáltatásmenedzsment összefüggései [69]*

## 2.2 Az információbiztonság állapota és fejlesztése

### 2.2.1 Az információbiztonság állapota

Az információbiztonság egy dinamikus állapot, függ a biztonságtudatosság aktuális állapotától, a szervezet által alkalmazott szabályzatok és eljárásrendek betarthatóságától és betartásától, a szervezet infrastruktúrájának adottságaitól és az alkalmazott információtechnológiai megoldások aktuális sérülékenységi állapotától. Ugyanakkor figyelembe kell venni azt a tényt, hogy az üzleti érdekek és jogszabályok változása miatt a szervezetek folyamatos változáson mennek át, amelynek következében változnak a szolgáltatásaik és ezzel együtt a támogató folyamatok és az infokommunikációs infrastruktúra is.

Mint látjuk, az információbiztonság sok tényezőtől függ. A változó infokommunikációs infrastruktúra, a fejlődő technológia, a napról napra megjelenő szoftver és hardver sérülékenységek, a mobil kommunikáció és okostelefonok használata, az Advanced Persistent Threat (APT) támadások és kibertámadások esetleges megjelenése, folyamatos kihívás elé állítja

a szervezeteket. Nem elegendő a biztonságtervezési folyamat rendszeres időközönkénti végrehajtása. Javasolt a szervezet változáskelési folyamatainak kiegészítése kockázatelemzéssel és szükség esetén védelmi intézkedések megvalósításával.

A szervezet által végrehajtott folyamatok érettségi szintje jól tükrözi a szervezet felépítésének és működésének fejlettségét, amely meghatározza a szervezet védekezőképességét is a biztonsági támadásokkal szemben. A COBIT érettségi modellje 5 szintbe sorolja a szervezet munkafolyamatainak fejlettségét:

0. szint – nem létező folyamat, azaz a szervezet fel sem ismerte annak szükségességét;
1. szint – kezdeti, ad-hoc, eseti folyamat;
2. szint – ösztönösen ismétlődő munkafolyamat;
3. szint – szabályozott munkafolyamat;
4. szint – irányított és mérhető munkafolyamat;
5. szint – optimalizált munkafolyamat.

A COBIT 5 szakmai segédletekkel támogatja az információbiztonság megvalósítását. A COBIT 5 for Information Security bevált gyakorlatokkal és módszerekkel támogatja az információbiztonság megvalósítását a napi üzemeltetés során [70]. A COBIT 5 for Risk –kockázatkezelés megvalósítását támogatja [71]. A COBIT 5 for Assurance az informatikai és belső ellenőrök számára nyújt részletes útmutatást [72].

### 2.2.2 Információbiztonság irányítási rendszerek megvalósítása

Az információbiztonság megvalósítása nem egy egyszeri feladat a szervezetek életében. A vonatkozó jogszabályok és szabványok, mind előírják az információbiztonság rendszeres felülvizsgálatát. Nagyobb szervezetek esetében jelentős informatikai infrastruktúra nyújtja az üzleti szolgáltatásokat támogató informatikai szolgáltatásokat. Az informatikai rendszerekben tárolt információ biztonságának megvalósítása jelentős mennyiségű műszaki, informatikai és adminisztratív jellegű feladatot ró a szervezetre. Az adminisztratív feladatok jellemzően a szabályozási háttér kialakítása, a humán erőforrás biztonságának felépítése, a biztonságtudatosság növelése témaköröket öleli fel. Ugyanakkor az informatikai szolgáltatások és az informatikai rendszerekben tárolt és feldolgozott adatok biztonságának megvalósítása fizikai és logikai védelmi intézkedéseket tesz szükségessé, amelyek végig követik az információs rendszerek teljes életciklusát. Az informatikai rendszerekben tárolt adatok védelmét fizikai és logikai védelmi módszerekkel lehet a legjobban megvalósítani, amelyek megakadályozzák az információ illetéktelenek általi hozzáférését, az adatok illetéktelen módosítását, az adatok

helyreállítását katasztrófa esetén, továbbá biztosítják az adatok rendelkezésre állását a megfelelő helyen és időben az illetékesek számára. Ez jellemzően informatikai beruházások árán valósulhat meg, amelynek mértéke függ a szervezet és a szervezet informatikai rendszereinek méretétől. Emiatt az információbiztonság megvalósulását nagymértékben befolyásolja az IT stratégia tervezése, amely szoros összefüggésben van az információbiztonsággal [73]. A technológia folyamatos fejlődése szükségessé teszi az információbiztonság folyamatos fejlesztését, amelynek fenntartása érdekében az IBIR kialakításának és felülvizsgálatoknak jól definiált munkafolyamatok mentén kell zajlaniuk [74]. Muha és Szádeczky arra hívja fel a figyelmet, hogy mindig rögzíteni kell az aktuális állapotot [75]. Ez teszi lehetővé az előrehaladás nyomon követését.

Shameli-Sendi és társai iteratív magvalósítást javasolnak az információbiztonság megvalósítására. Megerősítik, hogy az ISO/IEC 27001 szabvány a legjobb választás az információbiztonság megvalósítására. Az általuk javasolt ISO/IEC 27001 alapú keretrendszert a következő 8 tulajdonság köré építik fel [76]:

- monitoring – biztosítja a szerepkörök, felelősségek, eszközök, biztonsági politikák és a vezetőségi tanács folytonosságának megfigyelését;
- karbantartás és folytonosság – ami biztosítja, hogy az IBIR ne veszítse el stabilitását az évek során;
- jelentéskészítés – ami keretrendszert biztosít az egyszerű és folyamatos jelentéskészítéshez;
- ügyfélbizalom – mutatókat kell meghatározni, amelyek biztosítják, hogy a hatékony IBIR hozzájáruljon az ügyfelek bizalmának elnyeréséhez;
- kockázatelemzés – biztosítja, hogy a kockázatelemzési modellünk helyesen azonosítja és rangsorolja a magas kockázatokat;
- üzletmenet folytonosság – biztosítja, hogy az üzletmenet folytonossági terv megakadályozza az üzletmenet leállását és az alapvető üzleti folyamatok gyors visszaállítását;
- szerepkörök szétválasztása – biztosítja, hogy a létrehozott keretrendszerben a szerepkörök és felelősségek könnyen szétválaszthatók;
- konfiguráció és változáskezelés – biztosítja, hogy változásokat csak megfelelő kontrollok betartása mellett lehet végrehajtani.

A vizsgált ISO szabványok (EN ISO 90001, ISO/IEC 20000, ISO/IEC 27001) menedzsment rendszer létrehozását és működtetését írják elő, amelyek mellett jogszabályok és keretrendszerek követelményeit is figyelembe kell venni, amikor IBIR rendszert építünk egy szervezetben.

Az IBIR-t a szabvány a következőképpen definiálja: a menedzsment rendszer azon része, amely üzleti kockázat alapon létrehozza, implementálja, működteti, figyelemmel kíséri, karbantartja és folyamatosan fejleszti az információbiztonságot [24]. Ez a definíció jól kifejezi azt a tényt, hogy az IBIR azt a részét képezi a szervezet menedzsment rendszerének, amelynek segítségével képesek kialakítani és fenntartani az általuk kezelt információ biztonságát. Az információbiztonság megfelelő szintű megvalósítása konzisztens szabályozási rendszer és azzal összhangban kialakított fejlett információtechnológiai megoldások bevezetését igényli. Az IBIR kialakítása során figyelembe kell venni a szervezet gazdasági profiljának információbiztonsági szükségleteit. A szabvány és a jogszabályok által megkövetelt kockázatarányos védelem kialakítása nem mindig egyszerű feladat, hiszen előfordulhat, hogy a kockázatok besorolása okozza a legnagyobb problémát, amely információvédelmi hiányosságok kialakulásához vezethet. Az IBIR felépítése, konzisztenciája, kialakítása, illeszkedése a szervezet működéséhez nagymértékben befolyásolja az adatok és ezáltal az információ védelmének megvalósítását. Annak ellenére, hogy a szabványok, jogszabályok és keretrendszerek részletesen megfogalmazzák az általuk elvárt követelményeket, ezek megvalósítása függ az iparágtól, az alkalmazandó szabványoktól, keretrendszerektől és jogszabályoktól, valamint a szervezet méretétől és felépítésétől.

Calder: Nine Steps to Success: An ISO 27001 Implementation Overview alapján összefoglalhatók azon tevékenységek, amelyek megfelelő végrehajtása növeli az IBIR bevezetési projektek sikerét [77]. A szerző jól összegzi a sikerhez vezető út lépéseit, mint a bevezetések elengedhetetlen összetevőit, de nem tárgyalja a felépített IBIR minőségi paramétereit, amelyek biztosítják, az információ eredményes védelmét. Az IBIR bevezetések sikere nagyban függ attól, hogy a megvalósítást akadályozó tényezőket időben felismeri-e a projektvezető, illetve a projekt szponzor és megteszik-e a szükséges lépéseket ezek elhárítására. Ilyen sikert elősegítő és akadályozó tényezők:

**Kockázatok feltárása:** Kockázatcsökkentési lehetőség a kulcsemberekkel való interjúk, vagy fókuszcsoport keretében végzett problémafeltárás. Fontos, hogy nem csak a projekt kezdetén kell a kockázatokat kezelni, hanem a projekt végrehajtása során is.

**Érdekelt felek céljainak elemzése:** A projekt elején fel kell tárni a projektre hatással levő személyek elvárásait és azok prioritását.

**Felsővezetői támogatás:** Fel kell kelteni a felső vezetés figyelmét és a projekt során fenn is kell tartani. A lényeges kockázatok üzleti nyelven való bemutatása elősegíti a vezetők figyelmének

megszerzését. A figyelem fenntartását a változtatások megvalósulásának döntési pontjaihoz kapcsolódó vezetői tájékoztatók segítik.

**Szervezeti változtatás-menedzsment:** Egy IBIR projektre általában úgy tekintenek a szervezet munkatársai, hogy biztosan változást fog hozni, de nem tudják pontosan, hogy mit. Minden szervezetben vannak néhányan, akik értik, hogy miért szükséges az információbiztonság és támogatják a változást, ugyanakkor a többség passzívan szemléli vagy ellenáll, nem látja szükségesnek. Minden szervezetben van néhány olyan ember is, akik aktívan tesznek azért, hogy zátonyra futtassák a projektet.

**Tapasztalt projektvezető:** A tapasztalt IBIR projektvezető inkább menedzser, mint műszaki szakember. Ő az a személy, akihez bárki fordulhat a projekttel kapcsolatos kérdésekben.

**Belső kommunikáció:** Szervezeti változtatási projektekben kulcsfontosságú, hogy minél előbb adjunk tájékoztatást és gyakran informáljuk a munkatársakat a projekt előrehaladásáról. (pl. belső honlap, rendszeres belső hírlevél). Közérthető nyelven kell megfogalmazni, hogy miért fontos az információbiztonság és miért megfelelő módja a biztonság megteremtésének az IBIR bevezetése. Be kell mutatni, a szervezet jövőképét az IBIR bevezetése esetén és annak szervezetre gyakorolt pozitív hatását.

**Tudás megszerzése a szervezet számára:** A külső szakértők bevonását célszerű korlátozni, inkább az IBIR működését elősegítő tudást és képességeket kell beépíteni a szervezetbe. Ezt a tudást a bevezetési projekt során érdemes megszerezni, a projektben való aktív részvétellel. A projekt elején javasolt kijelölni az információbiztonsági felelőst, aki aktívan részt vesz az IBIR bevezetésében. A speciális biztonságtechnikai területeken célszerű külső szakértőket igénybe venni rugalmasan alkalmazható keretszerződés formájában.

**Minden érintett bevonása:** Minden érintett szervezeti egységet és kulcsszereplőt be kell vonni aktívan a projektbe, vegyenek részt a készülő anyagok (szabályzatok és eljárásrendek) elkészítésében és véleményezésében. Ez biztosítja, hogy minden lényeges szempontot időben figyelembe vesznek, és a szervezet munkatársai sajátjuknak érzik az elkészült rendszert. Ez megelőzi, hogy az egyébként ellenállást tanúsító munkatársak akadályozzák, vagy ellehetetlenítsék a projekt megvalósulását.

**Mérés, mutatószámok:** Azok a tevékenységek, amelyeket nem mérünk objektív mutatószámokkal nehezen irányíthatóak, ezért megvan a kockázata annak, hogy nem vesszük észre időben a

céloktól való eltérést. Törekedni kell arra, hogy a kulcskontrollok működésének mérhetősége megvalósuljon cél- és eredménymutatók alkalmazásával.

**Tesztelés:** A tesztelés kulcsfontosságú feladat. Elvégzése visszajelzést nyújt az előkészített változások által bevezetendő folyamatok működőképességéről. A tesztelés a folyamatok alapos ellenőrzése, amely minden részletre kiterjed. Addig kell tesztelni a folyamatokat, amíg azok minden elvárásnak megfelelően nem működnek.

Szádeczky felhívja a figyelmet arra, hogy a hazánkban érvényes szabályozási környezet heterogenitásának következtében nehéz egyértelműen meghatározni az információbiztonsági követelményeket. Ez rontja a szabályozás hatékonyságát és vele együtt nő a jogbizonytalanság. Ugyanakkor rámutatott arra, hogy a jogilag felületesen szabályozott területek megfeleltethetők a szakterületen alkalmazott valamely szabványnak, így összességében jól meghatározott informatikai biztonsági szabályrendszert alkotnak [28].

A szabályozási környezet heterogenitása nem csak a követelmények meghatározására van hatással. A szabványok, keretrendszerek és jogszabályok struktúrája is eltér egymástól. Ezt felismerve az információbiztonsági szakemberek megfeleltetéseket hoztak létre a szabályozási környezetekben megtalálható jogszabályok, szabványok és keretrendszerek között. Ez támpontot nyújt az IBIR bevezetésben dolgozó szakembereknek a célkörnyezetben alkalmazandó követelmények kiválasztásához.

Az IBIR-ben lefektetett biztonsági követelmények nagymértékben befolyásolják az információbiztonságra fordított kiadásokat. Ugyanakkor az információbiztonságra fordítható források végesek. Gordon és Loeb szerint a költség-haszon elemzés szilárd alapja az információbiztonsági kiadások tervezésének [78]. A kutatómunkám során bebizonyosodott, hogy ez jó kiindulópont lehet, de több olyan esettel is találkoztam, amikor jogszabályi előírások miatt nem volt mérlegelési lehetősége, hogy milyen megoldást választ a szervezet, így nem volt alkalmazható a költség-haszon elemzés.

A COBIT a szervezet működéséhez, üzleti és támogató munkafolyamataihoz és információbiztonsági stratégiájához illesztett információbiztonsági program létrehozását és végrehajtását javasolja. A program fontos elemei a szükséges erőforrások azonosítása és allokálása, az információbiztonsági architektúra megtervezése, az információbiztonsági szabályzatok és eljárásrendek kialakítása és karbantartása, az információbiztonsági előírásokból származó követelmények beépítése a szervezet munkafolyamataiba és a partnerekkel megkötött szerződésekbe. A program sikerességét a hatékonyságának és hatásosságának méréséhez köti.

### 2.2.3 Az információbiztonság fejlesztésének irányelvei

Az IBIR szerepe a szervezetek életében az általuk kezelt információ biztonságának megteremtése. A biztonsági követelmények a szabványok és jogszabályok esetében részletesen ki vannak fejtve, így azok alkalmazása biztosíthatja a szervezet által kezelt információ megfelelő szintű védelmét, miközben elég magas szintű ahhoz, hogy rugalmasan alkalmazható legyen tetszőleges méretű szervezet esetében. Ha a szervezetnek több jogszabály és szabvány követelményeinek kell megfelelnie, elengedhetetlen azok követelményeinek összefésülése. Ennek elősegítését szolgálják a szabványok és keretrendszerek összerendelési mátrixai. Jó példa erre a Horváthtal közösen bemutatott BMr követelmény, NIST-SP800-53 Rev 4 kontroll, ISO/IEC 27001:2013 kontroll összerendelés [79], az ITGI (IT Governance Institute) által kiadott COBIT 4.1 és ITIL v3 összerendelés [80], a Sheikhpour és Modiri által összeállított ITIL v3 – ISO/IEC 27001:2005 összerendelés [81] stb.

A jogszabályi követelmények mindig erősebbek a szabvány követelményeknél. Erre azért fontos kitérni, mert vannak szervezetek, amelyek a kötelező jogszabályi előírásokon túl célul tűzik ki az ISO 27001 szabvány szerinti tanúsítást is. Irodalomkutatásaim során megállapítottam, hogy IBIR bevezetéskor a szervezetre érvényes legerősebb jogszabály vagy szabvány követelményrendszerét kell alapul venni és ebbe integrálni a további releváns szabvány, jogszabály, és keretrendszer vonatkozó követelményhalmazát. A rendelkezésre álló szabványok, jogszabályok és keretrendszerek megfeleltetésének alkalmazása megkönnyíti az alkalmazandó követelmények összehangolását, ugyanis az elsődleges követelményrendszerből hiányzó követelményeket kell azonosítani és beépíteni a már kialakított követelményrendszerbe.

A szervezetre érvényes szabályozási környezet befolyásolhatja az IBIR kialakításának peremfeltételeit és részletekbe menően előírhatja a szervezet által kezelt adatok információbiztonsági osztályokba sorolásának szabályait, a megvalósítandó védelmi intézkedéseket és a biztonság fenntartásának eszközeit. Ilyen szabályozási környezet érvényes az állami és önkormányzati szervek esetében, ahol az Ibtv [33] és annak technológiai végrehajtási rendelete a BMr [34] határozza meg a követelményeket. A banki és biztosítási területek esetében, indirekt módon a vonatkozó jogszabályok követelményei szabályozzák az információbiztonságot.

Szádeczky részletesen tárgyalja az információbiztonsági jogszabályokat, szabványokat és keretrendszereket, amelyek alkalmazásával létrehozható a szervezet számára szükséges mértékű információvédelem. Művében részletesen bemutatja a COBIT és különböző szabványok és jogszabályok megfeleltetését, továbbá bemutat egy módszert az Infotv és COBIT

megfeleltetéséhez. Mivel a jogszabályok, szabványok és keretrendszerek hasonló struktúrával rendszereznek, azaz követelményekre és követelmény csoportokra bonthatók, a módszert általánosítva alkalmazható tetszőleges jogszabályok, szabványok és keretrendszerek megfeleltetésének elkészítéséhez [82].

Muha definiálja az informatikai biztonság – mint az információbiztonság része – szempontjából figyelembe veendő rendszerelemeket, amelyek a következők: személyek, az informatikai rendszer fizikai környezete és a kiszolgáló infrastruktúra, hardverek, szoftverek, hálózati kommunikációt biztosító eszközök, adathordozók és szabályozások [83], továbbá a rendszerelemek fizikai és logikai veszélyforrásaira hívja fel a figyelmet [84]. Muha és Tóth olyan pénzintézetekben alkalmazható kockázatelemzési módszert mutat be, amelyben a védelmi célok meghatározása kulcsfontosságú eleme a kockázatelemzés elvégzésének. A módszertan a védelmi célokat két területre osztja: értékek tulajdonlása és működőképesség, amelyek alapfenyegetettsége a sérülés és elvesztés. Megállapítják, hogy az értékeket (fizetőeszközök, értékpapírok, vagyontárgyak, információk, adatok, személyzet) rendszerelemek veszik körül, amelyekre közvetlenül hatnak a fenyegetések. A bemutatott módszer lényege, hogy a rendszerelemekre meg lehet határozni a fenyegetettséget, előfordulási gyakoriságot, kárértéket és elviselhető kockázati határt, így minden felmért rendszerkomponensre minősíthetők a kárértékek. [85]. Ez a módszertan nem csak a bankok és bankbiztonság esetében alkalmazható, hanem általánosítva minden szervezetre is.

Több kutatási projektemben igény volt az Ibtv, ISO/IEC 20001, ISO/IEC 20000 szabványok együttes bevezetésére, miközben ezeket ki kellett egészíteni a GDPR adatvédelmi előírásaival. A kérés logikus, hiszen a vonatkozó jogszabályokat be kell tartani, a szabvány szerinti tanúsítás versenyelőnyt biztosít miközben a szervezetnek fejlesztenie és üzemeltetnie kell az üzleti folyamatokat támogató informatikai szolgáltatásokat. Ha ezeket a követelményeket vesszük alapul, akkor adja magát, hogy az Ibtv vagy ISO/IEC 27001 struktúráját követve építsük fel az IBIR-t. A GDPR megfelelés jellemzően a személyes adatok biztonságára fókuszál, amelynek komponensei közül ez esetben a bizalmasság a legfontosabb tényező. Azon szervezetek esetében, amelyek személyes adatokat kezelnek egyértelmű, hogy a jogszabályi és szabvány követelményeket ki kell egészíteni azon GDPR követelményekkel, amelyek nem szerepelnek az IBIR alapjául választott követelményeknek. A GDPR teljesítéséhez szükséges biztonsági kontrollok kialakításához az ENISA (European Union Agency for Network and Information Security) gondozásában megjelent „Privacy and Data Protection by Design” [86] kiadványa nyújt segítséget.

Dey összefoglalja hogyan álljunk hozzá az IBIR ISO/IEC 27001 szerinti kialakításához, bemutatja a javasolt IBIR struktúrát és bevezetési módot. Az IBIR alapjául az ISO/IEC 27001 szabvány

követelményeinek struktúráját javasolja és felhívja a figyelmet arra, hogy be kell építeni a jogszabályi környezet követelményeit is [87]. Irodalomkutatásom több olyan publikációkat találtam, amelyek ugyanezt a logikát követték.

Sharkasi rávilágít arra, hogy a világviszonylatban megjelenő információbiztonsági jogszabályok a szabályozási követelményeknek való megfelelésre teszik a hangsúlyt és mellőzik a szervezetek információbiztonsági tanácsokkal való ellátását. A szerző 10 területet jelöl meg az információbiztonság fejlesztésére, amelyekkel ugyan lehet vitatkozni a fejlesztés nézőpontjából, de lefedi napjaink jellemző veszélyforrásainak kiküszöbölését: eszköz nyilvántartás és adatosztályozás, folyamatosan megjelenő technológiai kockázatok, a kockázatelemzés fejlesztésének és hangsúlyosságának növelése, az adattárolás és felhő alapú megoldások kockázatkezelése, a szervezeten belüli veszélyforrások kezelése, a végpontok biztonsága, fájlmegosztó alkalmazások, biztonság érettsége és távoli hozzáférés, elavult rendszerek biztonságának elérése, információbiztonság ellenőrzés és ellenőrző eszközök [88].

Az információbiztonság kialakítása során a szabványok, ajánlások és jogszabályok az adatok kockázatarányos védelmét írják elő. Ahhoz, hogy ez megvalósulhasson, össze kell gyűjteni a szervezet által kezelt adatokat és az adatkezelést érintő folyamatokat. Ugyanakkor figyelmet kell fordítani a szervezet méretére [77], elhelyezkedésére, üzleti stratégiájára, anyagi helyzetére és úgy kell megtervezni az információbiztonság irányítási rendszert, hogy az általa megkövetelt védelmi intézkedések megvalósíthatók legyenek a szervezet adottságainak keretében és megfelelő szintű védelmet biztosítsanak számára. Túlszabályozott információbiztonság esetén megvalósul a szabályozási szintű védelem, de a szabályzatok betarthatatlanná válnak, a munkavégzés ellehetetlenül, az érintettek nem tartják be az előírásokat. Alulszabályozott információbiztonság esetén az IBIR nem tartalmazza az adatok védelméhez szükséges szabályokat és előírásokat, így azok betartása nem biztosítja az információ kockázatarányos védelmét.

### 2.2.4 IT szolgáltatásmenedzsmentet támogató IBIR modell

Ahhoz, hogy a szervezetek belső IT szolgáltatói biztosítani tudják az Ibtv követelményeit és hosszabb távon optimális erőforrás felhasználással nyújthassanak magas szintű informatikai szolgáltatásokat, a biztonságos IT infrastruktúra (hardver, szoftver, környezet) kiépítése mellett meg kell feleljenek az ISO/IEC 27001 információbiztonsági és ISO/IEC 20000 ITIL alapú IT szolgáltatásmenedzsment szabványoknak is. Mivel az említett szabványok és az ITIL legjobb gyakorlat jelentős átfedésben vannak az Ibtv követelményeivel, olyan integrált IBIR bevezetésére van szükség, amely egyben és egységesen lefedi ezek összesített követelményeit. A hatékony

munkavégzés érdekében az információbiztonsági követelményeket be kell építeni a szervezet kockázatelemzési, kockázatkezelési továbbá ITIL alapokra helyezett IT fejlesztési, üzemeltetési és szolgáltatási munkafolyamataiba.

Az információbiztonsági szabályrendszer kidolgozása során figyelembe kell venni, hogy az állami és önkormányzati szervezetek számára az Ibtv megfelelés kötelező, tehát ez képezi a bevezetés alapját és a jogszabályi megfelelést. Ehhez kell hozzávenni azon ISO/IEC 27001 követelményeket, amelyek biztosítják a szabványmegfelelést. Az elkészített követelményrendszert be kell építeni az ITIL alapokra helyezett IT szolgáltatásmenedzsment folyamatokba. Ez biztosítja, hogy a biztonsági előírások betartása és végrehajtása automatikussá váljon. A 2-es táblázat átfogó (nem teljes mélységében és pontosságában) képet nyújt az ISO/IEC 27001 szabvány, a Ibtv követelmények és ITIL folyamatok átfedéseiről.

| **ISO/IEC 27001** | **Ibtv (BMr)** | **Érintett ITIL Folyamatok** |
|---|---|---|
| Az információbiztonság irányítási rendszer megvalósításához szükséges a szervezetek adatvagyonának felmérése, amely kitér az adatokat kezelő és tároló rendszerekre. | | |
| biztonsági szabályzat | Informatikai biztonsági keretrendszer kidolgozása, adminisztratív védelmi intézkedések: informatikai biztonsági szabályzat, kockázatelemzési szabályzat és eljárásrend, beszerzési eljárásrend | Információbiztonság menedzsment |
| javak és eszközök ellenőrzése és osztályozása | információs rendszerek biztonsági osztályba sorolása, kockázatelemzés | Konfigurációmenedzsment |
| biztonsági incidensek kezelése | adminisztratív védelmi intézkedések (biztonsági események kezelése) | Eseménykezelés, Incidenskezelés |
| biztonsági szervezet és személyi biztonság | adminisztratív védelmi intézkedések: emberi tényezőket figyelembe vevő személy biztonság | |
| fizikai és környezeti védelem | fizikai és környezeti biztonság | |
| kommunikáció és műveleti menedzsment | adminisztratív védelmi intézkedések (biztonságtudatosság és képzés) | Tudásmenedzsment |
| | logikai védelmi intézkedések: rendszer és információsértetlenség; naplózás és elszámoltathatóság; rendszer, kommunikáció és adathordozók védelme | Eseménykezelés, Incidenskezelés, Problémakezelés |
| rendszerfejlesztés és karbantartás | logikai védelmi intézkedések (általános védelmi intézkedések, tervezés, rendszer és szolgáltatás beszerzés, biztonsági elemzés, tesztelés képzés és felügyelet, adminisztratív védelmi intézkedések, karbantartás, rendszer és információsértetlenség) | Konfigurációmenedzsment, Változáskezelés, Kiadáskezelés, Kapacitáskezelés, Rendelkezésre állás menedzsment, Tesztelés, Kiértékelés, Tudásmenedzsment |
| hozzáférési jogosultság ellenőrzése | logikai védelmi intézkedések: azonosítás és hitelesítés, hozzáférés ellenőrzése | Hozzáférés menedzsment |
| az üzletmenetfolytonosság menedzsmentje | adminisztratív védelmi intézkedések: üzletmenet folytonosság tervezés | IT szolgáltatás folytonosság menedzsment |
| megfelelőség | megfelelőség | |

*2. táblázat ISO/IEC 27001, Ibtv és BMr átfedése az ITIL folyamatokkal (saját szerkesztés)*

Közelebbről megnézve a 2-es táblázatot jól látható, hogy a legtöbb biztonsági követelmény és intézkedéshez hozzákapcsolható egy-egy ITIL alapú munkafolyamat. Ezek integrációja az IBIR-be nagymértékben elősegíti az IT szolgáltatások biztonságos működését és az információbiztonsági követelmények megvalósulását.

## 2.3 Az információbiztonság hatása a munkafolyamatokra

A vállalatok megbízható működésre, az üzleti partnerek igényeinek időben, mennyiségben és minőségben történő kielégítésére törekednek. Feltérképezik vállalati folyamataikat, értékteremtéshez szükséges eszközeiket és ezek rendelkezésre állását. Csak az erőforrások (köztük a kiemelt szerepet kapó információ) biztosításával lehet az értékteremtő üzleti folyamatokat végrehajtani. A vállalat és folyamatainak biztonságmenedzsmentje olyan folyamatos tervezési, szervezési, irányítási és ellenőrzési tevékenységet jelent, amely a vállalat minden külső és belső érintettje számára elfogadható és fenntartható biztonsági szintet jelent.

A folyamat definiálására a Turner és társai általi meghatározást használom: „A folyamat egy vagy több tevékenység, amely értéket növel úgy, hogy egy bemenetkészletet átalakít a kimenetek készletévé (javakká vagy szolgáltatásokká) egy más személy (a vevő, ill. felhasználó) számára, emberek, módszerek és eszközök kombinációjával.” [89, p. 75]

Folyamatbiztonság olyan állapotnak tekinthető, ahol az előírt bemenetek (folyamat végrehajtásához szükséges erőforrások) biztosítása után a folyamat tevékenységeit végrehajtó szervezeti egységek az előírt időben megfelelő mennyiségű és minőségű kimenetet (termék, szolgáltatás, információ) nyújtanak és zavar esetén a folyamat normál működése a lehető legkisebb erőforrás ráfordítással és a legrövidebb idő alatt helyreállítható [90].

### 2.3.1 Üzletmenet folytonosság

Az üzletmenet folytonosság esetében a szervezet folyamatai zavartalanul és hibamentesen működnek és az azokhoz szükséges erőforrások megfelelő helyen és időben rendelkezésre állnak. A szervezetek elsősorban információbiztonsági vonatkozásban használják a fogalmat és az ún. „üzletmenet-folytonossági terv” információbiztonsági intézkedéseket tartalmaz. Célja a szervezeti folyamatokat támogató informatikai erőforrások meghatározott időben és funkcionális szinten történő rendelkezésre állásának biztosítása, valamint váratlan eseményekből bekövetkező károk minimalizálása. Számba veszi a folyamatok fenyegetettségeit, ezek bekövetkezési valószínűségét és a folyamat kieséséből eredő károkat. Megadja a lehetséges helyettesítő eljárásokat, amíg a helyreállított folyamat újra nem indul.

Minden folyamat végrehajtásához erőforrásokra van szükség, amelyek közül kiemelkedik a megfelelő helyen és időben, a jogosult személyek számára biztosított információ. A vállalati folyamatokat virtuálisan leképező információs rendszerek szabályozott működtetésével elérhetjük a folyamatok biztonságát. A szűken értelmezett információtechnológiai megközelítés azonban kiterjeszthető bármelyik más vállalati folyamat feltételeinek biztosítására, annak előírásszerű végrehajtására vagy zavar esetén normál működésének helyreállítására. A folyamatszemléletű üzletmenet-folytonosság nem csak információbiztonsági problémákra alkalmazható [91].

Godámnyi arra hívja fel a figyelmet, hogy az IT-központú katasztrófavédelemnek üzletmenet-folytonosság központúnak kell lennie [92]. Napjainkban a vállalatok üzletmenet-folytonosságát növekvő számú és egyre nehezebben átlátható veszély fenyegeti. Minden üzleti folyamatot (pénzügyi, működési, stratégiai és projekt-) és kapcsolódó erőforrást (ember, IT, berendezések, infrastruktúra, energia, üzleti partnerek) kockázatelemzésnek és -kezelésnek kell alávetni [93].

A klasszikus Porter féle értéklánc modell [94] alapján a folyamatok végrehajtását biztosító szervezeti erőforrásokat három lépésben vizsgálja:

- meghatározza, hogy a kimenetek létrehozásában milyen tevékenységek játszanak szerepet;
- elemzi, hogy ezek a tevékenységek hogyan járulnak hozzá a kibocsátás értéknöveléséhez;
- vizsgálja, hogy a szervezetek mennyit kötnek le erőforrásaikból és ezek milyen költséget jelentenek.

Itt a nyereségesség mellett előkerülnek biztonságos működést, illetve üzletmenet folytonosságot érintő kérdések is.

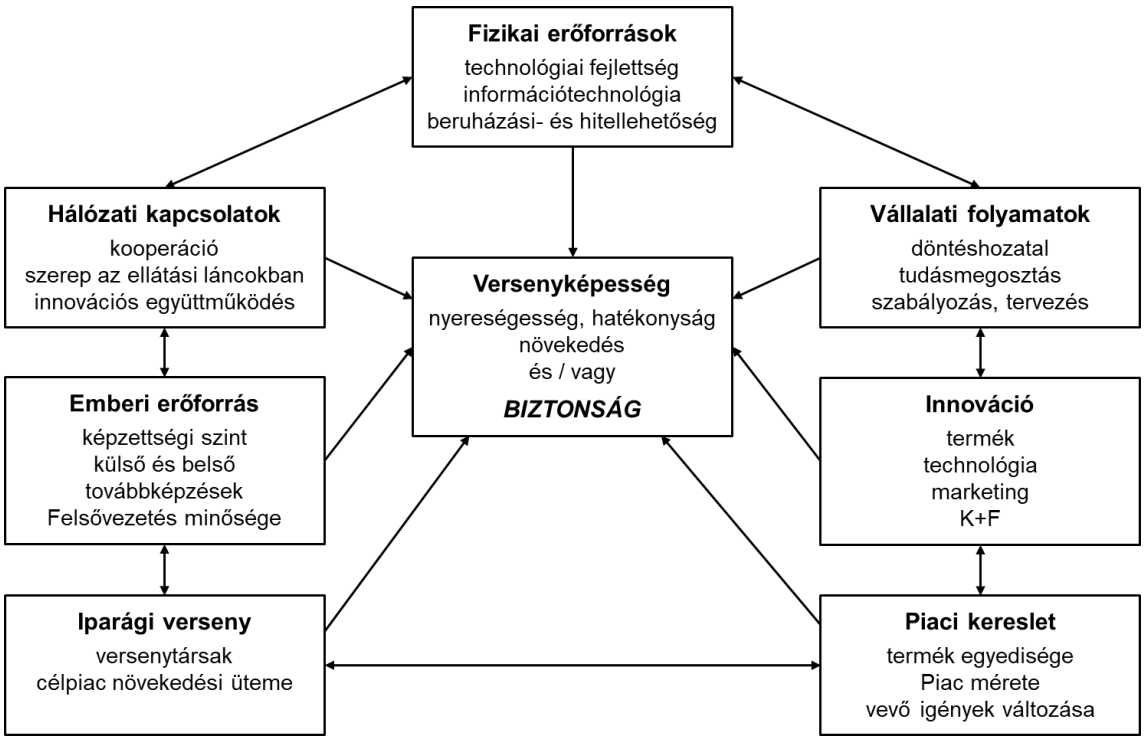
### 2.3.2 Versenyképesség és minőség

„Egy nemzetgazdaságban azokat a vállalatokat tekintjük versenyképesnek, amelyek társadalmilag elfogadható normák betartása mellett a számukra elérhető erőforrásokat minél nagyobb nyereségfolyammá képesek transzformálni, képesek a működésüket befolyásoló környezeti és vállalatukon belüli változások észlelésére és az ezekhez való alkalmazkodásra annak érdekében, hogy a nyereségfolyam lehetővé tegye tartós működőképességüket.” [95, p. 31]

A meghatározás a vállalati versenyképesség alapvető, de nem kizárólagos tényezőjének a nyereséges gazdálkodást tekinti. A tartós működőképesség feltételezi, hogy a vállalat törekszik a biztonságra, a fizikai és emberi erőforrások, a vállalati folyamatok, az innováció, a piaci kereslet és a vállalat közvetlen környezete szempontjaiból egyaránt. A vállalatok versenyképességét nagymértékben befolyásolja a folyamatok végrehajtásának időigénye és az előállított termékek,

szolgáltatások, információ minősége. Egyre fontosabb szerepet játszik a minőség és annak biztosításához szükséges minőségmenedzsment. A minőségi kimenet előállítása optimális ráfordítás mellett függ a vállalat munkafolyamatainak dokumentáltságától, szabályozottságától és automatizáltságától. Fontos szerepet játszik az egyes kimenetek előállítása során elvégzett feladatok dokumentálása [96]. Ez lehetővé teszi az előállított kimenetek életútjának nyomon követését, a hibásan elvégzett feladatok azonosítását, az összegyűjtött adatokból számított statisztikák alapján pedig a leggyakoribb hibák azonosítását, valamint a munkafolyamatok megújítását, optimalizálását. Korábbi tapasztalataim alapján kiemelt fontossággal bír a munkafolyamatok hatékony és hatásos végrehajtásában a folyamat számára valós időben rendelkezésre álló adat, amely nagy mértékben felgyorsíthatja, vagy meg is akadályozhatja az üzleti folyamatok végrehajtását, ami sok esetben az ügyfelek elvesztésével is járhat [97].

A vállalati folyamatok végrehajtása közben a folyamatlépések elvégzése során a munkatársaknak és partnereknek pontos adatokra van szükségük feladataik végrehajtásához. Ezek az adatok üzleti titkot képező információt hordozhatnak. Kezelésük, tárolásuk és továbbításuk kiemelt figyelmet igényelhet. Az adatok bizalmasságának megőrzése [89] befolyásolhatja a vállalat versenyképességét, kiszivárgása veszélyeztetheti a vállalat működését és fennmaradását. A versenyképesség és biztonság összefüggéseit a 2-es ábra mutatja be.




*2. ábra Versenyképességi modell [98]*

A folyamatok végrehajtásához szükséges adatok hiánya [99], hiányossága és pontatlansága az előállított kimenetek minőségének romlásához vezethet, amely megrengetheti a vevők bizalmát a vállalat termékeiben, illetve szolgáltatásaiban. A vállalat keretében működő minőségirányítási rendszernek biztosítania kell, az adatok rendelkezésre állását, sértetlenségét és nem utolsó sorban a bizalmasságát is, egyszóval támogatnia kell a folyamatok végrehajtásához szükséges információ biztonságát.

### 2.3.3 Versenyképesség és folyamat automatizálás

Felgyorsult világunkban nagy szerepet játszik a munkafolyamatok kimeneteinek előállítására fordított munkaidő és költség. A versenyképesség megőrzésének érdekében jó stratégiának tűnik a folyamatok által előállított kimenetekre fordított munkaidő és költség csökkentése a minőség javítása mellett. Az emberi erőforrás a legdrágább, így jó alternatíva a vállalati folyamatok automatizálása.

A folyamatok automatizálásával lehetővé válik a munkafolyamatok feladatainak pontos ismétlése, nő a termelékenység, javul és stabilizálódik a minőség, valamint nő a folyamatbiztonság. Ugyanakkor a termelési, üzleti és ügyviteli folyamatok automatizálásához automatizálási infrastruktúrára van szükség. Ezt az infrastruktúrát informatikai rendszerek vezérlik, amelyek megfelelő beállítása és programozása kiemelt figyelmet és ellenőrzést igényel az üzemeltetők részéről. Fontos szerepet játszik a feladatok végrehajtásához szükséges információ, megfelelő helyre megfelelő időben való eljuttatása. A hiányos, sérült vagy hibás adatok felhasználása hibás termékek és szolgáltatások előállításához, adott esetben akár a folyamat leállásához is vezethet, amely jelentős kárt okozhat a vállalatnak.

A beállításokon és programozáson túl, fontos szerepet játszik az automatizálást lehetővé tevő infrastruktúra és a vezérlő rendszerek minősége [100]. A megoldás-szállítók törekednek a megfelelő minőségű hardver és szoftver elemekből álló automatizálási infrastruktúra előállítására, de a folyamatos versenyhelyzet, a termékek mielőbbi piacra juttatására sarkallja őket. Ez adott esetekben a regressziós tesztelések elmaradásához, ez által a kész automatizálási termékek részleges teszteléséhez vezethet. A technológia gyors fejlődése, a hiányos, vagy tévesen összeállított tesztforgatókönyvek segítségével ellenőrzött automatizálási infrastruktúrák, a tesztelések teljeskörűségének hiánya, új veszélyforrások megjelenéséhez vezet. Előfordulhatnak olyan infrastruktúra vagy vezérlési hiányosságok és hibák, amelyek hibás kimenet előállításához, adott esetben személyi sérüléshez vezethetnek. Ezek kivédésére a megoldás-szállítók folyamatosan fejlesztik és tesztelik az előállított infrastruktúrát, szükség esetén szoftveres

javítócsomagokat állítanak össze és küldenek vásárlóiknak a már megvásárolt és üzembe helyezett infrastruktúra karbantartásához.

A számítógép vezérelte, programozható automatizált infrastruktúrák lehetőséget nyújtanak különböző kimenetek váltakozó előállítására. A különböző kimenetek különböző munkafolyamatok végrehajtását igénylik. A különböző munkafolyamatok implementálása az automatizálási infrastruktúrában feltételezi a munkafolyamatok részletes ismeretét, amelyet:

- működő folyamatok esetében a munkavégzés során elvégzett feladatok elemzésével és leírásával;
- új folyamatok esetében, a folyamat részletekbe menő megtervezésével és dokumentálásával lehet elérni.

A folyamatok végrehajtása előtt fontos szerepet játszik a munkafolyamat teszt jellegű végrehajtása és az előállított kimenetek ellenőrzése. A megfelelően tesztelt, automatizált infrastruktúra és infrastruktúra implementálás hozzájárul a magas minőségű kimenetek optimális időben való előállításához.

### 2.3.4 Folyamat-végrehajtás és biztonság

A feladatok végrehajtásához elengedhetetlen a tevékenységek elvégzéséhez szükséges útmutatók és erőforrások rendelkezésre állása. Fontossá válik a folyamatlépések dokumentációjának eljuttatása a feladatot végrehajtó illetékes munkatársakhoz, amely megfelelő részletességgel tartalmazza szükséges erőforrások listáját és a tevékenységek végrehajtásának módját [101].

A folyamatok zökkenőmentes végrehajtásához időben biztosítani kell, a megfelelő mennyiségű és minőségű erőforrást a kijelölt munkahelyeken [102]. Az erőforrások logisztikája kulcsszerepet játszik a folyamatos működés megvalósításában, amelyhez megbízható információra és logisztikai rendszerre van szükség. Az erőforrások egy része sok esetben információ, amely csak a feldolgozó személyek számára megismerhető.

A folyamatok végrehajtásának és az információ feldolgozásának érdekében a vállalatok folyamatokat támogató eljárásrendeket és szabályzatokat alkotnak. A szabályzatoknak a feldolgozandó információ bizalmassági besorolásának megfelelő módon kell kezelniük az információ védelmét. Ha a folyamat végrehajtása során adatfeldolgozás történik, a folyamat végrehajtását szabályozó eljárásrendeknek részletesen ki kell térniük az információbiztonság megvalósítására. Kritikus adatok feldolgozása esetén minden folyamatlépés leírásnak tartalmaznia

kell az információt feldolgozó személyek adatokkal kapcsolatos jogosultságait [103]. Ez esetben szerepkör alapú jogosultsági rendszer kialakítására van szükség, amelyben az egyes adatokhoz való hozzáférés lehet teljes körű vagy részleges. Az írási és olvasási jogosultságoknak el kell különülniük egymástól (bizonyos attribútumok csak olvashatók és bizonyos attribútumok írhatók). Például, ha személyes adatok tárolása és feldolgozása történik a folyamat végrehajtása során, az adatok védelmét jogszabályok határozzák meg, ez esetben a szabályzatoknak részletesen tárgyalniuk kell a jogszabály által előírt adatvédelmi céloknak megfelelő feldolgozási rendet.

Az alkalmazott folyamatautomatizálást támogató infrastruktúráknak biztosítaniuk kell az információbiztonsági követelményeknek megfelelő jogosultsági rendszer kiépítését. A felhasználóknak a szükségesnél bővebb jogosultságot lehetővé tevő folyamat automatizálási infrastruktúrák nagyobb teret engednek a platformfüggetlen úgynevezett social-engineering támadásoknak.

A folyamatok végrehajtása során a kimenetek előállításával egy időben a minőségirányítási rendszer további, a kimenet előállításhoz kapcsolódó adatokat gyűjt, amelyek feldolgozásával javítható a kimenetek minősége és optimalizálható a folyamatok végrehajtása. Fontos szempont, hogy a folyamatok dokumentációi, a folyamat végrehajtás során keletkezett minőségügyi információk bizalmasak, belső használatúak, ha konkurenciához kerülnek, az versenyelőnyre tehet szert annak felhasználásával.

A folyamat szemléletű információbiztonság kialakítása azt célozza meg, hogy megvalósuljon az információ védelme a folyamatok végrehajtása során. Ennek érdekében a részletes folyamat felmérés, tervezés és dokumentálás során összegyűjti az feldolgozott adatokra vonatkozó biztonsági követelményeket. A folyamatlépések végrehajtását és a végrehajtói szerepköröket úgy alakítja ki, hogy az megfelelő szintű információbiztonságot eredményezzen. A folyamat végrehajtást támogató rendszerek implementálása során követelményeket támaszt az információbiztonsági architektúra tervezésével kapcsolatban és a rendszer elkészítését követően teszteli annak biztonsági követelményeit. Kész automatizálási rendszer vásárlása esetén az információbiztonság megvalósítását a beszerzendő rendszerrel szemben megfogalmazott biztonsági követelmények formájában támogatja.

A legújabb európai uniós trendek nagy hangsúlyt fektetnek az információbiztonságra. Korábbi kutatásaink és fejlesztési projekt auditjaink azt igazolták vissza, hogy az informatikai rendszerekben megjelenő információbiztonsági hiányosságok a biztonsági tervezés hiányára vagy hiányosságaira vezethetők vissza. Az ENISA gondozásában megjelent „Privacy and Data

Protection by Design” tervezési modelleket mutat be [86], amelyek elősegítik az adatok és személyes információk védelmét az informatikai rendszerekben. A tanulmány kitér az adatvédelmi tervezési stratégiára, és technológiai szinteken rendelkezésre álló biztonsági technológiákra és technikákra [104].

Mint azt láthatjuk az információ bizalmasságának, sértetlenségének és rendelkezésre állásának hiányában a szervezetek által működtetett munkafolyamatok biztonságos végrehajtása megkérdőjelezhető, függetlenül attól, hogy melyik iparágban végzik a tevékenységüket.

## 2.4 Az IBIR bevezetésének módjai

A 2.3 és 1.3 fejezetekben láthattuk, hogy a folyamatok végrehajtásnak biztonsága szempontjából elengedhetetlen az, hogy a megfelelő információ, megfelelő időben és helyen elérhető legyen a munkafolyamat számára. Az automatizálás és az okos rendszerek bevezetésével a hiteles információ rendelkezésre állása sokkal nagyobb mértében befolyásolja a munkafolyamatok végrehajtását, mint a manuális folyamatvégrehajtás során. Honfi és Illési arra hívja fel a figyelmet, hogy az automatizált rendszerek nem megfelelő használata, a bevezetett megoldások biztonságának nem megfelelő minősége azonnali károkozással jár [105]. Az EU tanulmánya szerint az információbiztonság megvalósulása egyenesen kritikus az Ipar 4.0 esetében [61].

### 2.4.1 Az IBIR hagyományos bevezetése

Az információbiztonság irányítás ISO/IEC 27001 / ISO 27002 alapú kialakításának hagyományos megvalósítása során elemezni kell: a szervezet kialakítását, a szervezet szabályzatrendszerét, a szervezet által kezelt adatokat, a szervezet által végrehajtott üzleti folyamatokat, a szervezet által végrehajtott támogató folyamatokat, a szervezet informatikai és infokommunikációs infrastruktúráját a jogszabályoknak és szabványoknak való megfelelés szempontjából. A szervezet méretétől, a kezelt adatoktól és az informatikai infrastruktúrától függően ez más-más feladatot jelent. Az elemzés során figyelembe kell venni a szabvány és/vagy jogszabályok által előírt kontrollokat, azonosítani kell a hiányosságokat és tervet kell készíteni azok megszüntetésére.

Az információbiztonság tervezési feladat elvégzésének ciklikus folyamata:

- **helyzetfelmérés** – ennek keretében megtörténik, a szervezet adatvagyonának felmérése, az üzleti és ügyviteli folyamatainak azonosítása, a szervezet és támogató informatikai infrastruktúra (rendszerek, hálózat, környezet) felmérése;
- **veszélyforrás elemzés** – a szervezet adataira, folyamataira, infrastruktúra elemeire releváns veszélyforrások azonosítása;

- **javaslat azonnali intézkedésekre** – ha a veszélyforrás elemzés gyorsan, minimális erőforrás bevonásával elhárítható veszélyforrásokat tár fel, javaslat készítése védelmi intézkedések azonnali végrehajtására;
- **kockázatelemzés** – az azonosított veszélyforrások érvényre jutásának elemzése, az érvényre jutásuk esetén okozott gazdasági és presztízs károk, valamint törvényi következmények azonosítása, kockázatainak meghatározása;
- **döntés védelmi intézkedésekről** – a kockázatelemzés alapján alternatív javaslatok készítése az azonosított kockázatok elhárítására, csökkentésére és döntés a megvalósítandó védelmi intézkedések megvalósításáról;
- **védelmi intézkedések megvalósítása** - információbiztonság megerősítő program elindítása.

Az egyes szabványok és jogszabályok, mint például BMr jelentős mennyiségű szabályzat, eljárásrend és terv elkészítését írják elő követelményként. Kis szervezetek esetében sokkal értelmesebb összevonni ezeket, és a szervezet struktúrájához igazítani, hiszen a szervezet méretéből adódóan a kevés dolgozó és kevés szervezeti egység hajtja végre a munkafolyamatokat. A szabályzatok, eljárásrendek és tervek elkészítése jelentős terhet ró a szervezetekre, mivel a jogszabályok és szabványok csak követelményeket fogalmaznak meg, de nem tesznek konkrét javaslatokat, ajánlásokat ezek elkészítéséhez. A szabályzatok és eljárásrendek elkészítése során figyelembe kell venni a szervezet méretét és adottságait, hogy a megtervezett információbiztonság irányítási rendszer védelmi intézkedéseiben megfogalmazott technikai, technológiai követelmények feltételei teljesülhessenek és beleférjenek a szervezet költségvetésébe.

A bevezetés során fontos szerepet játszik az oktatás. A biztonság tervezése során az általános biztonságtudatosságon túl, be kell vonni az érintetteket a védelmi intézkedések kialakításába és oktatást kell biztosítani számukra, hogy az elvárásoknak megfelelő információbiztonsági megoldások születhessenek.

### 2.4.2 Az IBIR integrált bevezetése

Az ITIL mint az IT szolgáltatásmenedzsment legjobb gyakorlata lefedi az informatikai rendszerek menedzsmentjének teljes életciklusát a szolgáltatás stratégiától elindulva a tervezésen, beszerzésen, fejlesztésen, bevezetésen, folyamatos fejlesztésen át a selejtezésig. Ajánlásai részlegesen ugyan, de figyelembe veszik az információbiztonság és minőségirányítás követelményeit.

Az EN ISO 9001 alapú teljes körű minőségirányítási rendszert működtető szervezetek esetében, a minőségirányítási rendszer kiterjed a szervezet munkafolyamataira, ez által biztosítja, hogy az üzleti, ügyviteli és működéstámogató folyamatok teljes körű és megfelelő minőségű információval dolgozzanak, így kielégítik az információbiztonság sértetlenségre vonatkozó követelményeit.

A BMr és ISO/IEC 27001 szabvány által előírt szabályzatok, eljárásrendek és tervek többségének követelményei jól működő – minőség- és informatikai szolgáltatás-menedzsment irányítási rendszerrel rendelkező – szervezetek esetében elérhetők az üzleti, ügyviteli és működést támogató folyamatokba integrálva és azok dokumentációi rendelkezésre állnak. A még hiányzó követelmények listája úgynevezett gap elemzéssel meghatározhatók, ezt követően ki kell dolgozni és integrálni azokat a meglévő irányítási rendszerbe.

Egy újonnan bevezetendő integrált minőségirányítási, informatikai szolgáltatásmenedzsment és információbiztonság irányítási rendszer esetében, figyelembe véve, hogy a nemzetközi szabványügyi testület egységesítette a szabványok szerkezetét, első körben a közös irányítási keretrendszert kell kialakítani, majd feltölteni az egyes szakterületekre vonatkozó tartalommal.

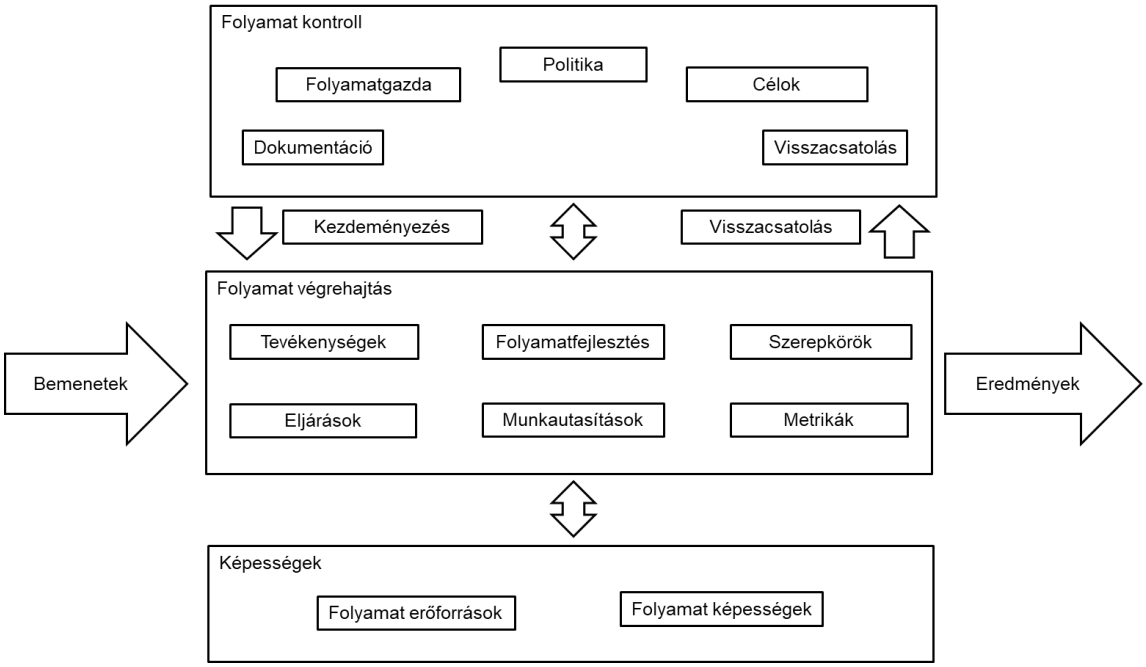
Mint azt korábban láthattuk az egyes szakterületek részlegesen átfedik egymást, így össze kell hasonlítani és hangolni a követelményeket, hogy kiszűrésre kerüljenek az átfedések. Erre a célra léteznek megfeleltetési táblázatok, amelyek segítik a beépítendő követelmények kiválasztását és integrálását. A szabványok szerinti bevezetési sorrendet befolyásolhatják a helyi jogszabályok és piaci trendek. Ugyanakkor érdemes figyelembe venni, hogy az információbiztonság ráépül minőségbiztosítási és informatikai szolgáltatásmenedzsment folyamatokra.

### 2.4.3 Az IBIR folyamatszemléletű bevezetési módja

Mivel manapság az üzleti, ügyviteli és támogató folyamatok elképzelhetetlenek információ tárolása, feldolgozása és továbbítása nélkül. Minden dolgozó feladatához hozzátartozik az általa kezelt információ védelme, ez biztosítja a szervezetek által végrehajtott folyamatok biztonságát.

Ennek analógiájára létrehoztam a folyamatszemléletű információbiztonság bevezetési módot, amelynek alapjául az integrált IBIR bevezetési módot választottam. A modell tartalmazza az MSZ EN ISO 9001 szabvány szerinti minőségirányítási és ITIL alapú IT szolgáltatásmenedzsment munkafolyamatokat. Ezek adják az információbiztonsági, miniségirányítási és IT szolgáltatásmenedzsment követelmények vázát, amelyhez hozzácsatoltam a vonatkozó információbiztonsági és szakterületi jogszabályok követelményeit. Ez a követelményrendszer biztosítja a jogszabályi és szabvány megfelelőséget.

A folyamatszemléletű IBIR bevezetés második alapkövét az ITIL folyamatmodellje alapján leírt jól definiált folyamatok képezik. Az ITIL folyamatmodelljét a 3. ábra mutatja be.




*3. ábra Folyamatmodell ITIL alapján [50]*

A folyamatmodellhez hozzátartozik a folyamat dokumentálása, a folyamatkontroll, amelyet a folyamatgazda gyakorol és amely biztosítja a folyamat mindenkori célokhoz való igazítását, optimalizálását a végrehajtóktól érkező visszajelzések alapján, a folyamat végrehajtásához szükséges képességek és erőforrások biztosítását [50]. A jól definiált folyamat dokumentációja folyamatábrából és táblázatos leírásból áll. A folyamatlépések folyamatábrán szereplő azonosítója biztosítja összekapcsolásukat a táblázatos leírással, ahol szerepelnek az érintett szabályzatok, informatikai rendszerek, bemenetek, folyamatlépések részletes leírása, végrehajtásban érintett adatok biztonsági besorolással, szerepkörök (felelős, számonkérhető, közreműködő és informált), eredmények és végül a kapcsolódó folyamatok.

A bevezetés során végrehajtandó feladatok:

1. A szervezet által végrehajtott folyamatok felmérése és kockázatelemzésen alapuló rangsorolása kritikusság szerint.
2. Munkafolyamatok részletes elemzése, az egyes folyamatlépésekben érintett adatok azonosítása, biztonsági osztályba sorolása, szerepkörök hozzáférési szintjének meghatározása.
3. MSZ ISO/IEC 27001 szabvány vagy Ibtv alapú informatikai biztonsági szabályzat elkészítése, felhasználói informatikai biztonsági útmutató elkészítése, információbiztonság ellenőrzési

eljárások kialakítása, kommunikáció és határvédelmi eljárások és megoldások kialakítása, fizikai védelmi eljárások kialakítása, biztonságtudatossági oktatási program megvalósítása, személybiztonsági eljárásrend megvalósítása.

4. Szervezeti szintű változáskezelés kialakítása, amely gondoskodik az érintett folyamatok információbiztonsági felülvizsgálatáról is.
5. A folyamatok végrehajtását támogató informatikai rendszerek és infrastruktúra felkészítése az érintett adatok védelmére.
6. A folyamatok végrehajtásában résztvevő adatgazdák, alkalmazásgazdák, rendszergazdák, munkatársak és folyamatfelelősök oktatása és felkészítése az általuk használt információs rendszerek biztonságos használatára és információ védelmére.
7. MSZ ISO/IEC 20000 vagy ITIL alapú informatikai szolgáltatásmenedzsment folyamatok szükség szerinti bevezetése az MSZ ISO/IEC 27001 szabvány és/vagy BMr követelményeinek integrálásával, amely gondoskodik az események (információbiztonsági is) naplózásáról, naplóbejegyzések és incidensek kezeléséről, a problémák megoldásáról, hozzáférés menedzsmentről, az informatikai változások kezeléséről, az alkalmazás- és hardververziók kiadásáról, a konfigurációk nyilvántartásáról és kezeléséről, a folyamatokat támogató informatikai rendszerek és infrastruktúra rendelkezésre állásról, a beszerzések, fejlesztések, rendszer monitoring és felügyelet, IT szolgáltatás folytonosság megvalósításáról megfelelő biztonsági tervezés mellett.

Az elvégzendő feladatok listájából látható, hogy egy bevezetett MSZ ISO 9001 alapú minőségirányítási, illetve ITIL alapú IT szolgáltatásmenedzsment rendszer nagymértékben támogatja az információbiztonság irányítási rendszer folyamatszemléletű bevezetését. Az információbiztonság folyamatszemléletű kialakítása hasonlóan működik minden üzleti, ügyviteli és támogató folyamat esetében. Az adatgazdáknak, folyamatgazdáknak és a folyamat végrehajtóinak részt kell venniük a folyamat kialakításában és/vagy információbiztonsági átalakításában. A munka elvégzéséhez elengedhetetlen egy-egy profi folyamatmenedzsment és információbiztonsági tanácsadó részvétele a munkában. Az adat- és alkalmazásgazdák folyamatmenedzsment ismeretekkel való ellátása, oktatása kritikus pontja az IBIR bevezetésének.

### 2.4.4 Bevezetési módok összehasonlítása

Az információbiztonság irányítási rendszerek bevezetését több módon is elvégezhetjük: hagyományosan ISO/IEC 27001 és vonatkozó jogszabályok alapján önállóan, más szabványokkal integrált módon (ISO/IEC 20000, EN/ISO 9001 stb.) és folyamatszemléletű, amikor a biztonsági követelményeket beépítjük a munkafolyamatokba is [69].

A 3-as táblázatban összehasonlítottam a 2.4.1-2.4.3 bevezetési módok előnyeit és hátrányait.

| Megközelítés | Előnyök | Hátrányok |
|---|---|---|
| Hagyományos megközelítés | • A bevezetés alapjául választott szabvány vagy jogszabály által támasztott követelmények egyszerűen azonosíthatók.<br>• Egyszerűen ellenőrizhető a tervezett védelmi intézkedések megvalósulása a gyakorlatban.<br>• Alacsonyabb kezdeti költség. | • Az irányítási rendszerben megfogalmazott kritériumok elszakadnak a gyakorlatban megvalósított védelmi intézkedésektől.<br>• Túl szigorú védelmi intézkedések beépítésének kockázata a szabályzatokba és eljárásrendekbe, amelyek:<br>o betarthatatlanok;<br>o akadályozzák a munkavégzést;<br>o jelentős többletköltséget generálnak;<br>o nem valósíthatók meg a gyakorlatban.<br>• A szabályzatok és eljárásrendek kialakításában nem feltétlenül vesznek részt az érintettek, nem érzik magukénak és elszabotálják azok végrehajtását.<br>• Előfordulhat, hogy a bevezetés nem tér ki részleteiben az üzleti/ügyviteli folyamatok sajátosságaira.<br>• A szabvány és a jogszabály nem nyújtanak gyakorlati útmutatást a védelmi intézkedések megvalósításához.<br>• Előfordulhat, hogy a kialakított védelmi intézkedések nem biztosítják a szükséges védelmi szintet. |
| Integrált megközelítés | • Az ITIL gyakorlati útmutatói segítséget nyújtanak az irányítási rendszer védelmi intézkedéseinek kialakításában.<br>• Egyszerűen ellenőrizhető a tervezett védelmi intézkedések megvalósulása a gyakorlatban.<br>• A minőségbiztosítási irányítási rendszer szerint kialakított védelmi intézkedések megfelelnek az elvárásoknak. | • A bevezetés alapjául választott szabványok, ajánlások és jogszabályok követelményei közül kiválasztandók az adott környezetben alkalmazandó követelmények.<br>• A nem megfelelően kialakított informatikai szolgáltatásmenedzsment folyamatok akadályozzák a munkavégzést.<br>• Az irányítási rendszerben megfogalmazott kritériumok elszakadnak a gyakorlatban megvalósított védelmi intézkedésektől.<br>• Túl szigorú védelmi intézkedések beépítésének kockázata a szabályzatokba és eljárásrendekbe, amelyek:<br>o betarthatatlanok;<br>o akadályozzák a munkavégzést;<br>o jelentős többletköltséget generálnak;<br>o nem valósíthatók meg a gyakorlatban.<br>• Előfordulhat, hogy a bevezetés nem tér ki részleteiben az üzleti/ügyviteli folyamatok sajátosságaira.<br>• Magasabb kezdeti költség. |
| Folyamat-szemléletű megközelítés | • A működési folyamatok részletes elemzésével magasabb szintű információbiztonság érhető el.<br>• Kis szervezetek és kevés folyamat esetében jól alkalmazható.<br>• A bevezetési költség függ az üzleti és ügyviteli folyamatok számától. | • Nagyszámú üzleti/ügyviteli folyamat esetén, jobban támaszkodik a folyamatgazdákra és a folyamat résztvevőire ezáltal a bevezetés ellehetetlenülhet.<br>• Az ITIL alapú támogató folyamatok kialakítása elengedhetetlen a sikeres bevezetés érdekében. |

*3. táblázat IBIR bevezetési módok összehasonlítása [69]*

## 2.5 Összegzés

Megvizsgálva az információbiztonságot és adatvédelmet előíró legfontosabb jogszabályokat, szabványokat és keretrendszereket, megállapítottam, hogy az információbiztonságra vonatkozó követelményeik részleges átfedésben vannak egymással. Fontos következtetés, hogy a minőségirányítási rendszer az információ sértetlenségét, az IT szolgáltatásmenedzsment rendszer pedig az információ rendelkezésre állását biztosítja [69].

Elemeztem az információbiztonság hatását a szervezetek munkafolyamataira nézve. A vállalati folyamatok típusától függetlenül (ügyfélkiszolgálás, működéstámogatás) kiemelt szerepet játszik az információbiztonság. A termelési folyamatok esetében az információ rendelkezésre állásának hiánya gyártósori leállást, így termeléskiesést okozhat, amely jelentős anyagi kárral társulhat. Az információ bizalmasságának megőrzése főleg a személyes adatokat kezelő szervezetek esetében kritikus, amelyet jogszabály ír elő, de a belső információk konkurenciához való eljutása versenyhátrányhoz is vezethet. A hibás vagy sérült adatok hibás termékelőállítást, de adott esetben személyi sérülést is okozhatnak. Összességében elmondható, hogy az információbiztonság alapvető követelményként jelenik meg a vállalati folyamatok végrehajtásának biztonságát illetően és ezáltal befolyásolja a vállalat versenyképességét is [104]. Megállapítottam, hogy az információbiztonság követelményeinek beépítése a munkafolyamatokba amellett, hogy javítja a szervezetek információbiztonságát elősegíti a munkafolyamatok zavartalan és biztonságos végrehajtását is. Ennek alapján létrehoztam, az információbiztonság folyamatszemléletű bevezetési módját, amelynek alapja az IBIR minőség- és IT szolgáltatásmenedzsmenttel integrált bevezetése kiegészítve a szervezet munkafolyamataiba épített biztonsági követelményekkel. Az IBIR minőség- és IT szolgáltatásmenedzsmenttel integrált bevezetése biztosítja az elvárt és szükséges biztonsági szintet. A folyamatokba épített biztonsági követelmények pedig biztosítják a szervezet munkafolyamatainak zavartalan és biztonságos működését [69].

**A kutatási tevékenységem alapján igazoltnak tekintem a H4. hipotézist mely szerint létezik olyan IBIR bevezetési mód, amelynek alkalmazásával megvalósítható a munkafolyamatok zavartalan végrehajtása a szükséges biztonsági szint elérése mellett.**

# 3 INFORMÁCIÓBIZTONSÁGI HIÁNYOSSÁGOK ELŐFORDULÁSA

Annak ellenére, hogy egyre több szabvány és jogszabály támogatja a szervezetek információbiztonságának megtervezését és egyre pontosabb leírást adnak a védelmi intézkedések kialakításához, egyre több információbiztonsági incidensről lehet hallani, amelyek több tíz, száz, ezer vagy akár milliós nagyságrendű felhasználót érintenek és hatalmas károkat okoznak az érintett szervezeteknek, partnereiknek és ügyfeleiknek. Ez arra engedett következtetni, hogy a szervezetek által bevezetett IBIR hiányos.

Az IBIR hiányosságok feltárását 12 kutatási projekt keretében végeztem el összesen 9 szervezet esetében, a szervezetek az államigazgatás, szolgáltatás, gyártás és pénzügyi szakterületen tevékenykedtek. A projektek három nagy kategóriába sorolhatók: információbiztonság szabályozás kialakítása és megújítása (a továbbiakban IBSZK), új vagy megújítandó informatikai rendszerek információbiztonsági követelményeinek meghatározása és specifikálása (a továbbiakban IBKS), információbiztonsági követelmények meglétének és megfelelőségének ellenőrzése informatikai rendszer követelményspecifikációjában (a továbbiakban IBKE). Az IBSZK projektek esetében az aktuális állapot felmérése felölelte a teljes szabályozási térképet, továbbá a szabályzatok végrehajtásának környezetét. Az IBKS és IBKE projektek során az érintett rendszerek működési környezetét, a vonatkozó információbiztonsági szabályzatokat és a rendszerre vonatkozó jogszabályi hátteret vizsgáltam. Mint a projektek résztvevője adta magát az akciókutatás módszertana, amelynek keretein belül interjú és esettanulmányok készítése, valamint a tudásrendezés módszertanainak segítségével azonosítottam az IBIR hiányosságokat. Ezt követően az esettanulmányokat elemezve a megalapozott elmélet módszertanát alkalmazva kidolgoztam a saját IBIR modellemet, amelyet projektről-projektre finomítottam. Mivel az esettanulmányok bizalmas információt is tartalmaznak, titkosak maradtak, de azok eredményét anonim módon felhasználhattam. A kutatási projektekben elméleti kutatásaimra [41] és a korábban elvégzett projektek eredményeire támaszkodtam.

Az IBIR szabályozás kialakítási és megújítási projektekben vizsgáltam a szervezet meglévő szabályzatait, azok a szervezet működéséhez való illeszkedését, a betartandó szabványok és jogszabályok tükrében. Ezt követően esettanulmányt készítettem, amelyben részletesen összegyűjtöttem a szervezet jogszabályi megfelelőségének követelményeit, megjelölve a szervezet megfelelési állapotát a felmérés időpontjában, továbbá a megfelelés eléréséhez elvégzendő feladatokat.

Az IBKS és IBKE projektekben a meglévő vagy tervezett informatikai rendszerek információbiztonsági követelményrendszerének megállapításához, illetve ellenőrzéséhez áttekintettem és elemeztem a IBIR kialakítását és a célrendszer jogszabályi hátterét. Ezekhez kellett igazítani, illetve ellenőrizni az informatikai rendszer biztonsági követelményeit. Amennyiben a szervezet az Ibtv hatálya alá tartozott, a feladat kiegészült rendszerbiztonsági terv elkészítésével, de volt olyan eset is, amikor az IBIR is megújításra szorult.

Kutatási projektjeimet a 4-es táblázatban foglaltam össze. Mivel az adatok szenzitívek, ezért a táblázat kódoltan tartalmazza a szervezetek neveit, ahol a kutatási projektek során információt gyűjtöttem. A táblázat feltünteti a szervezet méretét, a projekt típusát, az információbiztonsággal kapcsolatos fontosabb követelményeket és az IBIR megfelelőségét a projektindítás időpontjában. A táblázat oszlopainak fejlécei Szervezet: a szervezet kódolt neve; Méret: a szervezet mérete: kicsi: 1-100 fő, közepes:101-500 fő, nagy: 501 fő felett; Projekt: a projekt típusa; Ibtv, ISO 27001, GDPR: mezők mutatják az adott jogszabály, illetve szabvány szerinti működést; ITIL: elvárt az ITIL alapú IT szolgáltatásmenedzsment integrálása; IBIR: a szervezet rendelkezik-e IBIR-rel. Az utolsó oszlop a meglévő IBIR elvárásoknak való megfelelését mutatja.

| Szervezet | Méret | Projekt | Ibtv | ISO 27001 | GDPR | ITIL | IBIR | Megfelelő? |
|---|---|---|---|---|---|---|---|---|
| Sz1 | közepes | IBSZK | Igen | Nem | Igen | Igen | Van | Nem |
| Sz2 | közepes | IBSZK | Igen | Igen | Igen | Igen | Van | ISO 27001 |
| Sz3 | közepes | IBSZK | Igen | Nem | Igen | Igen | Nincs | Nem |
| Sz4 | kicsi | IBSZK | Igen | Nem | Nem | Igen | Van | Igen |
| Sz5 | nagy | IBSZK | Igen | Nem | Igen | Igen | Van | Nem |
| Sz6 | nagy | IBSZK | Nem | Igen | Igen | Igen | Van | Igen |
| Sz7 | nagy | IBSZK | Nem | Felkészülés | Igen | Nem | Van | Nem |
| Sz8 | kicsi | IBKS | Igen | Nem | Nem | N/A | Nincs | Nem |
| Sz9 | közepes | IBKE | Igen | Nem | Nem | N/A | Van | Nem |
| Sz4 | kicsi | IBKS | Igen | Nem | Nem | N/A | Van | Nem |
| Sz7 | nagy | IBKE | Nem | Felkészülés | Igen | N/A | Van | Nem |
| Sz3 | közepes | IBKE | Igen | Nem | Igen | Igen | Nincs | Nem |

*4. táblázat Információbiztonsági projektek (saját szerkesztés)*

A táblázat jól mutatja, hogy amennyiben rendelkezésre is állt IBIR, az csak 1 szervezet esetében felelt meg teljes mértékben az elvárásoknak a projekt elkezdésének pillanatában. A projektek megvalósítása során az IBIR rendszer elemzését és vizsgálatát top down megközelítéssel, részletekbe menően csak a projekt megvalósításához szükséges mértékben vizsgáltam. Az általam elvégzett vizsgálatok kiterjedtek az IBIR struktúrájára, a szabályzatok tartalmi összetevőire, a végrehajtási környezetre, teljességére, végrehajthatóságára, végrehajtásának minőségére és a végrehajtás által eredményezett információbiztonság színvonalára. Teljesség alatt azt értem, hogy

a szabályzatok kielégítik a vonatkozó jogszabályi környezet vagy a szervezet által teljesíteni kívánt szabvány követelményeit. Végrehajthatóságon azt értem, hogy a célközönség elolvasva a szabályzatot érti, tudja azonosítani és végre tudja hajtani a szabályzat betartásához szükséges feladatokat, továbbá az IBIR nem akadályozza a szervezet üzleti tevékenységét. A végrehajtás minősége alatt pedig azt, hogy az érintett személyek milyen mértékben tarják be az IBIR előírásait. A vizsgálatok eredményeként kapott információbiztonság színvonalát a követelményekhez képest feltárt hiányosságok határozzák meg.

Mint az látható 3 szervezet esetében fordult elő, hogy az információbiztonság szabályozási és információs rendszerek biztonsági követelményeivel is foglalkoztam. Ebből egy esetben új szervezetről lévén szó még nem álltak rendelkezésre szabályzatok, így a rendszerkövetelmények összeállítása során a jogszabályi hátteret kellett vizsgálni, az elkészült anyagot pedig felhasználtam az IBIR elkészítéséhez. A prioritásokat a szervezet határozta meg, mert a rendszer fejlesztésének rövid határidőn belül kellett elindulnia. Egy esetben az IBKS projekt követelmények írták elő az IBIR megújítását, a másik esetben pedig az IBIR szabályozási projekt vonta maga után a fejlesztés alatt álló rendszerek információbiztonsági követelményeinek átvizsgálását.

Összességében 9 szervezet információbiztonságát vizsgáltam meg, amelyből 7 esetben teljes körű elemzést végeztem, majd a szabályzatokat a helyi információbiztonságért felelős vezetővel és az érintettek bevonásával megújítottuk, hogy megfeleljenek a hatályos jogszabályi előírásoknak és választott szabványnak.

A 7 szervezetből 6 szervezetnek volt szüksége IT szolgáltatásmenedzsment bevezetésre, amelyből 3 szervezetnek már volt valamilyen szinten kiépített fejlesztési és üzemeltetési szabályzatrendszere. 2 szervezet esetében nem álltak rendelkezésre IT szolgáltatásokat érintő szabályzatok (fiatal szervezetekről van szó, ahol még nem alakultak ki az írott szabályok). Egy szervezet esetében pedig csak magas szintű fejlesztési szabályzat állt rendelkezésre, mert az IT szolgáltatások üzemeltetését teljes mértékben kiszervezték. A 9-ből 2 esetében, az adminisztratív terhek csökkentése érdekében fontos szempont volt az IT szolgáltatásmenedzsment integráció. Az IBIR kialakítását követő évben mindkét szervezetnél független auditor vizsgálta a szervezet Ibtv és ISO/IEC 27001 megfelelőségét és a kiépített rendszer működését. A kialakított rendszerek mindkét esetben jelesre vizsgáztak, megjegyezték, hogy az IT szolgáltatásmenedzsment folyamatok integrációja jelentős mértékben javítja az IBIR eredményességét.

Öt projekt esetében csak a bevezetendő információs rendszerekre vonatkozó információbiztonsági követelmények meghatározásához az IBIR-t és annak követelményeit csak a szükséges

mértékben vizsgáltam. Az öt esetből háromban volt elérhető IBIR, két esetben fiatal szervezetről beszélünk, ahol zöldmezős beruházás keretében megvalósuló informatikai rendszer követelményeit kellett meghatározni, mindkét projekt esetében párhuzamosan zajlott az IBIR kialakítása a szervezetben.

## 3.1 IBIR-rel kapcsolatos problémák azonosítása

Az IBIR szabályozási projektek egy kivétellel minden esetben valamilyen jogszabályi, illetve szabvány megfelelőségi probléma megoldását célozták meg. Az IBIR felmérését minden esetben a szervezetre vonatkozó legszigorúbb követelményeket támasztó szabvány/jogszabály mentén végeztem el, amelyet kiegészítettem további követelményekkel a 4-as táblázatban megfogalmazott projektelvárásoknak megfelelően. A felmérést az információbiztonsági vezető által megküldött IBIR dokumentációval kezdtem. A dokumentáció átnézését követően a vele folyatott interjú keretében azonosítottuk a megküldött szabályzatok erősségeit és gyengeségeit. Egy projekt kivételével az információbiztonsági vezetővel közösen egyeztettük a szabályzatok jogszabályi megfelelőségének megvalósításához szükséges további felmérések listáját, amelyek szakterületi vezetőkkel és IT rendszerek kulcsfelhasználóival folytatott interjúk és rendszerdokumentáció vizsgálatok formájában jelentkeztek. Az IBSZK projektek során két szervezetben az ISO/IEC 27001, 4 szervezetben pedig a BMr struktúráját követve történt az IBIR felmérése. Az 7 esetből 1 szervezet már rendelkezett ISO/IEC 27001 tanúsítvánnyal, de IBIR-jét ki kellett egészíteni a BMr szerinti hiányzó követelményekkel.

### 3.1.1 Az Ibtv és BMr hatálya alá tartozó szervezetek IBIR elemzése

A 5-ös táblázat a BMr struktúrájának megfelelő bontásban mutatja be a 7 szervezet IBIR-jének vizsgálati eredményét az elvárások tükrében. Az egyes cellákban szereplő értékek mutatják, hogy a szervezet maradéktalanul, egyáltalán nem vagy részben teljesíti a felsorolt követelményeket.

Az elemzés BMr fejezetenként összesített formában mutatja be a vizsgált szervezetek IBIR jogszabályi megfelelőségét az elemzés pillanatában. Mivel a BMr az intézkedések megvalósulását is vizsgálja sokkal árnyaltabb képet kapunk. Az Ibtv előírja az állami és önkormányzati szervek számára az elektronikus információbiztonság megvalósítását. A jogszabály végrehajtási rendelete a BMr sok tekintetben átfedésben van az ISO/IEC 27001 szabvánnyal, ugyanakkor vannak olyan eltérések, amelyek miatt a jogszabályi feltételek nem teljesülnek automatikusan a szabvány alapján bevezetett IBIR esetén. A 5-ös táblázatból egyértelműen kiolvasható, hogy az **Sz3** és **Sz8** szervezetek esetében fiatal szervezetekről lévén szó, még nincsenek szabályzataik. Ezekben az esetekben a jogszabály mentén kellett felépíteni az IBIR-t.

| T | Témakör | Sz1 | Sz2 | Sz3 | Sz4 | Sz5 | Sz8 | Sz9 |
|---|---|---|---|---|---|---|---|---|
| A | Szervezeti szintű alapfeladatok | Részben | Részben | Nem | Részben | Részben | Nem | Részben |
| A | Kockázatelemzés | Részben | Részben | Nem | Részben | Részben | Nem | Igen |
| A | Rendszer és szolgáltatás beszerzés | Részben | Igen | Nem | Igen | Igen | Nem | Igen |
| A | Üzletmenet- (ügymenet-) folytonosság tervezése | Részben | Részben | Nem | Részben | Igen | Nem | Igen |
| A | A biztonsági események kezelése | Részben | Igen | Nem | Igen | Igen | Nem | Igen |
| A | Emberi tényezőket figyelembe vevő - személy - biztonság | Részben | Igen | Nem | Részben | Igen | Nem | Igen |
| A | Tudatosság és képzés | Részben | Igen | Nem | Részben | Igen | Nem | Igen |
| F | Fizikai védelmi intézkedések | Igen | Igen | Nem | Igen | Igen | Nem | Részben |
| L | Általános védelmi intézkedések | Részben | Részben | Nem | Részben | Részben | Nem | Részben |
| L | Tervezés | Részben | Igen | Nem | Részben | Részben | Nem | Nem |
| L | Rendszer és szolgáltatás beszerzés | Részben | Igen | Nem | Igen | Igen | Nem | Igen |
| L | Biztonsági elemzés | Nem | Igen | Nem | Nem | Részben | Nem | Nem |
| L | Tesztelés, képzés és felügyelet | Nem | Igen | Nem | Igen | Igen | Nem | Nem |
| L | Konfigurációkezelés | Alapszintű | Igen | Nem | Alapszintű | Részben | Nem | Nem |
| L | Karbantartás | Igen | Igen | Nem | Igen | Igen | Nem | Nem |
| L | Adathordozók védelme | Igen | Igen | Nem | Igen | Igen | Nem | Nem |
| L | Azonosítás és hitelesítés | Részben | Igen | Nem | Igen | Igen | Nem | Részben |
| L | Hozzáférés ellenőrzése | Részben | Igen | Nem | Részben | Igen | Nem | Részben |
| L | Rendszer- és információsértetlenség | Részben | Részben | Nem | Részben | Részben | Nem | Részben |
| L | Naplózás és elszámoltathatóság | Részben | Részben | Nem | Részben | Nem | Nem | Nem |
| L | Rendszer- és kommunikációvédelem | Részben | Részben | Nem | Részben | Részben | Nem | Részben |

*5. táblázat Ibtv alá tartozó vizsgált szervezetek BMr szerinti elemzése (saját szerkesztés)*

Az **Sz1** szervezet rendelkezett ugyan egy átfogó IBIR-rel, amely az ISO/IEC 27001 szabványra épült, továbbá az IT ITIL alapon működő munkafolyamatok mentén végezte üzemeltetési folyamatait. Az IBIR szabályzatok csak részben feleltek meg a BMr előírásainak. Az IBIR megújítására a szervezeti átalakulások és a szervezet Ibtv alá sorolása miatt volt szükség. Annak ellenére, hogy a szervezet jól működő információbiztonsági szabályozási háttérrel rendelkezett a változások szükségessé tették az IBIR megújítását. Az információbiztonsági vezető szerint, aki információbiztonsági képesítéssel rendelkezett és évtizedes információbiztonsági és ellenőri tapasztalata is volt, azért kellett megújítani az IBIR-t, hogy követelményei beépüljenek a szervezet mindennapi munkafolyamataiba, ezáltal támogassák és ne akadályozzák a mindennapi feladatok elvégzését. Első körben a meglévő IBIR kiterjesztését ezt követően pedig az IT szolgáltatások nyújtásának ITIL alapokra helyezését tűzte ki célul a csatlakozó intézmények számára. Megjegyezte, hogy az átalakulások miatt ki kell alakítani egy általánosabb jellegű IBSZ-t és ez alá

kell létrehozni az operatív szabályzatokat, amelyek gyakorlatilag az IT szolgáltatások üzemeltetésére és biztonságára vonatkozó eljárásrendek. Hangsúlyozta, hogy az eljárásrendek a különböző informatikai rendszerek esetében eltérhetnek a kiadott egységes eljárásrendtől, ez esetben rendszer szintű eljárásokat kell létrehozni. Az eljárásrendek végrehajtása során igazoló dokumentumok keletkeznek, amelyeket a szervezet rendszerenként és eljárásrendenként tárol. Fontos szempontként határozta meg, hogy a végrehajthatóság és ellenőrizhetőség alapkövetelmény és nem jöhetnek létre olyan szabályzatok és eljárásrendek, amelyek betartása ellehetetleníti vagy akadályozza a szervezet feladatainak ellátását. Ezt úgy képzelte el, hogy a szabályzati szint (IBIR legfelső szintjén), meghatározza a szervezetben érvényes általános követelményeket, amelyeket az IBIR kialakítása során be kell építeni a következő szinten lévő eljárásrendekbe. Ezt követően a szervezetnek össze kell vetnie a munkafolyamatait az IBIR rendszerrel és hozzá kell igazítania. Ez utóbbi egy hosszabb folyamat, amelynek során előfordulhat, hogy az IBIR módosítására is szükség lesz, a szabályzatok és eljárásrendek közötti ellentmondások felszámolása érdekében. Ahhoz, hogy a szabályzatok alkalmazhatók legyenek, nem tartalmazhatnak olyan szakkifejezéseket, amelyek nem értelmezhetők a célközönség által. További kérése volt, hogy a szabályzatok rövid, pontos és lényegre törő szövegezéssel készüljenek és ne tartalmazzanak átfedéseket. Ha mégis előfordulnának átfedések, akkor azt hivatkozással kell feloldani, hogy a szabályzatok karbantartása során ne léphessen fel inkonzisztencia.

Az **Sz2** esetében a szervezet ISO/IEC 27001 szabvány szerinti IBIR-t üzemeltetett és ennek megfelelő tanúsítvánnyal is rendelkezett. Mint az látható az összefoglaló táblázatban is, a szervezet felkészült, jól megírt szabályzatrendszerrel rendelkezett, az általa tárolt és feldolgozott információ védelmének érdekében. Az IBIR megújításának egyetlen célja az Ibtv megfelelés volt, mivel a szabvány nem fedi le teljes mértékben az Ibtv követelményeit. Az IBIR BMr szerinti átvilágítását követően az információbiztonsági és informatikai vezetőkkel folytatott interjúk során megerősítették, hogy annak ellenére, hogy jónak tartják a szabályozási rendszert, több olyan változtatásra van szükség, amelyek elősegítik annak betartását és betartatását. Az egyik ilyen pont az IBSZ hossza és relevanciája a teljes dolgozói állományra. Több olyan pontot is megneveztek, amelyek részletes ismerete csak bizonyos munkacsoportok számára hordoz releváns információt. Ilyen fejezetek a kockázatelemzési eljárásrend részletes leírása, az információbiztonsági incidenskezelési munkafolyamat, a működésfolytonossági terv részletezése. Amellett, hogy ezek a részletes leírások növelik a szabályzat hosszát, csak részben tartalmaznak hasznos információt

a teljes dolgozói kör számára, ezen munkafolyamatok minden dolgozó általi részletes ismerete kockázatot is jelent, hiszen illetéktelenek jutnak hozzá az IBIR bizalmas részeihez.

Nehézséget okoz, hogy a munkafolyamatok végrehajtása mellett a dolgozóknak figyelniük kell a biztonsági szabályok betartására, amelyek időnként ütköztek egymással. Ilyenkor a dolgozók a munkautasítás végrehajtása során figyelmen kívül hagyják a munkavégzést ellehetetlenítő biztonsági szabályokat. Ugyanakkor az újonnan tervezett vagy átalakított munkafolyamatok esetében már figyelembe vették és beépítették az IBIR előírásokat. Ez megkönnyíti a biztonsági szabályok betartását, hiszen azok lefordításra kerültek a dolgozók által ismert munkafolyamatok nyelvezetére, nem tartalmaznak a dolgozók által ismeretlen informatikai és információbiztonsági szakkifejezéseket, továbbá a munkautasítások részévé vált, azaz megkerülhetetlen a munkavégzés során.

Fontos szempontként jelölték meg az információbiztonsági követelmények beépítését az informatikai fejlesztési és üzemeltetési munkafolyamatokba. Megjegyezték, hogy jelenleg az informatikai és információbiztonsági kockázatelemzés párhuzamosan zajlik a szervezet általános kockázatelemzési tevékenységeivel, az információbiztonsági, biztonsági és IT incidenskezelési munkafolyamatok jelentős átfedéssel működnek. Az említett munkafolyamatok megújításával és ITIL alapokra helyezésével, valamint a biztonsági követelmények beépítésével csökkenthető az adminisztráció, megszűnnek a párhuzamos tevékenységek és hatékonyabbá válik a munkavégzés.

**Sz3** szervezet esetében még nem állt rendelkezésre IBIR. A szervezet IT igazgatója töltötte be az információbiztonsági vezető szerepkörét. Az IT igazgató tisztában volt azzal, hogy ez a szituáció nem felel meg a jogszabálynak és a vonatkozó szabványoknak sem. Mivel jelentős tapasztalattal rendelkezett információbiztonság tekintetében, tudatosan építette fel az informatikai stratégiát, már az infrastruktúra és a fejlesztés alatt álló rendszerek üzleti funkcióinak tervezése során beépíttette az információbiztonsági követelményeket a specifikációba. Fontos szempontként jelölte meg, és ragaszkodott hozzá, hogy a kialakított IBIR harmonikusan működjön együtt az IT üzemeltetési folyamatokkal és kikötötte, hogy a jogszabályi követelményeket be kell építeni a szervezet munkafolyamataiba is, nem csak az IT által végzett feladatok elvégzésébe.

Az **Sz4** szervezet esetében az ISO/IEC 27001 alapon elkészített IBIR Ibtv megfeleléshez való átalakítást kellett elvégezni. Mivel a szabvány nem áll távol a BMr-től, első látásra egyszerű feladatról volt szó. A szabályzat elemzését követően kiderült, hogy túlsúlyban van a fizikai biztonság, a logikai biztonsági részek pedig csak nagyvonalakban határozzák meg az

információvédelmi követelményeket. Az IBSZ, amelynek betartása minden munkatárs számára kötelező, olyan szenzitív adatokat tartalmaz, amelyek nem tartoznak minden munkatársra. Az informatikai fejlesztési és üzemeltetési szabályzatok támogatják az IT működését, de nincsenek összekötve a biztonsági előírásokkal, így nincs garancia a biztonsági intézkedések betartására. Tovább bonyolítja a helyzetet, hogy kis szervezetről beszélünk, ezért az egyes szerepkörök kiosztása során előfordulhatnak ütközések. Ilyen ütköző szerepkör az információbiztonsági felelős, amelyet az IT igazgató tölt be. Ennek egyik oka, hogy az IT igazgató rendelkezett megfelelő információbiztonsági tapasztalattal és jártas volt az IT szolgáltatásmenedzsment területén is. Megfogalmazása szerint a bevezetett IBIR a szervezet több működési területén okozott fennakadást, emellett redundánssá tette az IT és biztonsági események és incidensek kezelését, valamint a kockázatelemzési és kockázatkezelési folyamatokat.

Mint jó vezetőnek, az volt a kérése, hogy az új IBIR épüljön be a szervezet munkafolyamataiba és szüntesse meg a párhuzamosságokat, azaz integrálja az információbiztonságot az IT és üzleti munkafolyamatokba. Az érintett munkafolyamatok: kockázatkezelés, eseménykezelés, incidenskezelés, változáskezelés.

Az **Sz5** szervezet esetében a projekt célja az információbiztonság megerősítése, hogy megfeleljen az Ibtv elvárásainak. Fontos megjegyezni, hogy a szervezet informatikai biztonsági felelőse rendelkezett információbiztonsági képesítéssel. A projekt kezdetén felsorolta az IBIR-rel szembeni elvárásait, amelynek többségét a BMr előírásai tették ki. Nagyon fontos kijelentésként fogalmazta meg, hogy az új IBIR-nek végrehajthatónak kell lennie. Ez alatt azt értette, hogy minden szabályzatnak valamilyen formában munkafolyamatokhoz kell kapcsolódnia és minden követelmény/szabály egyértelműen vonatkozik valamilyen szerepkörre, amely hozzá van rendelve a szervezet dolgozóihoz. Érdekes volt az a körülmény, amely a munkámat övezte. Nem nagyon volt arra lehetőség, hogy az érintett szerepköröket betöltő munkatársakkal konzultáljak, ami megkönnyítette volna a feladatok elvégzését. A munkafolyamatok és a szervezet szabályzatai elérhetők voltak, ezek alapján lehetett összeállítani egy első verziót. Ennek átadását követően egy új szakmai vezető érkezett a projekt élére, aki frappánsan és pragmatikusan fogalmazta meg az elvárásokat: az új IBIR-t úgy kell kialakítani, hogy teljes mértékben integrálódjon az ITIL alapján kialakított IT szolgáltatási folyamatokba. Az informatikai biztonsági felelőstől kapott IBSZ kb. 300 oldal volt. Mint kiderült a szabályzat részletesen taglalta azokat a tématerületeket, amelyek az IT beszerzésre, üzemeltetésre, működésfolytonosságra, fizikai védelemre, az információbiztonsági incidensek kezelésére, a humán erőforrás védelmére vonatkoznak. Emellett tele volt elavult általános módszertani leírásokkal az informatikai fejlesztésre és üzemeltetésre vonatkozóan,

amelyek újabb verziói már megjelentek. Az informatikai biztonsági felelős elmondta, hogy az IBSZ-t darabokra kellene szedni, hogy mindenkinek csak a saját szerepkörére vonatkozó részt kelljen ismerni. Ez biztonsági kérdéseket is felvet, mint például miért kell egy takarítónak ismerni az IT szervezetre vonatkozó részletes biztonsági előírásokat. Az IBSZ szétbontása szerepkörökre vonatkozó szabályzatokra nagy munka, hiszen azzal jár, hogy az összes érintett területet fel kell mérni, a munkafolyamatokat pedig konszolidálni, de arra egyelőre nem állt rendelkezésre megfelelő mennyiségű erőforrás. Az IBIR része a szervezet szabályzatrendszerének, a szabályzatok hivatkoznak egymásra, a frissítésük rendje meghatározott. A szabályzat hivatkozik az érintett és hatályos jogszabályokra, továbbá kitér a hazai és nemzetközi szabványokra és legjobb gyakorlatokra, amelyeket használtak a kidolgozás során. Ezek közül a legfontosabbak az ISO/IEC 27001, ITIL, COBIT és a Common Criteria. Az IBIR egy részletesen kidolgozott – sok felesleges és szenzitív információt tartalmazó - IBSZ-ből, Adatvédelmi, Hozzáférés kezelési, Működésfolytonossági és Katasztrófa elhárítási szabályzatból áll. A belső ellenőrzési osztály vezetője szerint komoly kihívást jelent az ellenőrzése, mert azok fejezetei nem hivatkoznak a jogszabályok megfelelő pontjaira. Amikor rátérünk az információbiztonsági események kezelésére, kiderült, hogy a szervezet rendelkezik naplóelemző szoftverrel, amit évek óta nem üzemeltek be.

Az **Sz8** esetében annyira új szervezetről beszélünk, hogy a szervezeti struktúra is kialakítás alatt állt. Ez lehetővé tette az információbiztonsági szervezetének, a szerepkörök és funkciók jogszabályi követelményeknek megfelelő, szükséges és elégséges mértékű kialakítását. Mivel ez esetben csak egy informatikai rendszer bevezetéséhez szükséges információbiztonsági követelményhalmaz összeállítását kellett elvégeznem, a kialakítás alatt álló IBIR-rel, csak a rendszer és a számára kialakítandó infrastruktúra mértékéig foglalkoztam. Összevetve a BMr-rel, javaslatot tettem az IBIR kezdemény vonatkozó részeinek kiegészítésére. A projekt végrehajtása során a szervezet információbiztonsági felelőse az IT vezető volt. Ő nem rendelkezett információbiztonsági képzettséggel, de korábbi IBIR bevezetési projektek tapasztalatai alapján konkrét elképzelésekkel segítette az IBIR kialakítását. Fontos szempontként jelölte meg az IBIR integrációját a szervezet munkafolyamataiba, megkövetelte, hogy az informatikai biztonság igazodjon az IT stratégiához, amelyek segítségével hatékonnyá tudta tenni a szervezet működését, és ki tudta küszöbölni az információbiztonsági szabályok ütközését a végrehajtandó munkafolyamatokkal. Egy évvel a projekt befejezését követően hívott a megrendelő és örömmel újságolta el, hogy hatósági információbiztonsági ellenőrzést végeztek a szervezetben. Az auditor visszajelzései alapján ők az egyik olyan szervezet, amelynél a felhasználók ismerik és betartják a szabályokat, az elvégzett feladatok eredményét a folyamatok végrehajtása közben megfelelő

módon dokumentálják, és nem találtak ellentmondást a szabályzatok és munkafolyamatok előírásai között, miközben megfelelnek a jogszabályi előírásoknak. Emellett megdicsérte az integrált incidenskezelési és kockázatkezelési szabályzatokat és eljárásrendeket.

Az **Sz9** esetében egy rendszer információbiztonsági követelményrendszerének vizsgálatát kellett elvégeznem. A szervezet kinevezett információbiztonsági vezetője sem képesítéssel, sem tapasztalattal nem rendelkezett az információbiztonság terén. A feladat első látásra egyszerű volt: a szervezet számára korábbi projekt során elkészült IBIR-hez kellett igazítani a rendszer már megírt információbiztonsági követelményeit. Az IBIR vonatkozó részeinek áttekintése során kiderült, hogy az Ibtv megfeleléshez készült. Tartalmazza a szervezet információbiztonsági felépítését, az információs rendszerek bizalmasság, sértetlenség és rendelkezésre állás szerinti besorolását, a kiszervezett informatikai üzemeltetés és külső partnerek felelősségeit és további magas szintű jogszabály által előírt követelményeket. Sok esetben szó szerint idézi a jogszabályt és emelt be abból szövegrészeket mint követelményeket. Hivatkozott el nem készült szabályzatokra, továbbá „El kell készíteni a … szabályzatot." szövegek is szerepeltek benne. Az IBIR egy átalános mindenki által betartandó IBSZ-ből és az Üzletmenet folytonossági szabályzatból állt. Mivel a mindenkire vonatkozó IBSZ túl általános volt, a benne megfogalmazott követelmények és feladatok nem voltak szerepkörökhöz rendelve, például: „az informatikai rendszereket biztonsági szintbe kell sorolni az Ibtv-nek megfelelően", de nincs meghatározva, hogy kinek a felelőssége és mikor kell végrehajtani a feladatot. Ennek következtében a feladatok felelősei nem ismerték a biztonság érdekében betartandó szabályokat és elvégzendő feladatokat, így esetlegessé vált a szabályzat betartása és betartatása. Ha a jogszabályi megfelelőséget néztük, akkor a szervezet csak látszólag felelt meg a jogszabályi követelményeknek. Mivel az IBIR túl általános volt, az első feladat a tervezett rendszer információbiztonsági követelményeinek meghatározásához a rendszer működési környezetének felmérése és a felelősségi körök meghatározása volt. Ezt követte a rendszer információbiztonsági követelményeinek specifikálása Ibtv és BMr alapokon. A projektnek nem volt része a biztonsági szabályozás megújítása, de az információbiztonságért felelős felismerve a helyzet súlyosságát javaslatot kért az IBIR működőképessé tételének javítására.

### 3.1.2 Az ISO 27001 szerint működő szervezetek IBIR elemzése

A 6-os táblázat témakörökre bontva mutatja be ISO/IEC 27001 szabvány struktúrájának megfelelő bontásban a két szervezet IBIR rendszerének szabvány szerinti vizsgálatát.

| Téma | Sz6 | Sz7 |
|---|---|---|
| I., A SZERVEZET ÉS KÖRNYEZETE | Igen | Igen |
| II., VEZETÉS | Igen | Igen |
| III., TERVEZÉS | Módszertannal támogatott | Módszertan nélküli leírás |
| IV., TÁMOGATÁS | Igen | Részleges |
| V., MŰKÖDÉS | Igen | Nem |
| VI., TELJESÍTMÉNYÉRTÉKELÉS | Igen | Igen |
| VII., FEJLESZTÉS | Rendszeresen frissített | Elméletben szabályozva |
| A./1. Információbiztonsági irányelvek | Igen | Igen |
| A./2.Az információbiztonság szervezete | Igen | Igen |
| A./3. Az emberi erőforrások biztonsága | Igen | N/A |
| A./4.Vagyonelemek kezelése | Igen | Nem |
| A./5. Hozzáférés-felügyelet | Általános irányelvek, Rendszerenként jogosultságkezelési folyamat | Általános irányelvek, Informatikai jogosultságkezelési szabályzat |
| A./6. Titkosítás | Igen | N/A |
| A./7. Fizikai és környezeti biztonság | Fizikai védelem szabályozása | Nem |
| A./8. Az üzemelés biztonsága | Igazoló dokumentumok | N/A |
| A./9. A kommunikáció biztonsága | Részletes, gyakorlati | Elméleti |
| A./10. Rendszerek beszerzése, fejlesztése és karbantartása | Fejlesztési eljárásrend | Fejlesztési eljárásrend |
| A./11. Szállítói kapcsolatok | Igen | Nem |
| A./12. Az információbiztonsági incidensek kezelése | Igen | Igen |
| A./13. A működésfolytonosság biztosításának információbiztonsági vonatkozásai | Üzletmenet folytonossági szabályzat. | Igen |
| A./14.Megfelelés | Részletes alkalmazhatósági kritériumok az érintett szabványok mentén. | Csak hivatkozott jogszabályok és szabványok. |

*6. táblázat ISO 27001 szerint működő vizsgált szervezetek általános IBIR jellemzői (saját szerkesztés)*

Első látásra mindkét szervezet jól teljesít a szabályzatok megfelelőségének terén. Ennek ellenére jelentős különbségek vannak a szabályozás minőségét illetően, ami az információbiztonság megvalósításának eredményességében csapódik le.

Az **Sz6** szervezet esetében az IBIR legfelső szintjén egy 90 oldalas részletesen kidolgozott Információbiztonsági szabályzat (továbbiakban IBSZ) áll. A Szabályzat részletesen bemutatja az IBIR komponenseit és fejlesztési folyamatát, kitér a biztonságtervezés alapjául szolgáló kockázat elemzési és kezelési módszertanra, az érintett személyek felelősségi köreire, a vezetői elkötelezettségre, a kommunikációra, az IBIR működtetésére, a biztonsági szervezet részletes bemutatására, az IBIR teljesítménymérésére és auditálására. Az alkalmazhatósági kritériumok

esetében hivatkozik azon szabályzatokra és eljárásrendekre, amelyek végrehajtása biztosítja a kritériumra vonatkozó követelmények teljesülését.

Az IBIR jelentős mennyiségű dokumentumból épül fel, amelyek tartalmazzák az IBIR végrehajtásához szükséges eljárásrendeket és igazoló dokumentum mintákat. Ezek a dokumentumok biztonsági kategóriákba soroltak és hozzáférésük szakterülethez kötött. Ez biztosítja, a dokumentumokban megfogalmazott eljárásrendek bizalmasságának megőrzését. A szervezet esetében az információbiztonsági felelős rendelkezik információbiztonsági szakképesítéssel, a szervezet biztonsági igazgatójának beosztottja, neki tartozik beszámolási kötelezettséggel.

A dokumentáció átvizsgálását követően az információbiztonsági, IT fejlesztési és üzemeltetési vezetőkkel folytatott megbeszélések során kiderült, hogy szigorúan veszik a szabályok betartását, ugyanakkor a szabályzati struktúrát nem tartják teljesen megfelelőnek. Az IBSZ általános szintű információbiztonsági szabályokat és egyes területekre vonatkozóan részletes útmutatást is tartalmaz. Megfelel az elvárásoknak, de jobb lenne, ha csak magasszintű, mindenkire érvényes részletezettségű követelményeket fogalmazna meg. Közvetlenül az IBSZ alá tartozó szabályozási réteg tartalmazza az összes szabályzatot és eljárásrendet. Sok esetben az igazoló dokumentumok is erre a szintre kerülnek. Ezen a szinten négy olyan szabályzat található, amelyeknek direkt módon kell kapcsolódniuk az IBSZ-hez: a kockázatkezelési, hozzáféréskezelési, informatikai fejlesztési és üzemeltetési szabályzat. Ezek a szabályzatok további hivatkozásokat tartalmaznak informatikai rendszer szintű munkautasításokra és igazoló dokumentumokra. Mivel az IBIR-ben ezt a négy szabályzatot kivéve a középréteg (egyes szakterületekre vonatkozó általános szabályzatok és eljárásrendek) hiányzik, és a többi dokumentumra jó esetben az IBSZ hivatkozik, a szabályzatok betartásának ellenőrzése nehézséget okoz. Az információbiztonsági audit során nehéz azonosítani azokat a szabályzatokat, amelyek garantálják az egyes rendszerekben kezelt adatok biztonságát. Az IT fejlesztési és üzemeltetési vezetők néhány helyen korlátozónak tartják a szabályzatokat, más esetekben pedig túlságosan megengedőnek. Ez abból adódik, hogy a szabályzatok nem igazodnak teljes mértékben a szervezet működéséhez. Ez részben annak a következménye, hogy készültek olyan szervezeti egységekre vonatkozó szabályzatok, amelyek a szervezet átalakításai során elvesztették a relevanciájukat, így ezek betartása és betartatása ellehetetlenül, aktualizálásukra nem minden esetben áll rendelkezésre a megfelelő emberi erőforrás. A szabályzati háttér struktúrájának, a szabályzatok közötti átfedéseknek és az elévülésnek köszönhetően nem mindig világos a dolgozók számára, hogy mely szabályzatokat kell betartani és mely eljárásrendeket kell végrehajtani.

Az **Sz7** szervezet esetében az IBIR legfelső szintjén egy rövid pár oldalas Innformációbiztonsági politika áll, amelyhez kapcsolódik egy 30 oldalas IBSZ. A szabályzat irányelveket és magas szintű követelményeket fogalmaz meg, nem tartalmaz végrehajtható eljárásokat. Definiál szerepköröket, de azokat nem rendeli hozzá a szervezet munkaköreihez és munkatársaihoz. Az IBIR következő szintjén a Fejlesztési szabályzat és az Informatikai jogosultságkezelési szabályzat található. Az informatikai üzemeltetés kiszervezett, nincs üzemeltetési szabályzat. Az informatikai üzemeltetéssel kapcsolatos magas szintű követelményeket az IBSZ tartalmazza. Az IBSZ-hez tartozik egy Felhasználói informatikai szabályzat, amely a felhasználók jogait és kötelezettségeit taglalja. Ezt minden dolgozónak meg kell ismernie és alá kell írnia, hogy ismeri a tartalmát és betartja. A szervezet információbiztonsági felelőse az operatív igazgató, nem rendelkezik információbiztonsági képesítéssel és a vezérigazgatónak tartozik beszámolási kötelezettséggel. A szervezetben az információbiztonsági javaslatokat az IT vezető állítja össze, de ő sem rendelkezik információbiztonsági képesítéssel.

Az információbiztonsági felelőssel és IT vezetővel folytatott interjúk kapcsán kiderült, hogy a szervezet szabályozási rendszere nem felel meg teljes mértékben az elvárásoknak. Vannak olyan szabályok, amelyek akadályozzák a mindennapi munkát, továbbá akadozik a működésfolytonossági tervek frissítésének folyamata, amelyek karbantartását rendszerenként szerződés keretében a szállítóktól várják el. Az IBSZ alá tartoznak a munkautasítások (tevékenységek, amelyek nem munkafolyamatok): mentés, helyreállítás, jogosultság kezelés és egyéb információbiztonsággal kapcsolatos munkafolyamatok. A szervezet célul tűzte ki az IBIR továbbfejlesztését azzal a céllal, hogy megfeleljen az ISO/IEC 27001 szabványnak. A szervezet kiszervezte az IT üzemeltetést, az IT fejlesztések megvalósítására a Fejlesztési szabályzat követelményei az irányadók.

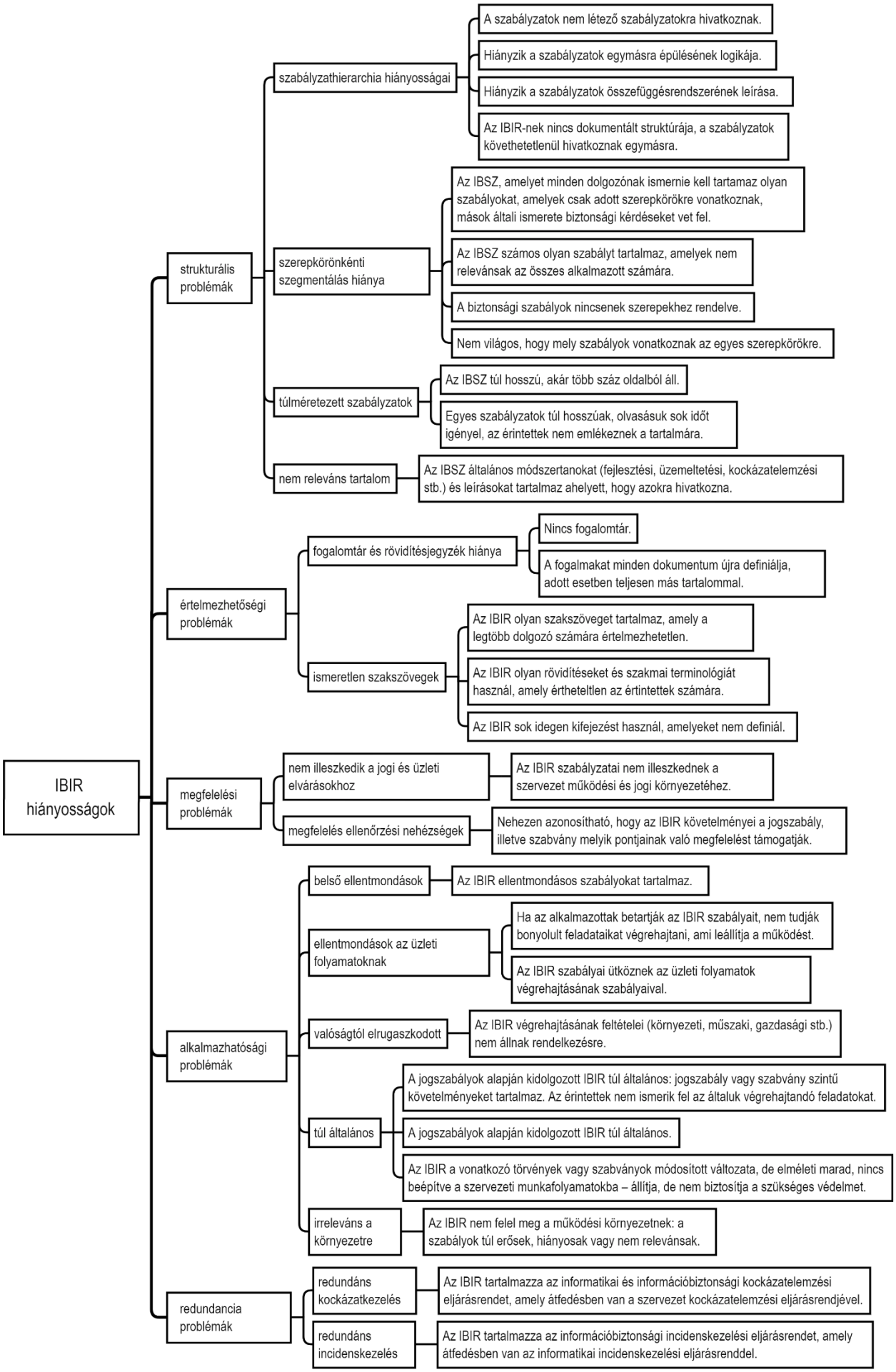
### 3.1.3 Feltárt problémák strukturálása és csoportosítása

Az esettanulmányokat elemezve kigyűjtöttem az IBIR-rel kapcsolatos problémákat és hiányosságokat, amelyeket az 7. táblázatban foglaltam össze. A táblázatban nem soroltam fel külön-külön a különböző projektekben egy-az-egyben megismétlődő problémákat és hiányosságokat. A sorszámok nem jelölnek prioritási sorrendet, csak az összegyűjtött hiányosságok számosságát tükrözik.

| # | Probléma, hiányosság |
|---|---|
| 1. | A szabályzatok nem létező szabályzatokra hivatkoznak. |
| 2. | Hiányzik a szabályzatok egymásra épülésének logikája. |
| 3. | Hiányzik a szabályzatok összefüggésrendszerének leírása. |
| 4. | Az IBSZ, amelyet minden dolgozónak ismernie kell tartamaz olyan szabályokat, amelyek csak adott szerepkörökre vonatkoznak, mások általi ismerete biztonsági kérdéseket vet fel. |
| 5. | Az IBSZ számos olyan szabályt tartalmaz, amelyek nem relevánsak az összes alkalmazott számára. |
| 6. | A biztonsági szabályok nincsenek szerepekhez rendelve. |
| 7. | Nem világos, hogy mely szabályok vonatkoznak az egyes szerepkörökre. |
| 8. | Az IBSZ általános módszertanokat (fejlesztési, üzemeltetési, kockázatelemzési stb.) és leírásokat tartalmaz ahelyett, hogy azokra hivatkozna. |
| 9. | Az IBSZ túl hosszú, akár több száz oldalból áll. |
| 10. | Az IBIR-nek nincs dokumentált struktúrája, a szabályzatok követhetetlenül hivatkoznak egymásra. |
| 11. | Nincs fogalomtár. |
| 12. | A fogalmakat minden dokumentum újra definiálja, adott esetben teljesen más tartalommal. |
| 13. | Az IBIR olyan szakszöveget tartalmaz, amely a legtöbb dolgozó számára értelmezhetetlen. |
| 14. | Egyes szabályzatok túl hosszúak, olvasásuk sok időt igényel, az érintettek nem emlékeznek a tartalmára. |
| 15. | Az IBIR olyan rövidítéseket és szakmai terminológiát használ, amely értheteltlen az értintettek számára. |
| 16. | Az IBIR sok idegen kifejezést használ, amelyeket nem definiál. |
| 17. | Az IBIR szabályzatai nem illeszkednek a szervezet működési és jogi környezetéhez. |
| 18. | A jogszabályok alapján kidolgozott IBIR túl általános. |
| 19. | Az IBIR a vonatkozó törvények vagy szabványok módosított változata, de elméleti marad, nincs beépítve a szervezeti munkafolyamatokba - állítja, de nem biztosítja a szükséges védelmet. |
| 20. | Nehezen azonosítható, hogy az IBIR követelményei a jogszabály, illetve szabvány melyik pontjainak való megfelelést támogatják. |
| 21. | Az IBIR ellentmondásos szabályokat tartalmaz. |
| 22. | Ha az alkalmazottak betartják az IBIR szabályait, nem tudják bonyolult feladataikat végrehajtani, ami leállítja a működést. |
| 23. | Az IBIR végrehajtásának feltételei (környezeti, műszaki, gazdasági stb.) nem állnak rendelkezésre. |
| 24. | Az IBIR nem felel meg a működési környezetnek: a szabályok túl erősek, hiányosak vagy nem relevánsak. |
| 25. | A jogszabályok alapján kidolgozott IBIR túl általános: jogszabály vagy szabvány szintű követelményeket tartalmaz. Az érintettek nem ismerik fel az általuk végrehajtandó feladatokat. |
| 26. | Az IBIR szabályai ütköznek az üzleti folyamatok végrehajtásának szabályaival. |
| 27. | Az IBIR tartalmazza az informatikai és információbiztonsági kockázatelemzési eljárásrendet, amely átfedésben van a szervezet kockázatelemzési eljárásrendjével. |
| 28. | Az IBIR tartalmazza az információbiztonsági incidenskezelési eljárásrendet, amely átfedésben van az informatikai incidenskezelési eljárásrenddel. |

*7. táblázat Feltárt IBIR problémák (saját szerkesztés)*

A kutatás alatt projektről-projektre haladva feltártam az információbiztonság rendszer eredményes megvalósulását akadályozó tényezőket. Kigyűjtöttem, elemeztem és megpróbáltam általánosítani a szervezetekben előforduló hiányosságokat és problémákat. Az aktuális projekt keretében vizsgáltam az addig definiált általános és korábban kigyűjtött problémák előfordulását. A 7. táblázat jól szemlélteti, hogy több egymáshoz hasonló vagy kapcsolódó probléma és hiányosság fordult elő. A kutatási projektek keretében vizsgáltam a problémák kiváltó okait és összefüggéseit, amelyek mentén csoportosítottam a már definiált általános problémákat. Az előforduló problémák, hiányosságok, általános problémák és csoportosításuk összefüggéseit a 4. ábra mutatja be.




*4. ábra Problémák, hiányosságok, általános problémák és csoportosításuk (saját szerkesztés)*

Az 4. ábrán jól látható, hogy egy háromrétegű hierarchiát hoztam létre. A legalsó szinten helyezkednek el a feltárt problémák és hiányosságok, amelyeket a második szinten lévő általános problémákhoz rendeltem hozzá. Az így kapott általános problémákat az előfordulási okok és az általuk érintett problémakör mentén a harmadik szinten található csoportokba rendeztem. A kutatás ideje alatt folyamatosan felülvizsgáltam az általános problémák definícióit. Hozzákapcsoltam az újonnan felderített és közel álló hiányosságokat, szükség esetén pedig pontosítottam az általános probléma definícióját, törekedve az általános problémák fogalmainak telítésére [15].

Az általános információbiztonsági problémák definícióit a 8. táblázatban foglaltam össze.

| # | Általános probléma | Általános probléma leírása |
|---|---|---|
| 1. | **szabályzathierarchia hiányosságai** | Az IBIR-nek nincs dokumentált struktúrája. Nincs definiálva a szabályzatok összefüggéseinek és egymásra épülésének rendszere. |
| 2. | **szerepkörönkénti szegmentálás hiánya** | A biztonsági szabályok nincsenek szerepekhez rendelve. Nem világos, hogy mely szabályok vonatkoznak az egyes szerepkörökre. A szabályzatok nem szerepkörök mentén vannak összeállítva. |
| 3. | **túlméretezett szabályzatok** | Az IBSZ túl hosszú, akár több száz oldalból áll. |
| 4. | **nem releváns tartalom** | Az IBSZ általános módszertanokat (fejlesztési, üzemeltetési, kockázatelemzési stb.) és leírásokat tartalmaz ahelyett, hogy azokra hivatkozna. |
| 5. | **fogalomtár és rövidítésjegyzék hiánya** | A teljes IBIR-en átívelő egységesített fogalom és rövidítésjegyzék hiánya. |
| 6. | **ismeretlen szakszövegek** | Az IBIR nehezen olvasható a szakszövegek, idegen kifejezések és rövidítések használata miatt. |
| 7. | **túlméretezett szabályzatok** | Egyes szabályzatok túl hosszúak, olvasásuk sok időt igényel, az érintettek nem emlékeznek a tartalmára. |
| 8. | **nem illeszkedik a jogi és üzleti elvárásokhoz** | Az IBIR szabályzatai nem illeszkednek a szervezet üzleti elvárásaihoz és jogi környezetéhez. |
| 9. | **megfelelés ellenőrzési nehézségek** | Az IBIR nem tartalmaz megfelelő hivatkozásokat a jogszabályi és szabvány követelményekre, fejezetekre. |
| 10. | **belső ellentmondások** | Az IBIR szabályzatai tartalmaznak egymásnak ellentmondó szabályokat. |
| 11. | **ellentmondások az üzleti folyamatoknak** | Az IBIR szabályai ütköznek az üzleti folyamatok végrehajtásának szabályaival. Az IBIR egyes szabályainak betartása akadályozza vagy ellehetetleníti a munkavégzést. |
| 12. | **valóságtól elrugaszkodott** | Az IBIR végrehajtásának feltételei (környezeti, műszaki, gazdasági stb.) nem állnak rendelkezésre a szervezetben, jellemzően a szervezeti kultúra és anyagi erőforrások. |
| 13. | **túl általános** | A jogszabályok alapján kidolgozott IBIR túl általános: jogszabály vagy szabvány szintű követelményeket tartalmaz. Az érintettek nem ismerik fel az általuk végrehajtandó feladatokat. |
| 14. | **irreleváns a környezetre** | Az IBIR nem felel meg a működési környezetnek: a szabályok túl erősek, hiányosak vagy nem relevánsak. |
| 15. | **redundáns kockázatkezelés** | Az IBIR tartalmazza az informatikai és információbiztonsági kockázatelemzési eljárásrendet, amely átfedésben van a szervezet kockázatelemzési eljárásrendjével. |
| 16. | **redundáns incidenskezelés** | Az IBIR tartalmazza az információbiztonsági incidenskezelési eljárásrendet, amely átfedésben van az informatikai incidenskezelési eljárásrenddel. |

*8. táblázat Általános IBIR problémák definíciója (saját szerkesztés)*

A 8-as táblázatban definiált általános problémák 4-es ábrán bemutatott csoportosításához a problémacsoport definíciókat a 9-es táblázatban gyűjtöttem össze.

| Problémacsoport | Probléma, hiányosság |
|---|---|
| **strukturális problémák** | Strukturális problémának nevezek minden az IBIR szerkezetére és felépítésére vonatkozó hiányosságot. Ide tartoznak a szabályzatok hierarchiáját, összefüggésrendszerét, szerepkörökhöz rendelését, hivatkozásait érintő hiányosságok, valamint az irreleváns tartalom és a túlméretezettség. |
| **értelmezhetőségi problémák** | Értelmezhetőségi problémának nevezek minden olyan tényezőt, ami befolyásolja a szabályzatok megértését. Összefoglalva ez azt jelenti, hogy a célközönség nem érti a szabályzatokban megfogalmazott követelményeket. Ide tartoznak az ismeretlen rövidítések és kifejezések, a szakzsargon és az érthetetlen nagy körmondatok. |
| **megfelelési problémák** | A szervezetre vonatkozó jogszabály vagy szervezet által választott szabvány követelményeinek való megfeleléssel kapcsolatos problémák. |
| **alkalmazhatósági problémák** | A szabályzatok betartásával, betartatásával és eljárásrendek végrehajtásával kapcsolatos problémák. Ide tartoznak az IBIR belső ellentmondásai, ellentmondások az üzleti szabályzatoknak, munkafolyamatok ellehetetlenítése, feladatok felelősökhöz rendelésének problémái, az irreális elvárások és a valóságtól való elrugaszkodottság a védelmi intézkedések terén. |
| **redundancia problémák** | Az IBIR előír más szervezeti szintű szabályzatok által is előírt munkafolyamatot alternatív végrehajtással. |

*9. táblázat Azonosított problémacsoportok definíciója (saját szerkesztés)*

A feltárt problémák és hiányosságok általánosítása során nyomon követtem az általános problémák elfordulását a szervezetekben, amelyeket később összesítettem. Az általános problémák előfordulását a vizsgált szervezetekben a 10-es táblázat mutatja be.

| Általános probléma | Sz1 | Sz2 | Sz3 | Sz4 | Sz5 | Sz6 | Sz7 | Sz8 | Sz9 |
|---|---|---|---|---|---|---|---|---|---|
| **Strukturális problémák** | | | | | | | | | |
| szabályzathierarchia hiányosságai | igen | nem | N/A | igen | igen | igen | igen | N/A | igen |
| szerepkörönkénti szegmentálás hiánya | nem | igen | N/A | igen | igen | nem | igen | N/A | igen |
| túlméretezett szabályzatok | nem | nem | N/A | nem | igen | nem | nem | N/A | nem |
| nem releváns tartalom | nem | nem | N/A | nem | igen | nem | nem | N/A | nem |
| **Értelmezhetőségi problémák** | | | | | | | | | |
| fogalomtár és rövidítésjegyzék hiánya | nem | nem | N/A | igen | igen | nem | igen | N/A | igen |
| ismeretlen szakszövegek | igen | igen | N/A | nem | igen | igen | nem | N/A | igen |
| **Megfelelőségi problémák** | | | | | | | | | |
| nem illeszkedik a jogi és üzleti elvárásokhoz | igen | igen | N/A | igen | igen | nem | igen | N/A | igen |
| megfelelés ellenőrzési nehézségek | igen | nem | N/A | igen | igen | igen | igen | N/A | igen |
| **Alkalmazhatósági problémák** | | | | | | | | | |
| belső ellentmondások | igen | nem | N/A | nem | igen | nem | nem | N/A | nem |
| ellentmondások az üzleti folyamatoknak | igen | igen | N/A | igen | igen | igen | igen | N/A | igen |
| valóságtól elrugaszkodott | igen | igen | N/A | nem | igen | nem | nem | N/A | igen |
| túl általános | nem | igen | N/A | igen | igen | nem | igen | N/A | igen |
| irreleváns a környezetre | nem | nem | N/A | nem | igen | nem | nem | N/A | igen |
| **Redundancia problémák** | | | | | | | | | |
| redundáns kockázatkezelés | igen | igen | N/A | igen | igen | igen | igen | N/A | igen |
| redundáns incidenskezelés | igen | igen | N/A | igen | igen | igen | igen | N/A | igen |

*10. táblázat Általános információbiztonsági problémák előfordulása a vizsgált szervezetekben (saját szerkesztés)*

Összesítve a 10-es táblázatban szereplő adatokat a szervezetek mérete szerint 11-es táblázatban látható ministatisztikát kapjuk. A táblázatban logikusan csak a projekt indulásakor IBIR-rel rendelkező szervezetek szereplenek.

| Problémacsoport / Általános probléma | Kicsi | Közepes | Nagy | Összesen |
|---|---|---|---|---|
| ***Strukturális problémák*** | ***1*** | ***3*** | ***3*** | ***7*** |
| *szabályzat hierarchia hiányosságai* | *1* | *2* | *3* | *6* |
| *szerepkörönkénti szegmentálás hiánya* | *1* | *2* | *2* | *5* |
| túlméretezett szabályzatok | 0 | 0 | 1 | 1 |
| nem releváns tartalom | 0 | 0 | 1 | 1 |
| ***Értelmezhetőségi problémák*** | ***1*** | ***3*** | ***3*** | ***7*** |
| fogalomtár és rövidítésjegyzék hiánya | 1 | 1 | 2 | 4 |
| *ismeretlen szakszövegek* | *0* | *3* | *2* | *5* |
| ***Megfelelőségi problémák*** | ***1*** | ***3*** | ***3*** | ***7*** |
| *nem illeszkedik a jogi és üzleti elvárásokhoz* | *1* | *3* | *2* | *6* |
| *megfelelés ellenőrzési nehézségek* | *1* | *2* | *3* | *6* |
| ***Alkalmazhatósági problémák*** | ***1*** | ***3*** | ***3*** | ***7*** |
| belső ellentmondások | 0 | 1 | 1 | 2 |
| *ellentmondások az üzleti folyamatoknak* | *1* | *3* | *3* | *7* |
| valóságtól elrugaszkodott | 0 | 3 | 1 | 4 |
| *túl általános* | *1* | *2* | *2* | *5* |
| irreleváns a környezetre | 0 | 1 | 1 | 2 |
| ***Redundancia problémák*** | ***1*** | ***3*** | ***3*** | ***7*** |
| *redundáns kockázatkezelés* | *1* | *3* | *3* | *7* |
| *redundáns incidenskezelés* | *1* | *3* | *3* | *7* |

*11. táblázat Általános IBIR problémák összesítése a vizsgált szervezetekre (saját szerkesztés)*

A 11-es táblázatban összesítve és a szervezetek mérete szerint csoportosítva látjuk, hogy az egységesített problémák és a problémacsoportok előfordulásai hogyan oszlanak el a kis, közepes és nagy szervezetekében. Az összesítés jól mutatja, hogy minden egységesített problémacsoport valamely eleme előfordul minden vizsgált szervezet esetében. Megállapítottam, hogy minden problémacsoport előfordul kis, közepes és nagy méretű szervezetben. Továbbá megállapítottam, hogy a 7 vizsgált szervezet mindegyikében előfordul minden problémacsoport, így kijelenthetem, hogy minden problémacsoport érint minden a kutatási projektekben érintett szakterületet.

A táblázatban dőlt betűvel szedtem azokat az egységesített problémákat, amelyek legalább 5 vizsgált szervezetben előfordultak. Ez azt is jelenti egyben, hogy a szabályzathierarchia hiányosságai, a szerepkörönkénti szegmentálás hiányosságai, az ismeretlen szakszövegek, a jogi és üzleti elvárásokhoz való illeszkedés, az ellentmondás az üzleti folyamatoknak, a túl általános IBIR és a redundáns incidenskezelési és kockázatkezelési folyamat problémakörök 1-2 kivétellel minden vizsgált szervezet esetében elfordulnak.

## 3.2 Információbiztonsági problémák okainak feltárása

Az IBIR-rel kapcsolatos problémák feltárása lehetőséget ad a kiküszöbölésükre. Ahhoz, hogy hatékony módot találjak a felmerülő problémák megszüntetésére annak kellett utánajárnom, hogy miért fordulnak elő. Feltárásuk során arra lettem figyelmes, hogy az IBIR és az információbiztonság megvalósítása elszakad egymástól. A szervezetek követve a jogszabályokat és szabványokat olyan IBIR-t alkotnak, amely papíron megfelel a szabályozási környezetnek, de követelményeik megvalósulásában jelentős hiányosságok lépnek fel. Az elemzés elvégzését elméleti kutatással kezdtem, igyekeztem olyan publikációkat keresni, amelyek megvalósított IBIR rendszerek felméréseit mutatják be. Nassar nemcsak feltárja a hiányosságokat, hanem COBIT érettségi modell alapján ISO/IEC 27001 szerinti érettségi szintet is vizsgál [106]. A bemutatott gap elemzés szabályozási szempontból nézi az információbiztonság megvalósulását, sajnos nem tér ki a kontrollok megvalósulásának vizsgálatára és a megvalósulás minőségére a gyakorlatban. Fontosnak tartom ezt, mert kutatásaim arra engednek következtetni, hogy leginkább a megvalósulás és annak minősége környékén kell keresni a problémákat majd feltárni azok okait. Az információbiztonsági hiányosságok okainak feltárását az azonosított problémacsoportok mentén végeztem el.

### 3.2.1 Strukturális problémák vizsgálata

A vizsgált szervezetekben a strukturális problémákat jellemzően a szabályzathierarchia, a dokumentációs rend hiánya, a szabályzatok egymásra való hivatkozásának hibái és hiánya, az IBIR nem megfelelő tagoltsága, a túlméretezettség és a nem releváns tartalom okozta.

Az okok vizsgálatakor a szabályzatok létrehozásának és felülvizsgálatának körülményeit vizsgáltam. Az információbiztonsági vezetőkkel folytatott interjúk során kapott válaszok szerint a szervezetek arra törekedtek, hogy:

- az IBSZ fedjen le minden információbiztonságot érintő területet és tartalmazza a szükséges szakmai útmutatókat, hogy az olvasónak ne kelljen utánajárnia;
- az IBSZ biztosítsa a vonatkozó jogszabályok és szabványok követelményeit, de nem figyeltek a megfogalmazott követelmények kivitelezhetőségére és betarthatóságra;
- nem figyeltek arra, hogy a szabályzatokban helyben legyen elérhető fogalomtár;
- a szervezet átalakításakor szervezeti egységeket, szerepköröket és szabályzatokat hoztak létre, módosítottak és szüntettek meg de nem törődtek az IBIR konzisztens frissítésével;
- az IBIR létrehozását külső partner végezte, a szervezet nem vett részt a kidolgozásban.

Arra a kérdésre, hogy követtek-e valamilyen struktúrát, útmutatót vagy módszertant a szabályzatok elkészítésekor és felülvizsgálatakor szinte egybehangzó volt a válasz, hogy csak a vonatkozó szabványok és jogszabályok követelményeire figyeltek, mivel az elsődleges szempont a megfelelés volt.

Közelebbről megnézve a kapott válaszokat, kiderül, hogy a strukturális problémákat szabályzatírási módszertani hiányosságok okozták. Több Információbiztonsági szakértő kollégát is megkérdeztem, hogy milyen módszertant alkalmaznak IBIR kidolgozáskor. Arra a következtetésre jutottam, hogy mindenki saját módszerrel dolgozik, nincs egységes útmutató a szabványokban és jogszabályokban a követelmények kidolgozására.

### 3.2.2 Értelmezhetőségi problémák vizsgálata

Az IT és információbiztonsági vezetőkkel folytatott beszélgetések rámutattak arra, hogy az IT és információbiztonsági szakembereknek számára magától értetődő a szabályzatokban használt terminológia ismerete. Sok esetben fel sem merült bennük, hogy az átlagemberek nem értik vagy egyszerűen mást értenek a szabályzatokban használt rövidítések és kifejezések alatt. Három szervezet esetében volt fogalomtár a szabályzatokban, igaz mindhárom esetben elavult. Kiderült, hogy a szabályzatok és eljárásrendek felülvizsgálata során nem figyeltek arra, hogy az új rövidítések és fogalmak átvezetése megtörténjen, a régiek pedig kikerüljenek.

Szinte egybehangzó volt az információbiztonsági vezetők válasza arra a kérdésre, hogy hogyan lehetne az értelmezhetőségi problémákat kiküszöbölni, amelyhez három fontos tevékenységet jelöltek meg. Egységes IBIR rövidítésjegyzék és fogalomtár. Szabályzatok és eljárásrendek ellenőrzése és véleményezése a szervezet szabályzataiért felelős vezetőjével, aki jellemzően az operatív vezető. Módszertani útmutató készítése, amely leírja a rövidítés és fogalomtár szerepét, létrehozásának és frissítésének módját a szabályzatok írása és felülvizsgálata során.

### 3.2.3 Megfelelési problémák vizsgálata

A szervezetek törekednek a jogszabály és szabvány követelmények teljesítésére. Ez kivétel nélkül igaz minden vizsgált szervezetre, mégis előfordultak hiányosságok. Több szervezet tartozott az Ibtv hatálya alá, miközben személyes adatokat kezelt így vonatkozott rájuk a GDPR is. Némelyik szervezetben fontos követelmény volt az ISO 27001 szabvány szerinti tanúsítás és további a szektorra érvényes jogszabályok is támasztottak információbiztonsági követelményeket. Ennek következtében össze kellett fésülni a vonatkozó jogszabályok és szabványok követelményeit. Az IBIR struktúrájából kiolvasható volt, hogy mely szabványra vagy jogszabályra építették fel.

Az információbiztonsági vezetőkkel folytatott beszélgetések során kiderült, hogy a problémák jellemzően három forrásból származtak: a követelmények összefésülése során nem feltétlenül az erősebb követelmény került be a szabályzatba, a kockázatelemzés hibásan a reálisnál alacsonyabb vagy magasabb biztonsági osztályba sorolta a szervezetet és végül a követelmények jogszabályhoz vagy szabványhoz való kapcsolása nem került be a szabályzatba. A követelmények szabványponthoz kapcsolása nem előírás, de hiánya megnehezíti a megfelelés ellenőrzését és az IBIR későbbi felülvizsgálatát.

### 3.2.4 Alkalmazhatósági problémák vizsgálata

A leggyakoribb alkalmazhatósági problémakör a szabályzatok részleges betartása és az eljárásrendek végrehajtásának ellehetetlenülése vagy elmulasztása. Az információbiztonságért és informatikáért felelős vezetővel folytatott egyeztetések során kiderült, hogy több esetben is, kampányszerűen készültek az auditra, azaz a szabályok maradéktalan betartása nem folyamatos. Elmondásuk szerint az IBIR csak ideig óráig nyújtja a szükséges mértékű információbiztonságot, miközben jelentős adminisztrációs terhet ró a szervezet munkatársaira. Ennek kiküszöbölésére az érintett vezetők a rendszeres, rövidebb időközönként elvégzett ellenőrzést és az adminisztráció csökkentését látják megoldásnak. Többen megjegyezték, hogy az adminisztráció csak olyan mértékben csökkenthető, ami még biztosítja a szervezet ügyviteléhez szükséges biztonsági előírásokat. Elhangzott, hogy a modernebb biztonsági eszközök (egységesített fenyegetéskezelő (UTM) rendszerek, automatizált naplóelemző rendszer és hálózatfelügyeleti megoldások) alkalmazásával csökkenthető az adminisztráció, de az említett eszközök bekerülési és testre szabási költségei nem minden esetben férnek bele a szervezet költségvetésébe. További megjegyzésként hangzott el több projekt során az informatikai és üzleti vezetőktől, hogy az információbiztonsági követelményeket be kellene építeni a szervezet munkafolyamataiba, így harmonizálhatók lennének az üzleti és információbiztonsági követelmények.

A szervezetek működése során gyakran fordulnak elő olyan felelősségi kérdések és ezekre visszavezethető anomáliák, amelyek befolyásolják a szabályzatok betartását és a munkafolyamatok végrehajtását. Kutatási projektjeim során többször találkoztam olyan szituációval, amikor a szervezet felsővezetése elhatárolódott az információbiztonsági kérdésektől, azok kezelését áthárította egy kinevezett információbiztonsági vezetőre vagy felelős személyre, ugyanakkor nem adott megfelelő szintű jogosultságot és erőforrást feladatai ellátásához. Volt olyan eset amikor a szervezet első számú vezetője nem volt hajlandó elolvasni a pár oldalas, minimálisra csökkentett felhasználói biztonsági szabályzatot, amely a munkavégzéshez szükséges számítógépes biztonsági előírásokat tartalmazta. Feltettem magamnak a kérdést, hogy ez a vezető

hogyan tud dönteni információbiztonsági projektek elindításáról és azok mértékéről. IBIR projektjeim során több esetben fordult elő, hogy az IBIR-ben meghatározott szerepkörök hiányoztak a szervezeti működési szabályzataiból és nem szerepeltek a munkaköri leírásokban sem. Ez három fő okra volt visszavezethető. Az IBIR elkészítése során a szervezet nem vonta be megfelelő mértékben a kulcspozíciókban dolgozó munkatársakat (jellemzően folyamatgazdák, operatív vezetők) a szabályozás elkészítésébe. A szervezet teljes mértékben külső tanácsadóra bízta az IBIR megújítását vagy elkészítését, a célkitűzés a jogszabályi vagy szabvány szerinti megfelelés volt miközben a szervezet nem vett részt annak kidolgozásában. Az IBIR-ben definiált szerepkörök munkakörökhöz voltak rendelve, ugyanakkor a gyakori szervezeti átalakítások felborították a szervezetben definiált munkaköröket, miközben elmaradt az IBIR szerepkörök összehangolása az átalakított munkakörökkel. Ezekben az esetekben jellemző tünetként azonosítottam, a biztonsági szabályok végrehajtásának elmaradását, hiszen az IBIR szerepkörök egy része nem vonatkozott senkire.

A vizsgált szervezetek esetében az üzleti célok mielőbbi elérése érdekében sok eseten elhanyagolták a biztonsági követelmények meghatározását vagy a szükséges információbiztonsági intézkedések megvalósítását. Információbiztonsági szakértőkkel folytatott beszélgetéseimből kiderült, hogy ez nem csak a vizsgált szervezetekben, hanem általánosan előforduló probléma. Céljaik elréséhez a szervezetek szolgáltatásokat módosítanak vagy új szolgáltatásokat vezetnek be, miközben megújítják a munkafolyamatokat vagy újakat alakítanak ki, szoftvereket módosítanak vagy vezetnek be, új fizikai vagy virtuális hardvereket telepítenek, helyeznek el a szervezet informatikai infrastruktúrájában és kötnek rá az informatikai hálózatra. Ezek a tevékenységek hatással vannak a szervezet információbiztonságára. Nem szabad szem elől téveszteni, hogy az új vagy módosított szolgáltatásokat támogató munkafolyamatoknak és információs rendszereknek is illeszkedniük kell az IBIR előírásaihoz, teljesíteniük kell annak biztonsági követelményeit. Kutatási projektjeimben a kockázatelemzés és kockázatkezelés hiányosságaira lettem figyelmes: a kockázatelemzés elmaradása, a kockázatok alulértékelése és túlértékelése. Az alulértékelt kockázatok alacsonyabb biztonsági kategóriát és ezáltal hiányos, elégtelen védelmi intézkedéscsomagot eredményeztek. A túlértékelt kockázatok magasabb biztonsági kategóriát eredményeztek, túl szigorú szabályozáshoz és védelmi intézkedéscsomaghoz vezettek, amelyek feleslegesen akadályozták a napi munkavégzést és többletköltséget okoztak. Egyes esetekben ezek meghaladták a szervezetek számára rendelkezésre álló anyagi erőforrásokat, így megvalósításuk meghiúsult. A kockázatelemzés elmaradása esetén az információbiztonsági követelményeket becslések alapján állították össze,

amely, az esetek egy részében többletkiadást, más esetekben pedig hiányos információbiztonság megvalósítást eredményezett. A helyes egyensúly megvalósításában fontos szerepet játszik az információbiztonsági kockázatok felmérése és kezelése. Erre utal Jakus és Tick, amikor azt hangsúlyozza, hogy a biztonságtudatosság és a vállalati IT felelősségvállalás kulcsszerepet játszik az IT kockázatok csökkentésében [107].

Az információbiztonság megvalósítása és fenntartása a szervezeteken belül egy soha véget nem érő PDCA (Plan, Do, Check, Act) menedzsment ciklus keretében történik. A cél az információbiztonsági kockázatok elfogadható szintre való csökkentése. Azokban az esetekben amikor a szervezet nem rendelkezik megfelelő mennyiségű erőforrással az egyes kockázatok megfelelő mértékű csökkentéséhez, akkor általában léteznek olcsóbb alternatívák, amelyek nem ugyanakkora mértékben, de mégis csökkentik az adott kockázatot. Jó példa erre egy üzleti alkalmazás jogosultsági rendszerének nem megfelelősége, értem ez alatt, hogy a rendszer vagy túl kevés vagy túl sok jogot biztosít a felhasználók számára. A túl kevés jogosultság ellehetetleníti a munkát, a túl sok pedig információbiztonsági (bizalmassági és sértetlenségi) kockázatokkal jár. A rendszer jogosultsági rendszerének módosítása túl sokba kerül, nem járható út. Ez esetben a kockázatokat az érintett rendszerre érvényes szabályzatok kiegészítésével és betartatásával lehet csökkenteni. Az így bevezetett adminisztratív kontrollok nem feltétlenül kényszerítik ki az információbiztonság megfelelő szintjét, ami függ a szervezeti fegyelemtől. A menedzsment ciklus következő végrehajtása során megtörténik a védelmi intézkedés felülvizsgálata és a kockázatok csökkentésének érdekében, amennyiben a források rendelkezésre állnak elvégezhető a jogosultságok technológiai szintű korlátozása.

Több esetben is előfordult főleg állami és önkormányzati környezetben, hogy az információbiztonsági szabályozás követte az Ibtv és BMr előírásait, ugyanakkor szemmel láthatóan eltért a szervezet információbiztonsági igényeitől. A vizsgált esetekben a probléma az IBIR keletkezésének körülményeire volt visszavezethető. Ez jellemzően azokban az esetekben fordult elő, amikor jogszabályi határidő írta elő az IBIR létrehozását vagy a szervezet pályázni szeretett volna új információs rendszer megvalósítására és a pályázaton való részvétel meglévő IBIR-hez volt kötve. A szervezetek két módon tudták pótolni a hiányzó IBIR-t: profi tanácsadó cég segítségével, akinek már van tapasztalata vagy önerőből. A létrehozott IBIR követve a BMr struktúráját és megfelelt a jogszabályi követelménynek, de különbözőképpen jelentkeztek a végrehajtási problémák. Az IBIR-ben megfogalmazott szabályok túl szigorúak voltak, ami jellemzően akkor fordult elő, amikor külső tanácsadó készítette az IBIR-t és a szervezet nem vett részt a kialakításában. Ez esetben a biztonsági szabályok ütköztek a munkautasításokkal. A másik

eset az, amikor az IBIR-ben megfogalmazott szabályok túl általánosak voltak (jellemzően a jogszabály cikkelyeinek másolatai) és nem adtak elég támpontot a végrehajtáshoz. Mindkét modell esetében érvényes, hogy nem történt kockázatelemzés az IBIR-ben megfogalmazott a biztonsági követelmények pedig látszatintézkedések voltak.

Az alkalmazhatósági hiányosságok jellemzően az IBIR bevezetését követően jelentkeztek. Első látásra ezek végrehajtási problémák a követelmények alkalmazása során. Az érintettek (beleértem az IT és információbiztonsági vezetőket és az üzleti folyamatok felelőseit) interjúk keretében összegyűjtött tapasztalatai, azt mutatják, hogy ezek a problémák valójában tünetek, a problémát az IBIR hiányosságai és problémái okozzák. Az alkalmazhatósági problémák jellemzően a szabályok végrehajtásának pillanatában okoztak gondot, de probléma gyökere az IBIR létrehozása és frissítése során keletkezett. Az alkalmazhatósági problémák jellemzően az IBIR strukturális, értelmezhetőségi, vagy redundancia problémájára vezethető vissza, kivételt képez ez alól az egyensúlyozás az üzleti érdekek és biztonsági kontrollok között.

### 3.2.5 Redundancia problémák vizsgálata

Kutatásaim során a redundancia problémák jellemzően két területen fordultak elő. Az egyik ilyen terület a kockázatelemzés a másik pedig az incidenskezelés. Az IT és biztonsági vezetőkkel folytatott interjúk során kiderült, hogy az információbiztonsági szabványok kockázat alapú információbiztonság megvalósítást írnak elő – az Ibtv kockázati szinteket is meghatároz - miközben a szervezetek a működésfolytonosság érdekében végeznek szervezeti szintű kockázatelemzést. A szervezetek az IBIR kialakításakor már rendelkeznek kockázatelemzéssel, ami nem illeszkedik a szabvány vagy jogszabály előírásaihoz, így a szervezetek létrehoznak egy újabb kockázatelemzési eljárást, a meglevő mellett, ahelyett, hogy a meglévő kockázatelemzést alakítanák át úgy, hogy megfeleljen az információbiztonsági elvárásoknak is. Amellett, hogy a redundancia miatt feleslegesen emészt fel erőforrásokat, a két kockázatelemzés eredménye eltér egymástól, ami megkérdőjelezi az eredményüket.

A szervezetek az informatikai rendszerek üzemeltetése során fellépő incidenseket, IT incidenskezelési eljárások keretében oldják meg. Ezek az incidensek lehetnek leállást okozó rendszerhibák, adatsérülést okozó hibák, rendszerbiztonsági hibák stb. A személyes adatokat is kezelő vagy feldolgozó szervezetek találkozhatnak adatvédelmi incidenssel, amelyhez kivizsgálási folyamatra van szükségük. Az információbiztonsági szabványok és jogszabályok is előírják az információbiztonsági incidensek kezelését, amelyek átfedésben vannak az informatikai és adatvédelmi incidensekkel. A kutatási projektjeimben azt tapasztaltam, hogy a szervezetek

különböző egymástól független folyamatokat üzemeltetnek a különböző incidensek kivizsgálására és megoldására, miközben az incidensek többsége mindhárom rendszeren áthalad. A különböző incidenskezelési folyamatok jellemzően nem kommunikálnak egymással, így az adatáramlás lassú és késlelteti mindhárom folyamat végrehajtását.

Mind a kockázatelemzési mind pedig az incidenskezelési folyamatok esetében azt tapasztaltam, hogy a szervezetek nem mernek hozzányúlni a meglévő folyamatokhoz az optimalizálás érdekében, inkább létrehoznak egy új folyamatot, hogy teljesítsék az elvárt követelményeket.

## 3.3 Összegzés

Kutatási projektjeim során azonosítottam és általánosítottam a vizsgált szervezetekben előforduló információbiztonsági hiányosságokat. Ezek első látásra az IBIR végrehajtásával és betartásával állnak kapcsolatban és alkalmazhatósági problémáknak tűnnek. A problémák előfordulásának okait vizsgálva kiderült, hogy olyan tünetekről van szó, amelyeket az IBIR létrehozása során elkövetett hibák okoznak, odafigyeléssel és módszertannal kiküszöbölhetők a bevezetés során. Megállapítottam, hogy a felmerülő problémák besorolhatók strukturális, értelmezhetőségi, megfelelési, alkalmazhatósági és redundancia csoportokba [108].

Elkészítettem a problémák előfordulásának statisztikáját a vizsgált szervezetekre nézve. Kiderült, hogy minden problémacsoport minden szervezetben előfordult azok méretétől és tevékenységétől függetlenül.

**A kutatási tevékenységem alapján igazoltnak tekintem a H1. hipotézist, mely szerint a szervezetek információbiztonsági állapotát befolyásoló tényezők függetlenek a szervezet tevékenységétől és méretétől.**

# 4 EREDMÉNYES IBIR MODELL

## 4.1 Információbiztonsági infrastruktúra felépítése

A szervezetek információbiztonságának felépítése és fenntartása 3 fontos tényezőből tevődik össze. Ezek kiépítése és együttműködése határozza meg a szervezet információbiztonságának színvonalát. Az első komponens az információbiztonság szabályozása, azaz az IBIR kialakítása, amely felel a jogszabályi és szabvány megfelelések biztosításáért, a második komponens az IBIR-ben megfogalmazott követelmények megvalósítása, a harmadik komponens pedig a folyamatos nyomon követés és fenntartás.

A 3. fejezetben arra kerestem a választ, hogy milyen információbiztonsági hiányosságok fordulnak elő a szervezetekben és azok milyen okokra vezethetők vissza. A hiányosságok megszüntetése eredményes IBIR megvalósítását teszi lehetővé. A hiányosságok és problémák okainak feltárása segít elkerülni azokat az IBIR kialakítás és felülvizsgálat során elkövetett hibákat, amelyek az információbiztonsági hiányosságokat okozzák.

A saját IBIR modellem kialakítását a szabályzathierarchia megtervezésével kezdtem. Ezt követte a struktúra felépítése, amelyet a 1.3 és 2.1 fejezetek elméleti kutatásai alapján állítottam össze. A modellalkotás harmadik fázisa a megalkotott modell tökéletesítése megalapozott elmélet módszertan alkalmazásával a projektről-projektre feltárt hiányosságok kiküszöbölésével.

Ezt követően készítettem egy bevezetési és felülvizsgálati folyamatot, amelyet beépítettem a modellbe, hogy kiküszöböljem a bevezetés és felülvizsgálat során tapasztalt hibákat.

## 4.2 Az IBIR hierarchia alapelvei

A konzisztens IBIR kialakításához szükség van egy olyan dokumentum hierarchiára, amely egyértelműen meghatározza a szabályzatok egymáshoz viszonyított helyét az IBIR-ben. Ez a hierarchia független az IBIR alapjául választott szabványoktól és keretrendszerektől. A hierarchia egyes szintjein elhelyezkedő dokumentumok a felettük lévő szinten található dokumentumok alá tartoznak, a hierarchia valójában egy fastruktúrát ír le, amely illeszkedik a szervezet Szervezeti és Működési Szabályzatához. Az IBIR szabályzatokat tartalmazó dokumentum hierarchiát a 5-ös ábra mutatja be. Az ábrán jól látható az egyes szintek egymásra épülése.


*5. ábra Az IBIR dokumentumainak hierarchiába szervezése (saját szerkesztés)*

A **Stratégiai szint** globális, a szervezet minden dolgozójára érvényes és minden dolgozója által betartandó irányelvekből és szabályzatokból áll, ami közvetlenül van alárendelve a Szervezeti és Működési Szabályzatnak. Ez tartalmazza az **Információbiztonsági Politikát (IBP)**, amely megnevezi az alkalmazandó jogszabályokat, szabványokat és keretrendszereket, melyek mentén a szervezet kialakítja az információbiztonságot; az **Információbiztonsági Stratégiát és Irányelveket (ISI)**, amelyek meghatározzak az információbiztonság kialakításának és fenntartásának módját, szabályait és eljárásrendjét és az ezekre épülő általános **Informatikai Biztonsági Szabályzatot (IBSZ)**. Az általános IBSZ keretbe foglalja a teljes információbiztonsági szabályozási rendszer struktúráját, beleértve a szabályozási térképet, amely leírja a hierarchia második szintjén található összes információbiztonsági szabályzatot és eljárásrendet. Általános mindenkire érvényes szabályokat és biztonsági követelményrendszert tartalmaz, amely betartása kötelező érvényű a szervezet minden munkatársa számára; definiálja az IBIR általános fogalomtárát és az IBIR kialakításához és fenntartásához szükséges szerepköröket. Mellékletei tartalmazzák a szerepkörök összerendelését a szervezetben kialakított munkakörökkel és az IBIR elemeihez kapcsolódó szabvány és jogszabály hivatkozásokat.

A **Szabályzatok és eljárásrendek** csoport szintű szabályzatok és eljárásrendek, amelyek a megnevezett divízióra, osztályra vagy munkacsoportra vonatkoznak. Minden szabályzaton és eljárásrenden fel van tüntetve annak bizalmassági szintje, hogy kikre vonatkozik és kik ismerhetik meg. Hivatkozik az IBSZ érintett fejezeteire és minden más érintett szabályzatra. A szabályzatok előírják az érintettek által betartandó szabályokat. Az eljárásrendek tartalmazzák a vonatkozó munkafolyamatok leírását RACI (felelősségi körök: felelős, szamon kérhető, közreműködő, informált) mátrixos formátumban, feltüntetve a munkafolyamatok lépéseiben betartandó információbiztonsági előírásokat.

**Operatív szabályzatok és dokumentumok**: megadott rendszerre vonatkozó rendszer szintű dokumentáció, amelyek szabványosított sablonokra épülnek. Ezek közé tartoznak: a rendszerdokumentációk, a rendszer szintű speciális munkafolyamatok, feladatok végrehajtását igazoló dokumentumok, mint például: munkalapok, hibajegyek, változáskérelmek, ellenőrzési listák, telepítési naplók stb.

A hierarchia egyes szintjein elhelyezkedő dokumentumoknak ki kell elégíteniük az általuk hivatkozott magasabb szinten található dokumentumokban megfogalmazott követelményeket.

## 4.3 IBIR alapmodell hierarchikus struktúrája

A szabályzatok és eljárásrendek elkészítésekor mindig a legerősebb jogszabályi vagy szabvány előírást kell követni, amelyet ki kell egészíteni a szervezetre érvényes további jogszabály és bevezetni kívánt szabvány követelményeivel, így biztosított lesz mind a jogszabályi mind pedig a szabvány megfelelés. A kutatások megkezdése előtt ITIL alapú IT szolgáltatásmenedzsment bevezetéssel is foglalkoztam, amelynek során több esetben találkoztam Ibtv és ISO/IEC 27001 alapú információbiztonsági előírással. Ez ihlette azt a gondolatot, hogy dolgozzam össze azt IT szolgáltatásmenedzsment rendszer munkafolyamatait az ISO/IEC 27001 és Ibtv követelményeivel. Az alapmodell kialakítását a 2.2.4 fejezetben bemutatott 2-es táblázat alapján végeztem el. Az eredmény a hivatkozott jogszabályok és szabványok összes követelményének szakterületek mentén való összefésülése során előállított általános és teljes körű fastruktúrába rendezett információbiztonsági követelményhalmaz. Ez az alapja a kutatási projektjeim során, projektről-projektre haladva egyre részletesebben kidolgozott és a gyakorlatban kipróbált IBIR struktúrának.

Azon információbiztonsági követelmények esetében, amelyek IT fejlesztési, illetve üzemeltetési témakörökre vonatkozhatnak, azonosítani kell a szervezet érintett IT működési folyamatait. Amennyiben professzionális IT szolgáltatásnyújtás és a későbbiekben akár ISO/IEC 20000 szabvány szerinti tanúsítás is cél, a biztonsági követelményekkel párhuzamosan az ITIL ajánlásait

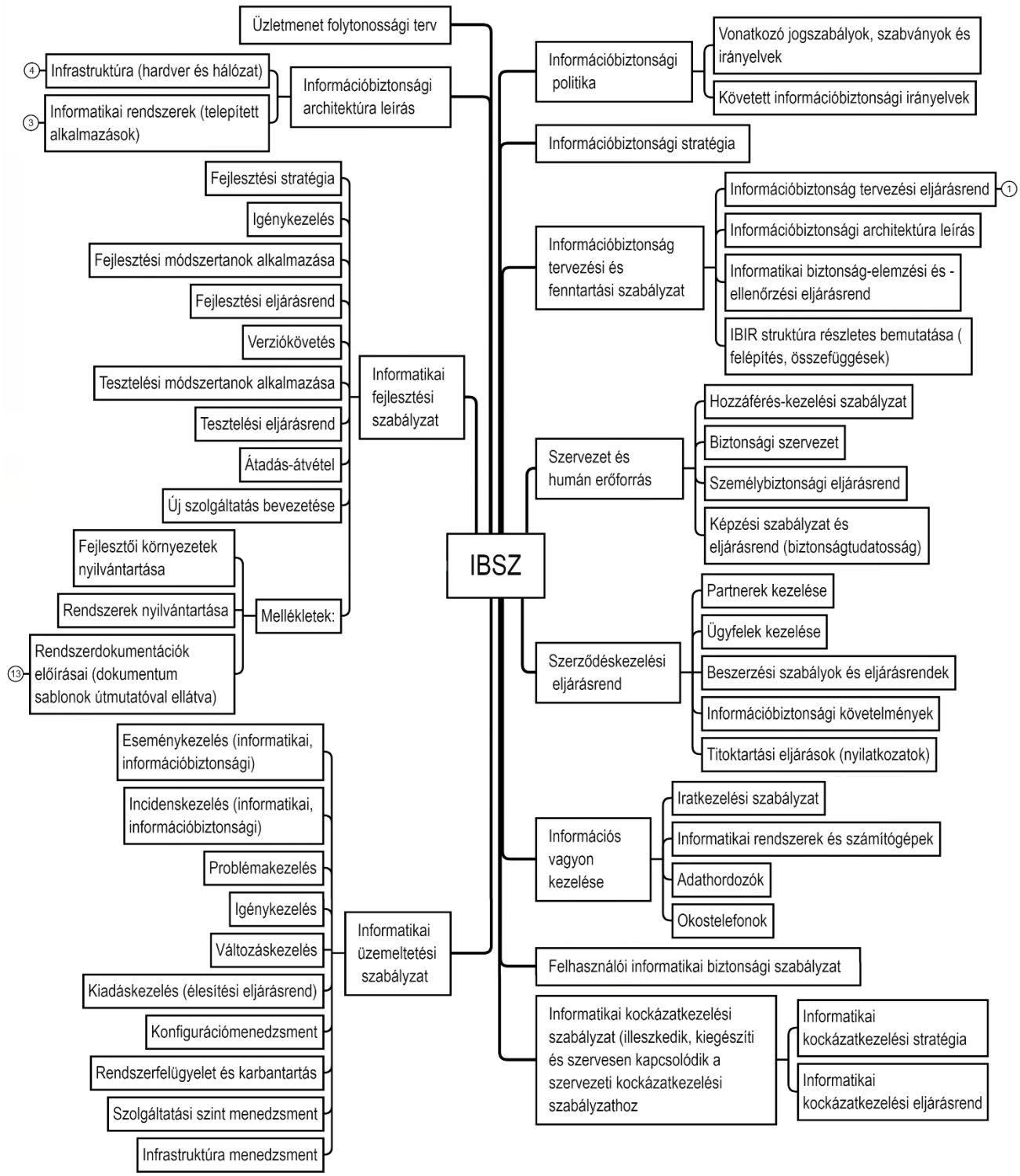
is be kell építeni ezekbe a munkafolyamatokba. Ugyanakkor minden szervezet rendelkezik IT munkafolyamatokkal, amelyek ITIL alapokra helyezése javítja az IT működését miközben optimalizálja az informatikai költségeket. Éppen ezért ITIL oldalról közelítettem meg az IT szervezetek információbiztonsági kérdését is, amely önmaga is tárgyalja az információbiztonságot és az ISO/IEC 27001 szabványhoz hasonlóan definiálja az „Információbiztonság menedzsment" folyamatot a szolgáltatás tervezés életciklus szakaszban [51]. Akárcsak az Ibtv, BMr és ISO/IEC 27001 ez is megköveteli az információbiztonsági politika, tervek, kontrollok létrehozását, implementálását, dokumentálását és üzleti elvárásokhoz való igazítását, továbbá az információbiztonsági incidensek és problémák kezelését. Mint legjobb gyakorlat, javasolja az információbiztonság integrálását a szervezet IT szolgáltatásmenedzsment folyamataiba, amelyeket nevezhetünk IT munkafolyamatoknak is [66].

Az IT munkafolyamatok rendszerint két nagy területre fókuszálnak, az IT rendszerek fejlesztése és üzemeltetése. Mivel minden információbiztonsági szabvány kiemeli a fejlesztés és üzemeltetés szétválasztását, az IT munkafolyamatokat két nagy szabályzatba csoportosítottam, és kiegészítettem a vonatkozó információbiztonsági jogszabályok és szabványok követelményeivel. Ennek megfelelően az IT rendszerekhez és munkafolyamatokhoz kapcsolódó biztonsági követelmények és eljárások az Informatikai Fejlesztési Szabályzatba és az IT Üzemeltetési Szabályzatba kerültek.

Az emberi erőforrásokkal kapcsolatos információbiztonsági szabályokat integrálni kell a szervezet humán erőforrás gazdálkodási szabályzatába és munkafolyamataiba, hiszen ide tartoznak a képzési és személybiztonsági kérdések.

A bemutatott struktúra nem tér ki a követelménycsoportok teljes részletezettségére, csak a szakterületek első szintű kibontására, de így is jól szemlélteti a követelménycsoportok hierarchiájának szakterületekre bontott struktúráját. Az alapmodell nem tér ki a hierarchia szabályzatokra való bontására. Az IBIR alapmodell egy fastruktúra, amelyben az IBIR hierarchia egymásra épülésének alapelveit követve az információbiztonsági követelményeket szakterületenként csoportosítottam. A követelmények csoportosítása lehetőséget nyújt azok szakterületek mentén történő szabályzatokra bontására.

A kialakított IBIR alapmodell hierarchikus struktúráját a 6-os ábra mutatja be.




*6. ábra IBIR alapmodell (saját szerkesztés)*

Az **IBSZ** általános, a szervezet minden munkavállalója számára kötelező érvényű információbiztonsági követelményeket tartalmaz, továbbá meghivatkozza a szakterületek szabályzatait és azok alkalmazásának követelményeit.

A szabályzat folyamatos fejlesztését és karbantartását az IBIR keretrendszer biztosítja, amely tartalmazza a szabályzatok összefüggésrendszerét, naprakészen tartását, alkalmazásának kereteit. Az „**Információbiztonság tervezési és fenntartási szabályzat**” „**IBIR struktúra részletes bemutatása (felépítés, összefüggések)**” fejezete mutatja be a szervezetben kialakított szabályzatrendszer felépítését.

A modell követelményrendszerének egyik legfontosabb eleme az „**Információbiztonság tervezési és fenntartási szabályzat**” „**Információbiztonság tervezési eljárásrend**” fejezete, amely részletesen taglalja az IBIR kialakításának munkafolyamatát és rögzíti a szabályzatrendszer minőségi megvalósításához szükséges feltételeket, szabályokat és eljárásokat. Az IBIR minőségét és végrehajthatóságát biztosító szabályok, univerzális, szervezeteken átnyúló irányelvek betartatását biztosítják.

Kutatásaim során a 3. fejezetben bemutatott IBIR hiányosságok vizsgálatának összesítésekor arra a következtetésre jutottam, hogy az IBIR rendszerek hiányosságait jellemzően strukturális, érthetőségi, megfelelőségi és redundancia problémák, amelyeket nem a szakmai háttértudás hiánya, hanem a kialakítás során alkalmazott módszerek és eljárások, valamint a felépített szabályzatrendszer szerkezetének hiányosságai okoznak. Ez adja az alapötletet, hogy az információbiztonság tervezési eljárásrendbe olyan szabályokat építsek be, amelyek biztosítják a rendszer konzisztenciáját, a szabályzatok értelmezhetőségét és alkalmazhatóságát. Az IBIR üzleti és jogszabályi környezetnek való megfelelését az alapmodell tartalmazza a szabványok és jogszabályok követelményeinek összefésülésével.

## 4.4 Szabályzatok hatókörének kialakítása

Alaposan szemügyre véve a jogszabályok és vonatkozó szabványok struktúráját megfigyelhetjük, hogy az információbiztonsági követelményeket témakörönként fejezetekbe csoportosítják, sőt sok esetben előírják, hogy egy-egy fejezet tartalma szabályzatot alkosson. Vannak jogszabályok és szabványok, amelyek elaprózzák a követelményeket és túl sok szabályzat létrehozását követelik meg, miközben mások túl magas szinten csoportosítják a követelményeket.

Mindkét követelmény csoportosításnak megvan a maga előnye és hátránya. Ha túl sokfelé osztjuk a követelményeket sok kis méretű szabályzattal találjuk szembe magunkat, ez lehetővé teszi a szabályzatok szerepkörökhöz rendelését – ezáltal biztosítva a bizalmassági kritérium teljesülését, ugyanakkor a szabályzatok közötti sok hivatkozás miatt bonyolulttá teszi a szabályzatok összefüggésrendszerét és megnehezíti az IBIR konzisztensen tartását is, miközben az érintetteknek nyomon kell követni az összes szabályzat és eljárásrend frissítését, naprakész

információval kell rendelkezni azok tartalmát illetően. Ha túl magasszintű a biztonsági követelmények csoportosítása, akkor egyszerű lesz az IBIR struktúra, de ellehetetlenül a biztonsági követelmények megfelelő szerepkörökhöz rendelése, azaz vagy több vagy kevesebb követelmény ismerete és betartása vonatkozik az érintettekre.

Jellemzően a szervezetek méretének növekedésével nő azok komplexitása is, egyre széttagoltabbak lesznek a szervezeti egységek és ezzel párhuzamosan egyre specifikusabb feladatokat látnak el. Ez azt is jelenti, hogy az egyes szervezeti egységeknek egyre specifikusabb szabályzatokat és eljárásrendeket kell betartaniuk. Mivel az információbiztonsági szabályok akkor működnek jól, ha beépülnek a szervezet munkafolyamataiba, az IBIR struktúráját (a szabályzatok széttagoltságát) hozzá kell igazítani a szervezet komplexitásához és struktúrájához. Ugyanakkor figyelembe kell venni, hogy a vezetők sok esetben hajlamosak a szervezet struktúrájának véget nem érő átalakítására, ami megnehezítheti a szabályzatok alkalmazását és naprakészen tartását. Például egy 10 fős informatikai osztály esetében nincs értelme elaprózni a szabályzatokat, hiszen a dolgozók többsége ugyanabban a fejlesztői vagy üzemeltetői szerepkörben hasonló feladatot lát el, így ugyanazok a szabályok vonatkoznak rájuk, tehát elegendő egy fejlesztési és egy üzemeltetési szabályzat létrehozása. Ha egy olyan szervezettel találkozunk, ahol külön osztály foglalkozik a hibabejelentésekkel és azok elhárításának koordinálásával továbbá az infrastruktúra, alkalmazás, hálózat és irodai eszköz üzemeltetési feladatok külön munkacsoportokhoz tartoznak, akkor érdemes elgondolkodni a szabályzatok tovább bontásáról, hiszen az egyes munkacsoportok más-más feladatokat és munkafolyamatokat hajtanak végre, más és más biztonsági követelmények vonatkoznak rájuk és az általuk végrehajtott tevékenységekre.

A kutatási projektjeim során találkoztam, a szervezet méretéhez képest elaprózott és túl magas szintű információbiztonsági szabályozással is, kijelenthető, hogy egyik esetben sem sikerült a szervezetnek elérni az általuk kívánt biztonsági szintet. Ugyanakkor az interjúk alatt gyűjtött információ elemzésekor arra a következtetésre jutottam, hogy gyakran változó struktúrájú szervezet esetén, a biztonsági követelményeket a szervezet struktúrájához képest magasabb szintű csoportosítás mentén kell szabályzatokba foglalni, hogy a szervezet változásai kevésbé befolyásolhassák azok végrehajtását, de így sincs garancia arra, hogy a változások ne lehetetlenítsék el a biztonsági szabályzatok követelményeinek végrehajtását.

## 4.5 Azonosított problémák kiküszöbölése

Az információbiztonsági hiányosságok vizsgálata során strukturális, értelmezhetőségi, megfelelési, alkalmazhatósági és redundancia problémákat azonosítottam. IBIR létrehozásakor ezek elkerülése, felülvizsgálatakor pedig kiküszöbölése a cél.

**Strukturális problémák kiküszöbölése**

A nem releváns tartalom jellemzően olyan szövegrészeket takar, amelyek nem határoznak meg biztonsági követelményeket. Ilyen tartalmak például: módszertanok, jogszabályok és szabványok bemásolt szövege. Az idézésnél sokkal jobb módszer a jogszabályra, szabványra és módszertanokra, való hivatkozás, hiszen azok követelményeit egyébként is teljesíteniük kell a szervezetnek. Azokon a helyeken, ahol az idézett szöveg szerepelne, annak alkalmazási módját és a végrehajtásában érintett szerepköröket kell beépíteni a szabályzatba.

A túlméretezett szabályzatok jellemzően több szakterületet fednek le, illetve tartalmaznak nem releváns részeket a hatókörre nézve. Ez esetben tisztázni kell a szakterületek hatókörét és hozzá kell igazítani a szervezeti struktúrához és szerepkörökhöz. A hatókörre nem releváns tartalmat el kell távolítani, amennyiben követelményeket fogalmaz meg, be kell építeni a vonatkozó szabályzatba.

A szabályzathierarchia hiányosságait olyan anomáliák alkotják, mint például a nem létező szabályzatokra való hivatkozások, hibás hivatkozások, a 4.2-es fejezetben bemutatott alapelvek megsértése, a szervezet struktúrájától eltérő szabályzati hatókörök kialakítása és a követelmények rossz csoportosítása. Ezek kiküszöbölését a 4.2-es fejezetben bemutatott alapelvek betartása és a 4.4-es fejezetben bemutatott szabályzati hatókör kialakítási logika biztosítja.

A strukturális problémák kiküszöbölésére a következő feladatokat és követelményeket építettem be az Információbiztonság tervezési és fenntartási szabályzatba:

1. Szabályzat katalógus kialakítása.
2. Szabályzatok hatókörének és terjedelmének rögzítése és karbantartása a katalógusban.
3. Szabályzatok hatókörének és terjedelmének igazítása a szervezet struktúrájához.
4. Követelmények csoportosítása szakterületenként és témakörönként.
5. Dokumentumok közötti kapcsolati térkép rögzítése a katalógusban.
6. Minden követelmény egy szabályzatban szerepel, más szabályzatok csak hivatkoznak rá.
7. A szabályzatok követelményeket fogalmaznak meg.
8. Az eljárásrendek munkafolyamatokat írnak le.

9. A folyamatok leírása folyamatábra és RACI mátrix együttes alkalmazásával történik.
10. Minden folyamatnak és folyamatlépésnek van felelőse.
11. Az igazoló dokumentumok a munka elvégzését, szabályok betartását rögzítik.

Az IBIR struktúrának illeszkednie kell a szervezet felépítéséhez és működéséhez. Ennek megfelelően össze kell hangolni a szervezet struktúrájával és működési szabályzataival. Ezt a legkönnyebben úgy tudtam elérni, hogy az IBIR-ben alkalmazott információbiztonsági szerepköröket leképeztem a szervezet működési folyamataihoz kialakított szerepkörökre, erre a célra létrehoztam egy mellékletet az IBSZ-ben.

A kutatási projektekben szerzett tapasztalataim alapján a szervezetek IBIR-rel szemben támasztott követelményei függenek a szervezet méretétől, a kezelt adatok minőségétől és a gazdasági szektortól. Minél nagyobb egy szervezet annál több szervezeti egységből áll, több munkafolyamatot hajt végre és több adatot kezel. Ennek következtében a szervezet szabályzatrendszere is egyre nagyobbá és bonyolultabbá válik, ami egyre részletesebb IBIR kialakítását teszi szükségessé. Ilyen esetekben nő a szabályzatok száma. Minél kisebb egy szervezet annál kevesebb szervezeti egységből áll, kevesebb munkafolyamatot hajt végre és jellemzően kevesebb adatot kezel. Ennek következtében a szervezet szabályzatrendszere is egyszerűvé válik, ami egyszerűbb és hatékonyabb IBIR kialakítást igényel.

**Érthetőségi és értelmezhetőségi problémák kiküszöbölése**

Az érthetőségi és értelmezhetőségi problémákat az átlagfelhasználó számára idegen kifejezések, a szakzsargon és a rövidítések ismeretének hiánya okozza. Fontos megemlíteni, hogy az egyre nagyobb információbiztonsági fenyegetések ellenére sem várható el az átlagfelhasználótól ezek ismerete. A kutatási projektek keretében folytatott interjúk az IT és információbiztonsági vezetőkkel, rámutattak arra, hogy kerülni kell az idegen szakkifejezések használatát a szabályzatokban. Ha mégis szükség van egy-egy kifejezésre akkor azt definiálni kell a fogalomtárban. Ugyanez érvényes a rövidítésekre. Egy IT végzettségű kollegánk, amikor egy információbiztonsági publikációt olvasott megjegyezte, hogy annyira tele van rövidítésekkel és szakzsargonnal, hogy sokat kellett szótáraznia és rövidítéseket böngésznie mire megértette a cikk lényegét. Ez utóbbi kijelentés irányította rá a figyelmemet arra, hogy a szakkifejezéseket és rövidítéseket a szövegben el kell látni a definíciójukra mutató hivatkozással.

Annak érdekben, hogy a szabályzatok könnyen érthetők és értelmezhetők legyenek, követelményeket építettem be az Információbiztonság tervezési és fenntartási szabályzatba:

1. Minden rövidítésnek szerepelnie kell az IBIR fogalomtárában.
2. Minden szakkifejezésnek szerepelnie kell az IBIR fogalomtárában.
3. Az IBIR szabályzataiban szereplő szakkifejezéseket és rövidítéseket a fogalomtárban szereplő definíciójukra mutató hivatkozással kell ellátni.
4. IBIR szinten egy fogalomtár építhető, minden szabályzat és eljárásrend abban definiálja a fogalmakat és rövidítéseket.

**Megfelelőségi problémák kiküszöbölése**

Az IBIR alapmodell megtervezésekor, nagy figyelmet fordítottam a jogszabályi és szabvány megfelelésre. Az alapmodellbe beépítettem a legfontosabb szabványok és jogszabályok követelményeit, de ez nem jelenti azt, hogy nem jelennek meg további követelmények. Ilyen követelmények származhatnak szabványok frissítéséből, új információbiztonsági vagy a gazdasági szektorra vonatkozó jogszabályok megjelenésével stb. Ezen helyzetek kezelésére az Információbiztonság tervezési és fenntartási szabályzatba építettem be követelményeket és tevékenységeket:

1. Szisztematikus tervezés, top-down megközelítéssel, a teljesség érdekében.
2. Üzleti folyamatok követelményeiből származó információbiztonsági követelmények beépítése a szabályzatokba.
3. Iparági és információbiztonsági szabványokból származó követelmények beépítése a szabályzatokba, átfedések azonosításával és egyesítésével.
4. Jogszabályokból és végrehajtási rendeletekből származó követelmények beépítése a szabályzatokba, átfedések azonosításával és egyesítésével.

**Alkalmazhatósági problémák kiküszöbölése**

Az információbiztonság irányítási rendszerek akkor működnek jól, ha az információbiztonsági szabályzatok konzisztensek egymással és szervesen beépülnek a szervezet működésébe. A közös szabályrendszer kidolgozását követően az elkészített szabályzatok követelményeit be kell építeni a szervezet mindennapi munkafolyamataiba. Ezt egy módon lehet elérni, ha a szervezet aktívan részt vesz az IBIR kidolgozásában. Ennek koordinálására a legalkalmasabb személy a szervezetben elfoglalt pozíciójánál fogva az Informatikai/Információbiztonsági vezető, aki szükség szerinti mértékben vonja be a különböző szakterületek képviselőit a szabályzatok kidolgozásába.

Az IBIR belső konzisztenciájának és szervezeti struktúrához való illesztésének érdekében követelményeket építettem be az Információbiztonság tervezési és fenntartási szabályzatba:

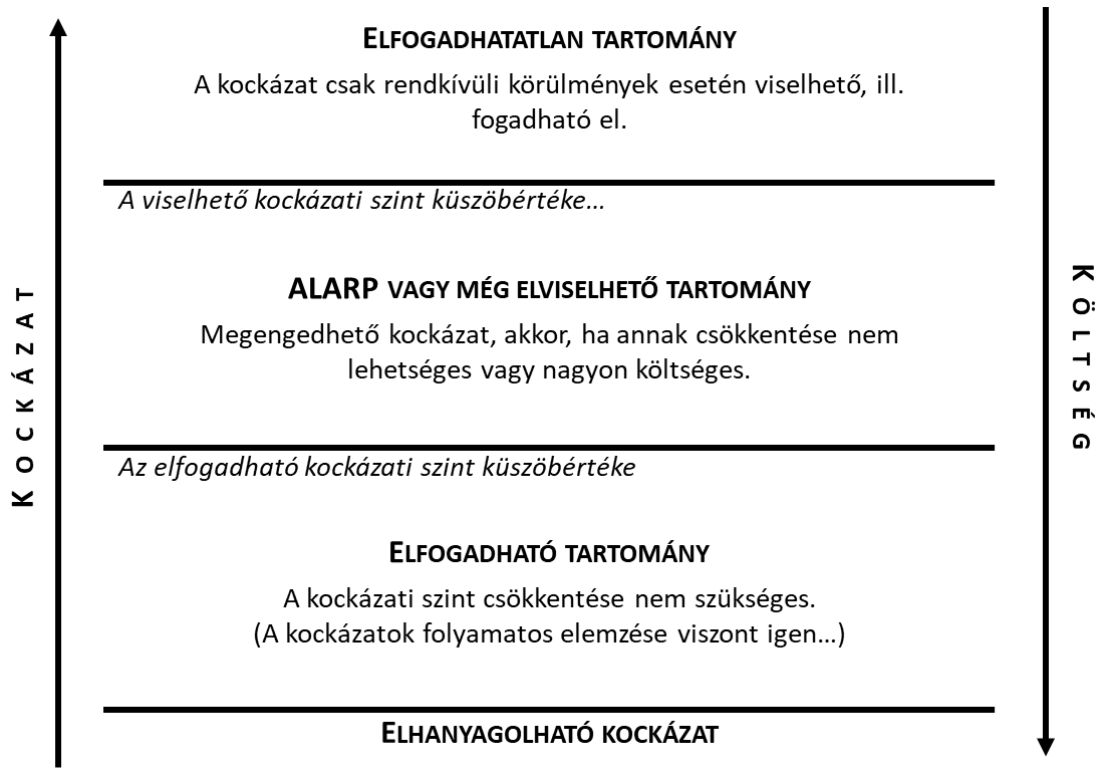
1. A szabályzatok hatóköre egyértelmű, nem fordulhat elő, hogy ugyanazt a kontrollt két szabályzat definiálja.
2. Nem definiálható olyan követelmény, amely ütközik az üzleti folyamatok végrehajtásával, ilyenkor meg kell keresni a módját az ütközések feloldásának és kontrollt kell beépíteni a munkafolyamatba a biztonsági követelmény megvalósulásához.

Az alkalmazhatósági problémák feltárásánál szó esett még a felelősségről és az egyensúlyozásról a biztonság és az üzleti érdekek között. Itt arról van szó, hogy a szervezet pénzügyi és emberi erőforrásai nem mindig állnak rendelkezésre a technológiai információbiztonsági kontrollok megvalósításához.

Az információbiztonság kialakításának fontos eleme a kockázatelemzés. Mind az ISO/IEC 27001 és NIST SP 800-53 szabványok, a COBIT és ITIL keretrendszerek, valamint az információbiztonságot előíró Ibtv és technológiai végrehajtási rendelete a BMr kiemelik az információbiztonság kockázatalapú megvalósítását.

Mivel napjainkban az információ jelentős részének tárolása és feldolgozása IT rendszerekben történik, az információbiztonsági kockázatok között kiemelt helyet foglal el az információbiztonsági intézkedések és kontrollok megvalósulása az IT rendszerekben. Azizi és Hashim kiemeli, hogy a kockázatelemzés fontos eleme a vállalati szintű menedzsmentnek és egy modern vállalat esetében ennek kulcseleme az IT kockázatelemzés. Feltárja a szervezet és IT számára elérhető szabványokat és keretrendszereket, többek között az ITIL legjobb gyakorlatot, COBIT keretrendszert és az IBIR-t mint az információbiztonság kulcselemét [109]. A kockázatokat a következő kategóriába sorolja, amelyeket további csoportokra bont: infrastruktúra és fejlesztés támogatás; üzleti folyamatok üzemeltetése és karbantartása; irodai informatikai támogatás; szoftverfejlesztés; kiszervezés menedzsment.

A Michelberger Pállal közösen írt folyóiratcikkünkben elemeztük az információbiztonság hatását az üzleti folyamatokra. Az üzleti kockázatok között szerepel az információ sértetlensége és rendelkezésre állása, amely sok esetben előfeltétele az üzleti folyamatok végrehajtásának. Az információ hiánya (ha nem áll rendelkezésre) munkafolyamatok leállásához, a hibás információ pedig hiányos vagy hibás termékek előállításához vezethet [19]. Tehát az információbiztonság kulcsszerepet játszik a szervezet működésében és alacsonyan kell tartani, amennyire csak lehet az információbiztonsági kockázatokat. Jó kiindulási pont lehet ehhez a műszaki területeken ismert és alkalmazott alapelv az ALARP (As Low As Reasonably Practicable), amelyet a 7-es ábra mutat be.




*7. ábra ALARP alapelv [110]*

Jó gyakorlat az, hogy az adott területre fókuszálva a szervezet az erőforrások rendelkezésre állásának függvényében fokozatosan egyre erősebb kockázatcsökkentő kontrollokat vezet be. Itt érdemes megemlíteni a felsővezetők felelősségét, hogy hol húzzák meg a szervezet kockázati éhségét, a kockázatelemzők és belső ellenőrök felelősségét, hogy valós képet adjanak a szervezet biztonsági állapotáról az elvárthoz képest.

A helyes aranyközépút megtalálására nincs garancia, mégis szükség van olyan követelmény megfogalmazására, amely elősegíti az ALARP alapelv szerinti kockázati szint meghatározását. Ennek érdekében két követelményt építettem be az Információbiztonság tervezési és fenntartási szabályzatba:

1. Ha üzleti érdek és biztonsági követelmény megvalósítása között kell dönteni az információbiztonsági vezető alternatív követelményeket fogalmaz meg a kockázat csökkentésére, amelyek hatását bemutatja a szervezet döntéshozóinak.
2. Ha üzleti érdek és biztonsági követelmény megvalósítása között kell dönteni és az információbiztonsági vezető alternatív követelményeket mutat be a szervezet döntéshozói meghatározzák azt a kockázati szintet, amelyet a szervezet vállalhat és ennek tükrében építik be a követelményt az IBIR-be és valósítják meg a hozzá tartozó kontrollokat.

### Redundanciák kiküszöbölése

Az IBIR problémák között azonosítottam a szervezetben előforduló, különböző szinteken vagy csoportok által párhuzamosan végrehajtott folyamatokat. Két olyan információbiztonságot direkt módon érintő munkafolyamatot sikerült azonosítani, amely több szervezet esetében is redundánsan fordult elő. Ezek a kockázatelemzés és az incidenskezelés.

Amikor közelebbről megvizsgáltam a kockázatelemzést a különböző szervezetek esetében, kiderült, hogy már rendelkeznek egy az általános szervezeti szintű kockázatelemzési és kockázatkezelési folyamattal, amely átfedésben van az ISO/IEC 27001 és az Ibtv előírásainak betartásához létrehozott kockázatelemzési és kezelési eljárásrenddel. Amikor jeleztem a szervezetek felé, az első kérésük volt az érintett szabályzatok összefésülése és egységesítése. Első lépésként a kockázatok nagyságrendi mértékét és a kockázati besorolásokat kellett egységesíteni, ezt követte a kockázatkezelési módszertanok egységesítése.

Az incidenskezelési munkafolyamatok esetében nem volt ennyire egyszerű a helyzet. Első körben fel kellett mérni a szervezetek különböző munkacsoportjai által végzet incidenskezelési munkafolyamatokat, elemezni kellett az incidensek azonosítása és kezelése során elvégzett feladatokat, a kezelt incidensek típusait, majd ezt követően kezdhettem el a munkafolyamatok egységesítést, amelynek eredménye az 5. fejezetben olvasható.

A redundanciák megtalálásához és kiküszöböléséhez két fontos feladatot azonosítottam, amelyeket az Információbiztonság tervezési és fenntartási szabályzatba építettem be:

1. Szervezeti munkafolyamatok áttekintése, IBIR által előírt munkafolyamatok azonosítása.
2. Azonosított munkafolyamat kiegészítése az IBIR követelményeinek megfelelően.

Ezen feladatok végrehajtása nehézségekbe ütközhet, mert együtt kell működni az azonosított munkafolyamatok felelőseivel, sok esetben pedig meg is kell győzni őket arról, hogy ez hosszú távon megkönnyíti a munkájukat és konfliktushelyzeteket szüntet meg.

### Információbiztonság fenntartása és fejlesztése

Az információbiztonság megvalósítása nem egy egyszeri feladat a szervezetek életében. A vizsgált jogszabályok és szabványok előírják a szabályzatok rendszeres felülvizsgálatát. Ezeket a követelményeket az Információbiztonság tervezési és fenntartási szabályzatba foglaltam bele, továbbá a szervezeti és informatikai változáskezelési folyamatokba kockázatelemzési követelményeket helyeztem el.

## 4.6 Összegzés

IBIR modellem megalkotását a szabályzati hierarchia szintjeinek meghatározásával kezdtem, amelyek: stratégiai és globális szint, szabályzatok és eljárásrendek, operatív szabályzatok és dokumentációk. Ezt követően összeállítottam az IBIR alapmodellt, amely szakterületenként csoportosítva és az ITIL munkafolyamatai mentén felépítve tartalmazza a NIST SP 800-53 alapú BMr és az ISO/IEC 27001 információbiztonsági követelményeinek redundanciamentes összefésülését, amelyet a 6-os ábrán láthatunk. Ezzel biztosítottam a szervezet számára szükséges információbiztonsági szint megvalósulását, jogszabályi és szabvány megfelelését. A 3. fejezetben bemutatott strukturális, értelmezhetőségi, alkalmazhatósági és redundancia problémák kiküszöbölését a modell beépített Információbiztonság tervezési és fenntartási szabályzata biztosítja. Modellem nagy előnye a hasonló IBIR modellekhez képest az ITIL alapú IT szolgáltatásmenedzsment folyamatok integrálása, a hiányosságokat kiküszöbölő beépített Információbiztonság tervezési és fenntartási szabályzat és a követelmények szakterületi bontása.

Modellemben az eredményesen működő információbiztonság irányítási rendszer paraméterei [108]:

1. illeszkedik és összhangban van a szervezet felépítésével, stratégiájával, működési folyamataival és gazdasági képességeivel;
2. szervesen kapcsolódik a szervezet IT szolgáltatásmenedzsmentjéhez;
3. teljesíti a vonatkozó jogszabályok és kiválasztott információbiztonsági szabványok követelményeit;
4. érthető és értelmezhető a munkatársak által;
5. eredményességének fenntartását a beépített Információbiztonság tervezési és fenntartási szabályzat biztosítja.

**A kutatási tevékenységem alapján igazoltnak tekintem a H2. hipotézist, mely szerint az ITIL munkafolyamatainak, a jogszabályok és szabványok követelményeinek integrálásával megépített IBIR modellem a feltárt problémák kiküszöbölésével biztosítja a szervezetek számára a szükséges szintű információbiztonságot.**

Az alapmodell követelményrendszerének csoportosított felépítése egyszerű módon teszi lehetővé annak leképezését a szakterületek mentén működő szervezeti egységekre. Ez lehetővé teszi az IBIR követelmények szakterületek mentén kialakított és szervezeti egységekhez igazított szabályzatokra és eljárásrendekre bontását [108].

**A kutatási tevékenységem alapján igazoltnak tekintem a H3. hipotézist, mely szerint csoportosíthatók úgy az IBIR követelmények, hogy a csoportok mentén létrehozott szabályzatok és eljárásrendek illeszkedjenek a szervezet struktúrájához megkönnyítve ezzel az IBIR bevezetését.**

A modell bevezetését 7 szervezetben végeztem el, annak szervezetre való testreszabásával. Ahogy a projektek során egyre több IBIR hiányossággal találkoztam, úgy építettem bele ezek kiküszöbölését a modellembe. A modellem bevezetését követő egy éven belül két szervezetben is volt hatósági vagy szabvány megfelelési ellenőrzés. A megrendelőktől kapott visszajelzések alapján a bevezetett rendszerek eredményesen védik a szervezet információt a gyakorlatban.

# 5 BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A szervezetek célja, hogy szolgáltatásokat nyújtsanak és termékeket állítsanak elő vevőiknek, ügyfeleiknek és partnereiknek. Gyártási tevékenységek során munkafolyamatokat hajtanak végre, amelyek során információt gyűjtenek, tárolnak, kezelnek szolgáltatásaikról, termékeikről, partnereikről, ügyfeleikről és vevőikről. A gyártás és szolgáltatásnyújtás során támaszkodhatnak harmadik felek szolgáltatásaira, igénybe vehetnek adatfeldolgozó szolgáltatásokat így információt cserélnek az érintettekkel és beszállítóikkal. Ezek az információk két nagy csoportba sorolhatók termék előállítással és szolgáltatás nyújtással kapcsolatos adatok és személyes adatok. Másik szempontból nézve ugyanezek az adatok lehetnek: nyilvános, bizalmas, titkos vagy szigorúan titkos adatok. Ez a két csoportosítás teljes mértékben átfedi egymást.

A 2.3 fejezetben tárgyalt folyamatvégrehajtás biztonsága érdekében a szervezetnek saját érdeke a gyártási tevékenység során előállított és felhasznált adatok integritásának és bizalmasságának megőrzése. Vannak olyan iparágak, amelyek esetében a termelés során kezelt adatok védelmét jogszabály írja elő, ilyen esetekben a szervezetnek biztosítania kell a jogszabályi környezetnek való megfelelést.

Az vevő-, ügyfél- és partner-menedzsment tevékenységek során előfordulhatnak személyes adatok, amelyek kezelését globális és lokális adatvédelmi jogszabályok írják elő.

A szervezeteknek saját üzleti érdeke az adatok védelme, hiszen azok sérülése vagy hiánya direkt módon okozhat kárt a termelésben vagy fennakadást a szolgáltatás nyújtásában, továbbá az adatok kiszivárgása előnyhöz juttathatja a konkurenciát. Ennek érdekében a szervezetek iparági és információbiztonsági szabványokra támaszkodnak.

A jogszabályok által védett adatok biztonságának sérülése jogszabálysértéssel jár, amely bírsággal vagy akár a működési licensz elvesztésével is járhat. A jogi környezet három típusú jogszabályból áll: általános információbiztonság, adatvédelem és ágazati jogszabályok. Az ágazati jogszabályok az általános információbiztonsági jogszabályokban megfogalmazott előírásokon túl további, az adott iparágra vonatkozó információbiztonsági követelményeket (pl. bankbiztonság) is tartalmazhatnak.

A szervezetek az információ védelmének érdekében az iparági környezetre vonatkozó szabványok és jogszabályok mentén információbiztonsági szabályzatokat hoznak létre, amelyek előírják az adatok megfelelő szintű védelmét. A szabályzatokat jellemzően valamely információbiztonsági szabvány vagy jogszabály mentén építik fel, amelyek együttesen alkotják az IBIR-t. Mind az

információbiztonsági jogszabályok, mind pedig az általános információbiztonsági szabványok előírják az információbiztonsági események kezelését [74]. Továbbá a jogszabályok előírhatják bizonyos információbiztonsági köztük az adatvédelmi incidensek jelentését is a hatóságok felé.

Míg az információbiztonság szerepe növekszik, és a kapcsolódó jogszabályokat folyamatosan szigorítják az információ és a személyes adatok megfelelő védelme érdekében, a szakemberek egyre több információbiztonsági eseményt fedeznek fel és hoznak nyilvánosságra. A károk minimalizálása érdekében ezek közlésére kiemelt figyelmet kell fordítaniuk a szervezeteknek.

A vállalatok általában rendelkeznek az IT-szolgáltatások incidenskezelési folyamataival, de sok esetben hiányzik a biztonsági események kezelésének megvalósítása vagy ezeket a folyamatokat egymástól függetlenül hajtják végre, anélkül, hogy bármilyen interakció is lenne közöttük.

Integrált incidenskezelési folyamatra van szükség az IT szolgáltatási és információbiztonsági incidensek gyors kivizsgálásának és elhárításának érdekében az informatikai és információbiztonsági szervezeti egységek részvételével.

## 5.1 Napjaink jellemző veszélyforrásai

A számítástechnikai eszközök elterjedése előtt az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében leginkább a fizikai védelemre és a humán biztonságra volt szükség. Napjainkban, amikor az információ egyre nagyobb részét elektronikusan, informatikai rendszerekben tárolják és dolgozzák fel, az információk biztonságát egyre több veszélyforrás fenyegeti. Ezen veszélyforrások érvényre jutását a következő tényezők befolyásolják.

**Fizikai környezet:** Ma, amikor információbiztonság keretében fizikai környezetről beszélünk első sorban az információ tárolását és feldolgozását biztosító berendezések elhelyezésére, áramellátására és működési feltételeinek biztosítására gondolunk. Ez jelenti a folyamatos működtetés feltételeinek biztosítását, amely az információ rendelkezésre állásáért felel, továbbá a berendezéseket tároló helyiségek védelmét – illetéktelen behatolók távoltartását –, ami az adatok bizalmasságának megőrzését biztosítja.

**A technológia fejlődése:** Az informatika és kommunikáció fejlődésének köszönhetően új távlatok nyíltak a szervezetek előtt. Az új lehetőségek új veszélyforrásokat is jelentenek. Ma már elképzelhetetlen a szervezetek IT rendszerek nélküli működése, ami egyre fokozódik. Az IT termékek siettetett, sokszor félkész állapotú, adott esetben részlegesen tesztelt piacra dobása egyre több sérülékenység megjelenését vonja maga után, amelyek folyamatos fenyegetést

jelentenek használóik számára. A támadók ma már nem véletlenszerűen támadják a szervezeteket, hanem céltudatosan gyűjtenek információt, kihasználják a sérülékenységeket és türelmesen kivárják a megfelelő pillanatot a támadáshoz. A biztonsági megoldásokat gyártó cégek statisztikái azt mutatják, hogy egyre több sérülékenység lát napvilágot. Ezek gyártók általi javítása sokszor hónapokba telik és az elkészült javításokat telepítés előtt a szervezeteknek tesztelniük kell, hogy meggyőződjenek arról, nem okoz problémát a saját infrastruktúrájuk működésében, mialatt folyamatosan ki vannak téve a sérülékenységek okozta veszélyforrások érvényre jutásának. A régi termékekre egyáltalán nem készülnek biztonsági frissítések, így azok felhasználói fokozott kockázatnak vannak kitéve.

**Szoftverfejlesztés:** A háromrétegű szoftvertechnológiák megjelenése, amelyek: adatbázisszerver, alkalmazásszerver és internet böngésző hármasra építenek, lehetővé teszik az alkalmazások internetböngészőn keresztüli használatát kliens szoftverek nélkül. Ezáltal lehetővé válik az adatokhoz való illetéktelen hozzáférés a böngészők sérülékenységeinek kihasználásával is. A szolgáltatás orientált architektúra, elősegítette a legacy – adott esetben biztonsági infrastruktúra nélküli - rendszerek integrálását az új rendszerekhez és bonyolult, pókhálószerű és átláthatatlan informatikai szolgáltatások kialakítását.

A The Standish Group Chaos Report alapján az informatikai projektek 16%-a sikeres, 53%-a kompromisszumokkal, a határidő és költségkeret túllépésével, valamint kevesebb funkció megvalósításával zárul, 31%-a pedig sikertelen. A szoftverfejlesztési trendeket figyelembe véve az információbiztonság sokadrangú tényező. A projektek rendszerint alultervezettek költség és határidő terén, a terjedelem meghatározásakor sokszor a nem funkcionális - köztük az információbiztonsági - követelmények beépítése marad ki [111].

Egy másik tényező a fejlesztési és projektmenedzsment módszertanok alkalmazása. Napjainkban közkedveltté váltak az agilis módszertanok, amelyek nagyobb odafigyelést igényelnek a biztonság megvalósítása érdekében [112].

**Szabályozási környezet:** A szervezetek törekednek információik védelmére, ennek érdekében előírják a titoktartási megállapodások megkötését munkavállalóikkal és partnereikkel. Az állami szervezetek jogszabályokon alapuló szervezeti és működési rend alapján végzik ügykezelési munkájukat, amelyek betartásának vizsgálatáról a belső ellenőrzés munkatársai gondoskodnak. Mivel az informatikai üzemeltetés közvetlenül nem része az ügyvitelnek, előfordul, hogy az üzemeltetés megszokáson alapul, reaktív módon, erőforrás hiányában tűzoltásszerűen működik. A szabályozási környezethez köthető veszélyforrások:

- az információbiztonsági szabályzatok és eljárásrendek nincsenek összhangban a szervezet tevékenységeivel;
- hiányoznak létfontosságú, jogszabályok által előírt szabályzatok és eljárásrendek;
- nincs dokumentálva a szabályzatok közötti összefüggésrendszer;
- túlszabályozás: a szabályzatok betartása akadályozza a munkavégzést;
- a szabályzatok követelmények helyett hosszú betarthatatlan leírásokat tartalmaznak;
- nincsenek információbiztonsági besorolási szabályok;
- beszerzési szabályok információbiztonsági hiányosságai.

**Humán erőforrás:** Az információk kezelése, feldolgozása és tárolása szorosan kapcsolódik a szervezetek munkafolyamataihoz és azok végrehajtóihoz, gyakorlatilag szinte minden dolgozót és partnert érint valamilyen szinten. Az adatokkal dolgozó személyzetnek tudatában kell lennie, hogy mely adatokhoz ki férhet hozzá, ez segít az információk bizalmasságának megőrzésében. Az illetéktelen hozzáférés, módosítás és rombolás megakadályozásához ennél többre, felhasználói biztonságtudatosságra és a munkatársak lojalitásának biztosítására is szükség van. A biztonságtudatosságot általános és vezetői szempontból kell megközelíteni. A vezetői biztonságtudatosság hiánya biztonsági funkciók kiépítésének elmaradásához vezethet, ami az egész szervezetre direkt módon hat és magas kockázatot jelent. Az általános felhasználói biztonságtudatosság körébe tartozó jelentősebb veszélyforrások: jelszavak kiszivárgása, jóhiszemű segítségnyújtás illetéktelen személyeknek, eszközök fizikai védelmének hiánya, irodai asztalon vagy képernyőn látható információk, illegális vagy feltört szoftverek telepítése, elektronikus levelezés és internethasználat szabályainak figyelmen kívül hagyása. A vétlen károkozáson túl előfordulhatnak szándékos károkozások is, például: alulfizetett munkatársak adatokat értékesítenek, kártékony kódok telepítése, amelyek adatszivárgást tesznek lehetővé vagy rombolást végeznek. A humán erőforrás veszélyeinek feltárásához elengedhetetlen eszköz a naplómenedzsment és elemzés, továbbá hatékony segítséget nyújthat a felhasználói profil alkotás [113].

**Rendszerek üzemeltetése:** Az informatikai rendszerek üzemeltetése azok beszerzésével és üzembe helyezésével kezdődik. A beszerzési szabályok információbiztonsági előírásainak hiányosságai fokozott veszélyforrást jelentenek, ugyanis itt jelennek meg először a biztonsági tényezők. Az üzemeltetésnek biztosítania kell az adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

Az informatikai rendszerek üzemeltetésében fontos szerepet játszanak a karbantartási feladatok, a rendszerfelügyelet és hibajavítások telepítése. Ezek elmaradása kiemelt kockázatot jelent a rendszerek rendelkezésre állásának biztosítására nézve. Rendszerfelügyeleti megoldások üzemeltetésének hiánya, amelyek folyamatosan követik az erőforrások kihasználtságát és működőképességét, nem várt leállásokhoz, túlterhelésekhez és ennek következtében lassulásokhoz vezethetnek. Egy másik kiemelt kockázat az elöregedett rendszerek üzemeltetése, ez az információbiztonság mindhárom alappillérét érinti.

A bizalmasság megőrzése szempontjából a biztonsági javítások és rendszerfrissítések rendszeres ellenőrzése, beszerzése, tesztelése és telepítése jelenti a legnagyobb kockázatot, de veszélyt jelentenek a partnerek karbantartást végző felügyelet nélkül hagyott munkatársai és a rendszerek gyenge pontjainak azonosítására indított sérülékenység vizsgálatok elmaradása.

**Hálózati kommunikáció:** Az informatikai rendszerek infokommunikációs hálózatokon keresztül kommunikálnak egymással és felhasználóikkal. Jóllehet mára fejlett hálózatvédelmi technológiák állnak rendelkezésre, de ettől függetlenül még mindig kihívást jelent az infokommunikációs hálózatok biztonságának megvalósítása. A munkavégzés folyamatossága és az adatok elérhetősége érdekében a hálózati forgalom megszakadása rendelkezésre állási kockázatot jelent, az illetéktelenek információs rendszerekhez való távoli hozzáférése bizalmassági és sértetlenségi kockázatot rejt magában. Ezen túl felmerül a rendszerek és felhasználók közötti kommunikáció bizalmasságának kérdése is mint veszélyforrás.

A technológia fejlődése, az IT rendszerek fejlesztésének és üzemeltetésének problémái, a hálózati kommunikáció veszélyforrásai, jelentős mértékben befolyásolják az információ biztonságát hiszen a szoftverfejlesztésben, rendszer és hálózat kialakításban és üzemeltetésben elkövetett hibák veszélyeztetik az adatok biztonságát. Ennek következtében a fizikai védelmi módszerek mára kevésnek bizonyulnak. Az információ bizalmasságát, sértetlenségét és rendelkezésre állását befolyásoló veszélyforrások így egyre nagyobb teret nyernek, érvényre jutásuk pedig információbiztonsági incidenseket okoz.

## 5.2 Incidensek

Általánosságban az incidensek olyan események, amelyek negatívan befolyásolják vagy befolyásolhatják a szervezetek működését vagy üzleti tevékenységét. Az incidenseket típusokba sorolhatjuk. Jelen esetben a következő incidens típusokat definiáljuk, amelyek befolyásolhatják az információbiztonságot vagy a személyes adatok védelmét: IT szolgáltatási incidens, információbiztonsági incidens, adatvédelmi incidens, biztonsági incidens.

**IT szolgáltatási incidens:** váratlan esemény, amely a szolgáltatás megszakadását vagy a szolgáltatás minőségének romlását okozza [53]. Ezt a típusú incidenst a szervezetek IT incidenseknek is nevezik.

**Információbiztonsági esemény:** ISO/IEC 27001:2005 szerint „olyan azonosított rendszer, szolgáltatás vagy hálózati állapot előfordulása, amely jelzi az információbiztonsági politika esetleges megsértését vagy védelmi megoldások meghibásodását, vagy egy ismeretlen helyzet, amely biztonság szempontjából releváns lehet" [24, p. 2].

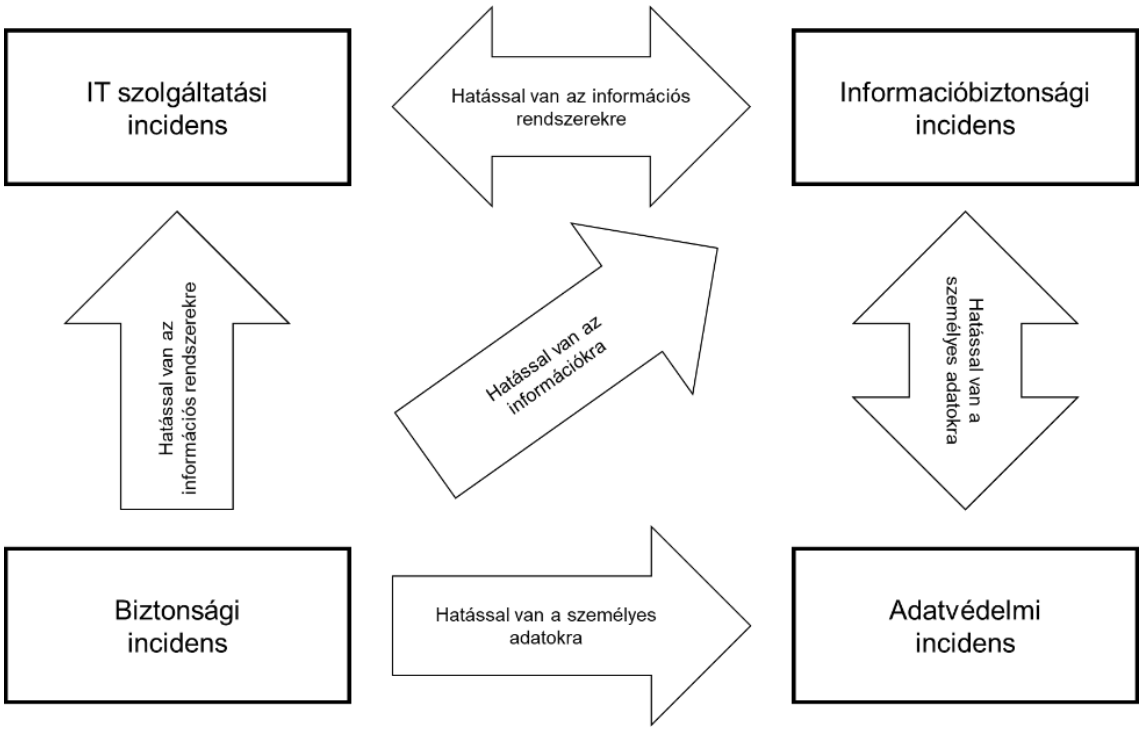
**Információbiztonsági incidens:** ISO/IEC 27001:2005 szerint "egy vagy több váratlan információbiztonsági esemény, amely nagy valószínűséggel veszélyezteti az üzleti tevékenységet és fenyegeti az információbiztonságot" [24, p. 2] [114, p. 40]. Például: a bizalmas információkhoz való illetéktelen hozzáférés, az adatok sérülése vagy jogosulatlan módosítása, az információk hozzáférhetetlensége.

**Adatvédelmi incidens:** GDPR szerint "a személyes adatok biztonságának megsértése, amely a továbbított, tárolt vagy feldolgozott személyes adatok véletlen vagy jogellenes megsemmisüléséhez, elvesztéséhez, megváltoztatásához, illetéktelen közzétételéhez vagy hozzáféréséhez vezet" [29, p. 34]. Ez azt jelenti, hogy a személyes adatokhoz kapcsolódó jogosulatlan hozzáférés, kiszivárgás, visszaélés, lopás, illetéktelen közzététel kimeríti az adatvédelmi incidens fogalmát.

**Biztonsági incidens:** váratlan biztonsági esemény, amely nagy valószínűséggel veszélyezteti az üzleti tevékenységet és a fizikai biztonságot. Ez azt jelenti, hogy az illetéktelen hozzáférés, behatolás, árvíz, értékek és dokumentumok ellopása vagy megsemmisítése, vagy egyszerűen meghiúsult biztonsági intézkedések mind biztonsági incidensnek számítanak.

## 5.3 Incidens típusok közötti összefüggések

A személyes adat az információ egy speciális előfordulása. Ez azt jelenti, hogy minden adatvédelmi incidens egyben információbiztonsági incidens is. Erről a nézőpontról elindulva definiálhatjuk a különböző incidenstípusok közötti kapcsolatot. Ezt a legjobban a 8-as ábra szemelteti, amelyen a különböző incidensek közötti összefüggéseket azonosíthatjuk.




*8. ábra Incidenstípusok közötti kapcsolatok [115]*

A **biztonsági incidens** esetén, ha bármilyen informatikai rendszer érintett akkor egyben **IT szolgáltatási incidens is**; ha bármilyen formában (elektronikus, papír alapú) előforduló információ érintett, akkor **információbiztonsági incidens** is egyben; ha személyes adatot tartalmazó dokumentum vagy információ érintett, akkor **adatvédelmi incidens** is egyben.

Az **IT szolgáltatási incidenst** okozhatja **biztonsági incidens;** a legtöbb esetben információt is érint, így **információbiztonsági incidens** is egyben.

Az **információbiztonsági incidens** esetén, ha személyes adat bizalmasságát vagy sértetlenségét érinti, akkor **adatvédelmi incidens** is egyben; ha informatikai rendszer is érintett, akkor **IT szolgáltatási incidens** is egyben.

Az **adatvédelmi incidens** egyben **információbiztonsági incidens** is, mivel a személyes adat információ. **Biztonsági incidens** is okozhat **adatvédelmi incidens**t.

## 5.4 Az incidenskezelés célja

Az incidenskezelés fő célja azonban az incidensek gyors felderítése, kivizsgálása, kezelése és elhárítása. Az incidens típusától függően az incidenskezelési folyamatok céljai minimálisan eltérnek egymástól és részben különböző tevékenységeket kell végrehajtaniuk. A különböző incidenstípusok esetében a célokat következő lista tartalmazza:

- **IT szolgáltatási incidens** esetén: az érintett információs rendszerek mielőbbi felderítése, az incidens kivizsgálása, a rendszer mielőbbi helyreállítása, a munkafolyamatok újraindítása és a veszteség minimalizálása;
- **információbiztonsági incidens** esetén: információbiztonsági esemény észlelése, okok felderítése és kivizsgálása, további információbiztonsági események megelőzése, az incidens által okozott károk minimalizálása, információk védelmének helyreállítása, szükség esetén az incidens jelentése a hatóságoknak, szükség esetén szankciók alkalmazása, felelősök felelősségre vonása;
- **adatvédelmi incidens** esetén**:** adatvédelmi esemény észlelése, okok felderítése és kivizsgálása, az adatvédelemi esemény által okozott állapot megszüntetése, károk minimalizálása, érintettek értesítése, szükség esetén az adatvédelmi incidens jelentése a hatóságoknak, szükség esetén szankciók alkalmazása, felelősök felelősségre vonása;
- **biztonsági incidens** esetén: a károk felderítése, felmérése, a további biztonsági események megelőzése, a károk minimalizálása, szükség esetén szankciók alkalmazása, felelősök felelősségre vonása.

Az, hogy a célok minimálisan eltérnek egymástól azt jelenti, hogy az eseménykezelési folyamatok is eltérnek egymástól, Mivel az észlelt incidensek adott esetben több típusba is tartoznak, kezelésük minden érintett incidenstípus elhárítási munkafolyamatát végre kell hajtani. Ez azt is jelenti, hogy átjárhatóságnak kell lennie az incidenskezelési folyamatok között, azaz függhetnek egymástól vagy támaszkodhatnak egymás eredményeire. Minden incidenskezelési folyamat esetében elérhetővé kell tenni az incidenssel kapcsolatos információkat és meg kell őrizni a rendelkezésre álló bizonyítékokat.

Az IT szolgáltatási incidensek kezeléséhez az ITIL legjobb gyakorlat ITIL Service Operation kötetében az incidenskezelési folyamat nyújt támpontot [53, pp. 72-86]. Az információbiztonsági incidensek kezeléséhez az ISO/IEC 27005 [116] és a NIST SP 800-61 szabvány [45] nyújt támpontot. Az adatvédelmi incidensek kezelése megegyezik az információbiztonsági incidensek kezelésével, de a helyi jogszabályoknak való megfelelés miatt további tevékenységek végrehajtására is szükség van. Az Európai Unióban az adatvédelmi incidensek kezelését a GDPR írja elő.

## 5.5 Az integrált incidenskezelés szükségessége

A szervezetek többsége informatikai rendszereinek üzemeltetését ITIL alapú IT szolgáltatásmenedzsment munkafolyamatokkal, köztük IT incidenskezelési folyamattal támogatja,

amelyhez IT ügyfélszolgálatot üzemeltet. Ezekben az esetekben az ügyfélszolgálat koordinálja az IT incidenskezelési folyamatot és felügyeli az incidensek szolgáltatási szint megállapodás keretében vállalt válasz és megoldási idejének betartását [53].

Az információbiztonsági jogszabályok, mint pl. az Ibtv előírják információbiztonsági vezető vagy felelős kijelölését az érintett szervezetek számára, aki az első számú vezetőnek tartozik jelentési kötelezettséggel és felelősségi körébe tartozik az információbiztonsági események/incidensek kezelése. Az információbiztonsági felelős nem lehet egyben az informatikai vezető is.

A személyes adatokat kezelő szervezetek esetében a jogszabályok pl. GDPR, Infotv előírják adatvédelmi felelős kijelölését. Az adatvédelmi incidensek kezelése az adatvédelmi felelős hatáskörébe tartozik, akiknek a hatályos jogszabályoknak megfelelően jelenteniük kell az adatvédelmi incidenseket a kijelölt hatóságnak.

Vannak szervezetek, amelyek dedikált biztonsági osztállyal vagy igazgatósággal rendelkeznek, amelynek feladata a biztonsági incidensek kezelése. Előfordulnak olyan szervezetek, amelyek esetében van dedikált információbiztonsági, illetve adatvédelmi osztály. Ezek az osztályok nem feltétlenül részei a biztonsági osztálynak vagy igazgatóságnak. Sok esetben ezek az osztályok vagy igazgatóságok egymástól függetlenül működnek és hajtják végre incidenskezelési munkafolyamataikat, miközben saját biztonsági szabályzataikra hivatkozva csak minimális információt osztanak meg egymással, ezzel is hátráltatják az incidenskezelési munkafolyamataik végrehajtását.

A vizsgált szervezetek esetében kezdetben ezek a munkafolyamatok más-más személyek felelősségi körébe és önálló munkafolyamatok keretében működtek, jelentős többletmunkát és információáramlási problémát okozva egymásnak, nem beszélve arról, hogy az átjárhatóság korlátozottsága miatt időnként az egyes típusú incidensek észlelése is akadozott.

Ez megerősítette, hogy a jogszabályokat és szabvány előírásokat követő, jó incidenskezelési gyakorlatokat alkalmazó szervezetek nem mindig ismerik fel munkafolyamataik optimalizálásának lehetőséget, ezáltal párhuzamos munkafolyamatok végrehajtásával és többletadminisztrációs teherrel végzik incidenskezelési munkafolyamataikat.

Összességében nézve az információbiztonsági és adatvédelmi jogszabályok előírják az információbiztonsági és adatvédelmi incidensek kezelését, másrészről a szervezeteknek üzemeltetniük kell informatikai rendszereiket, amelyek hibáinak elhárításához IT incidenskezelési munkafolyamatra van szükségük. Mivel az IT szolgáltatási, információbiztonsági, adatvédelmi és

biztonsági incidensek átfedésben vannak egymással ezek kezelése sok esetben párhuzamosan zajlik egymással a különböző incidenskezelési munkacsoportoknál, ami információáramlási és hatékonysági problémát vet fel.

Mindezt figyelembe véve felmerül a kérdése egy integrált incidenskezelési munkafolyamatnak, amely megfelel minden jogszabályi követelménynek és bevezetett szabványnak. Figyelembe véve a jogszabályok és bevezetett szabványok számosságát, felmerül a megvalósíthatóság kérdése is. Elemezve a jogszabályok előírásait, a szabványok követelményeit és alkalmazott keretrendszerek ajánlásait, megjelenik előttünk a munkafolyamatok hasonlósága, ami egyértelművé teszi, hogy az integrált incidenskezelési folyamatnak összehangolt eseménykezelésen kell alapulnia, amely a lehető legrövidebb időn belül újraindítja az üzleti folyamatok végrehajtásához szükséges IT szolgáltatásokat, összegyűjti az adat és információbiztonsági események kivizsgálásához szükséges információt, továbbá időt és pénzt takarít meg a redundáns tevékenységek kiküszöbölésével. Másrészt az incidenskezelésben résztvevő szervezetek információmegosztásának és együttműködésének, valamint az incidenstípusok közötti összefüggések felhasználásának köszönhetően felgyorsul az információbiztonsági és adatvédelmi incidensek kölcsönös azonosítása, ami lehetővé teszi a gyors reagálást és a felmerülő károk minimalizálását.

A törvények betartása és a munkafolyamatok optimalizálása érdekében együttműködésre van szükség a különböző típusú események elhárítását végző csapatok között. Ez a következő feladatok végrehajtásában való együttműködést jelenti:

- incidensek rögzítése és kivizsgálása;
- egymás értesítése, ha a rögzített incidens több incidenstípusba is tartozhat;
- bizonyítékok gyűjtése, megőrzése és tárolása;
- közös eseménykezelési eljárásrendek és megoldások: naplózás, naplóelemzés eseménykorreláció;
- információmegosztás: az informatikai és biztonsági rendszerek rendszeres sérülékenységvizsgálatának eredménye; az informatikai és biztonsági rendszerek automatizált monitoring rendszereinek riasztásai; automatizált hibajelentések adatai;
- együttműködés annak eldöntésében, hogy melyik megoldócsoportnak van elsőbbsége a törvények betartása, az információbiztonság megfelelő szintjének biztosítása és az IT szolgáltatás hibaelhárítása érdekében.

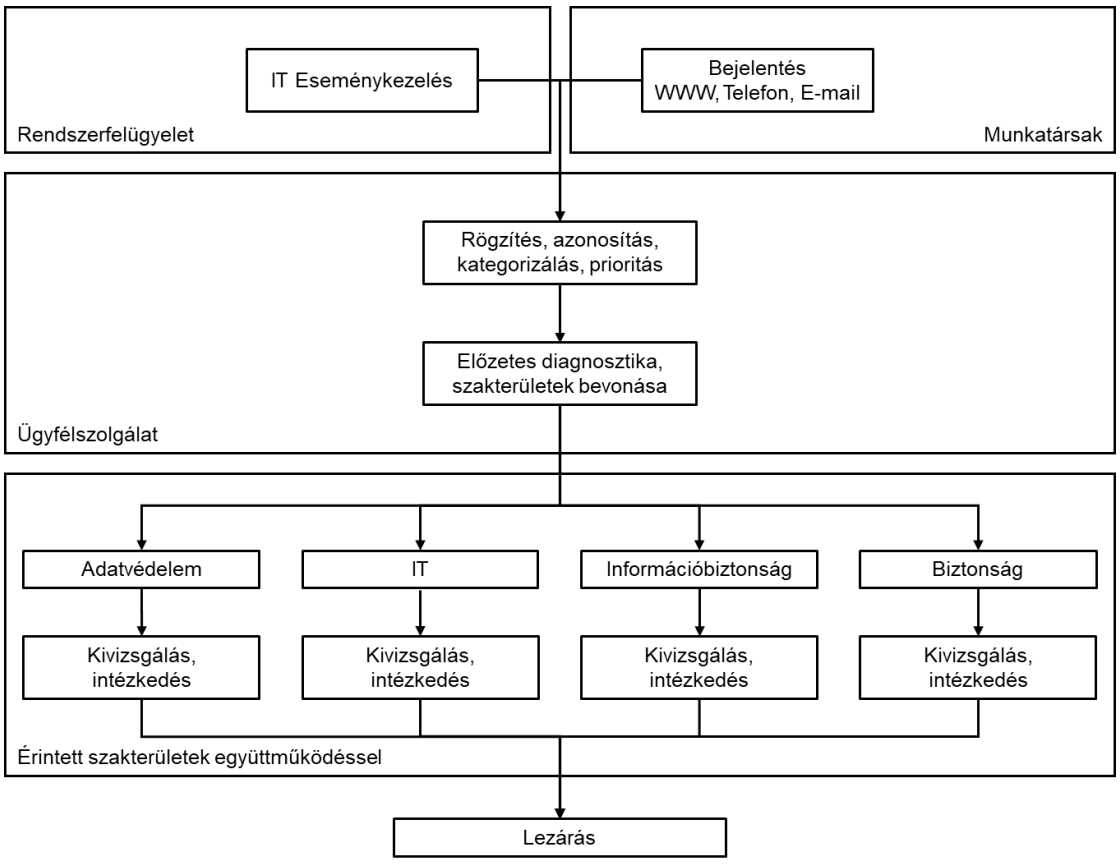
## 5.6 A javasolt integrált incidenskezelési modell

A „Computer Security Incident Handling Guide” című NIST SP 800-61 szabvány az informatikai rendszerek információbiztonságára összpontosít. Meghatározza az Információbiztonsági eseményhatás kategóriát, amelyek a következők: nincs, adatvédelmi jogsértés, saját jogsértés, integritásvesztés. Definiálja a helyreállíthatóság kategóriákat: rendszeres, kiegészített, kiterjesztett, nem helyreállítható. Kitér az incidensekre adott válaszok koordinációjára is [45].

Az ITIL incidenskezelési folyamata az informatikai szolgáltatási eseményekre összpontosít. Annak ellenére, hogy kitér az információbiztonságra, fő célja az informatikai szolgáltatások mielőbbi helyreállítása és újraindítása [53].

Mindkét megközelítés jó alapot nyújt az integrált incidenskezelési modell számára, mivel a teljes incidenskezelési folyamatra kiterjednek: az incidensek felderítésére, rögzítésére, elemzésére, megoldására, majd lezárására és utólagosan végrehajtandó tevékenységekre.

A 9-es ábrán bemutatott, javasolt incidenskezelési folyamatmodell tovább fejleszti a fent említett modelleket kiegészítve azokat minden a 5.2 fejezetben felsorolt incidenstípus kezelésével.




*9. ábra Javasolt integrált incidenskezelési modell [115]*

A javasolt integrált incidenskezelési folyamat modell két forrásból származó adatok alapján azonosítja az incidenseket:

- informatikai és biztonsági rendszermenedzsment megoldások eseménykezelő rendszeréből, amelyek képesek a biztonsági események azonosítására, adott esetben felhasználói profil elemzéssel támogatva [117];
- bejelentések ügyfelek, partnerek és munkatársak részéről.

A bejelentéseket egy központi ügyfélszolgálat fogadja és rögzíti egy a központi ügyfélszolgálati rendszerben. Az incidensek kezelését és felügyeletét az ügyfélszolgálat látja el.

Az új események fogadásakor az ügyfélszolgálat összegyűjti az incidenssel kapcsolatos rendelkezésre álló információt, elvégzi az incidens osztályozását, amelynek során rögzíti az érintett információ paramétereit:

- bizalmasságának szintjét, például: publikus, belső használatú, bizalmas, titkos, szigorúan titkos,
- az incidens által okozott információbiztonsági probléma kategóriáját: bizalmasság, sértetlenség, rendelkezésre állás;
- személyes adat érinett: igen vagy nem;
- besorolja az incidenst a megfelelő incidenstípusokba, azaz hozzárendel minden incidenstípust, amelybe besorolható: IT szolgáltatási incidens, információbiztonsági incidens, adatvédelmi incidens, biztonsági incidens;
- érintett információs rendszerek felsorolása.

Ezt követően az ügyfélszolgálat elvégzi az előzetes diagnózist, meghatározza az esemény súlyosságát, majd továbbítja a besorolás szerinti incidenstípusok kezelését végző incidenskezelési megoldócsoportoknak. Ezzel minden érintett munkacsoport azonnal hozzájut a rendelkezésre álló információhoz és egymással párhuzamosan elkezdhetik a munkát.

Mivel az incidenskezelő csoportok az incidenst közös nyilvántartásban, közösen kezelik, tudnak az érintett munkacsoportokról, ezáltal szükség esetén lehetőség nyílik a csoportok közötti együttműködésre és a feltárt bizonyítékok megfelelő kezelésére. Az incidens kezelését az ügyfélszolgálat felügyeli, szükség esetén konszolidálja a különböző incidenskezelési munkacsoportok tevékenységét.

Az esemény súlyosságától függően össze kell hívni a krízisbizottságot, amely az incidenst kezelő incidenskezelési munkacsoportok vezetőiből áll, vezetője pedig az információbiztonsági vezető

vagy felelős. Az információbiztonsági vezető vagy felelős a krízisbizottság tagjainak álláspontja alapján dönt a krízishelyzetet okozó incidens elhárításához szükséges tevékenységekről, továbbá szükség esetén jelentést nyújt be az illetékes hatóságokhoz.

A helyi és globális jogszabályi környezetnek való megfelelés érdekében a szervezeteknek be kell építeni az eseménykezelési modellbe a vonatkozó jogszabályok teljesítéséhez szükséges tevékenységeket.

Az incidens lezárását követően, annak súlyosságától függően, a résztvevő incidenskezelési munkacsoportok levonják és dokumentálják a tanulságokat, azok későbbi felhasználásának céljából.

## 5.7 Összegzés

Elemeztem a szervezetek IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági eseményekeinek kezelését megvalósító munkafolyamatokat. Megállapítottam, hogy a gyors és hatékony eseménykezelést ellehetetleníti a silószerűen kialakított incidenskezelési munkafolyamatok között akadozó információáramlás, amit az adatok bizalmasságára való hivatkozás okoz.

Feltártam a különböző incidenstípusok közötti összefüggéseket és ennek alapján létrehoztam egy olyan integrált incidenskezelési modellt, amelynek bevezetésével az incidensek bejelentése standard módon történik a szervezetben. Az informatikai rendszerekből származó biztonsági események többségét a rendszerfelügyeleti megoldások azonnal észlelik és továbbítják az illetékes ügyfélszolgálatra, ami növeli a szervezet reakcióképességét. Az incidenskezelési munkacsoportok együttműködésével, az incidensek adatainak standard kezelésével és illetékesek számára való elérhetővé tételével felgyorsul az események kivizsgálása és csökken az incidensek elhárításának átfutási ideje. A közös ügyfélszolgálat igénybevétele jobb erőforrás-felhasználást és együttműködést eredményez a munkacsoportok között. Az incidenskezelési munkafolyamatok integrálásával és az adatok azonnali elérhetővé tételével a biztonsági és adatvédelmi incidensek gyorsabb felderítése is lehetővé válik.

**A kutatási tevékenységem alapján igazoltnak tekintem a H5. hipotézist, mely szerint definiálható olyan integrált incidenskezelési munkafolyamat modell, amely összehangoltan irányítja az IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági eseményeket.**

# ÖSSZEGZETT KÖVETKEZTETÉSEK

## A kutatómunka összegzése

Pályafutásom informatikai rendszerek fejlesztésével indult, ezt követte az informatikai rendszerek bevezetése és üzemeltetése. Több mint 20 évet töltöttem el információs rendszerek kialakításával, bevezetésével, biztonságával, fejlesztésével és üzemeltetésével. Ez idő alatt megismertem az IT szolgáltatásmenedzsment és információbiztonság irányítási rendszerek bevezetését támogató keretrendszereket, szabványokat és jogszabályokat. Részt vettem számos IT szolgáltatásmenedzsment és IBIR rendszer tervezésében, bevezetésében és ellenőrzésében.

Kutatómunkám rámutatott arra, hogy az IT szolgáltatásmenedzsment és IBIR rendszerek bevezetésével a szerveztek növelik hatékonyságukat és információbiztonságukat. Az IT szolgáltatások ITIL alapokon való nyújtásával szabályozzák és optimalizálják az informatikai szolgálatásaik működtetését javítva az üzleti tevékenységek hatékonyságát. Az ISO/IEC 27001 szabvány alapú információbiztonság irányítási rendszer bevezetésével növelik az általuk kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását. A két szakterület erősen összefonódik, sok esetben a szervezetek mégis külön-külön megoldásokat alakítanak ki, amelyek utána egymástól függetlenül működnek.

A hazai és nemzetközi irodalomban az IBIR rendszerek kialakításának lehetőségeit kutattam, annak függőségét a szervezet méretétől és típusától, valamint más irányítási rendszerekkel (EN ISO 9001, ISO/IEC 20000) való integrált bevezetések módját és tapasztalatait. Áttekintettem a vonatkozó jogszabályokat és szabványokat, kerestem az IBIR rendszer alapjául választott szabvány és jogszabály, valamint a bevezetés eredményessége közötti összefüggéseket.

Az akciókutatásban részt vevő szervezetek esetében elemeztem a bevezetett IBIR rendszerek struktúráját, szabvány és jogszabályi megfelelését, követelményeinek alkalmazását, alkalmazhatóságát, betartását, betartatását, betarthatóságát, és az általa megvalósult információbiztonság eredményességét. Amennyiben a vizsgált szervezet IT szolgáltatásmenedzsment rendszert is üzemeltetett kitértem a két irányítási rendszer együttműködésére. Az IBIR és IT szolgáltatásmenedzsment rendszerek együttműködése kapcsán vizsgáltam a közös szakterületek együttműködését, az egymást átfedő folyamatok (incidenskezelés – biztonsági, incidensbiztonsági és IT szolgáltatási incidensek) kezelését. Ezen kívül elemeztem az IBIR illeszkedését a szervezetek működéséhez és gazdasági lehetőségeihez, valamint integrálását a szervezetek munkafolyamataiba.

Kutatási projektjeim során arra lettem figyelmes, hogy a bevezetett IBIR és IT szolgáltatásmenedzsment rendszerek nem mindig teljesítik maradéktalanul a velük szemben megfogalmazott elvárásokat, ez különösen igaz a külön-külön megvalósított irányítási rendszerekre.

Értekezésemben bevezetett IBIR rendszerek működését elemeztem különböző méretű és szakterületen működő szervezetek esetében, kitértem a vonatkozó hazai és nemzetközi jogszabályok, szabványok és keretrendszerek követelményeinek való megfelelésre. Az akciókutatásban feltárt gyakorlati tapasztalatok azt mutatják, hogy az egyre erősödő jogszabályi környezet és kifinomultabb szabványok alkalmazása sem garancia arra, hogy maradéktalan legyen a szervezetek információbiztonsága. A vizsgált szervezetekben feltártam, egységesítettem és csoportosítottam a hiányosságokat. Ezt követően kerestem előfordulásuk okait és megszüntetésük lehetőségeit, mind a hazai mind pedig a nemzetközi szakirodalomban, hogy olyan bevezetési módokat és technikákat találjak, amelyek segítenek fejleszteni az információbiztonság megvalósulásának színvonalát.

A szervezetek törekednek arra, hogy IBIR rendszerük megfeleljen a jogszabályi követelményeknek, ugyanakkor a biztonság megvalósulása sok esetben elmarad a szabályzatokban lefektetett szinttől. A hiányosságok feltárása, elemzése és csopoerosítása rámutatott azokra a hiányosságokra, amelyek gyakran fordulnak elő és kiküszöbölésükkel javítható az információbiztonság színvonala a szervezetekben.

A feltárt hiányosságok kiterjednek az IBIR strukturális felépítésére, érthetőségére és értelmezhetőségére, alkalmazhatóságára (a szabályzatok betartására, betarthatóságára, az IBIR előírásainak megvalósíthatóságára a szervezetben), redundanciák előfordulására (IBIR folyamatokon belül és a szervezet működési folyamataival). Megfelelőségi problémák ritkábban fordulnak elő, jellemzően azért, mert a szervezetek valamely szabvány vagy jogszabály mentén építik fel az információbiztonsági rendszerüket.

A kutatási projektek során elvégzett elemzések visszaigazolták, hogy a szabványok és jogszabályok jó keretet adnak az információbiztonság megvalósítására, így az IBIR struktúrája, nyelvezete, kialakítása és működtetése az, ami nagy mértékben befolyásolja a megvalósított IBIR rendszerek eredményességét. Ennek megfelelően olyan modellt alakítottam ki, amelynek alapja az információbiztonsági jogszabályok és szabványok követelményeinek összefésülése, struktúrája illeszkedik az IT szolgáltatásmenedzsment munkafolyamataihoz és tartalmazza azon információbiztonság fejlesztési és fenntartási folyamatok általánosított eljárásrendjét, amelyek

betartása kiküszöböli a bevezetés során elkövetett hibákat és eredményes IBIR-t hoz létre. Ez az eljárásrend biztosítja az IBIR ellentmondásmentes felépítését, a szervezet munkafolyamataival való hatékony együttműködését és az információbiztonság színvonalának folyamatos fejlesztését.

## Új tudományos eredmények

Doktori értekezésemben bemutatott kutatómunka eredményeként, új, tudományos eredményként kívánom feltüntetni az alábbiakat:

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

Azonosítottam a szervezetek információbiztonsági állapotát befolyásoló tényezőket. Felfedtem az IBIR strukturális, érthetőségi és értelmezhetőségi, alkalmazhatósági és redundancia problémáit. Jellegük, előfordulásuk (3.1 fejezet) és azok okainak feltárása (3.2 fejezet) alapján megállapítottam, hogy ezek a tényezők függetlenek a szervezet tevékenységétől és méretétől.

Kapcsolódó publikációim: [108].

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

Elméleti kutatás keretében vizsgáltam az információbiztonság, minőségirányítás és IT szolgáltatásmenedzsment összefügéseit (2.1 fejezet), állapotának és fejlesztésének irányelveit (2.2 fejezet), valamint bevezetésének módjait (2.4 fejezet). Ezek alapján létrehoztam az IBIR alapmodellt, amely a szabványok és jogszabályok követelményeit redundanciamentes fastruktúrába rendezi. Mivel a feltárt hiányosságok okait az IBIR kialakításának folyamatára vezettem vissza (3.2 fejezet), ezek kiküszöbölésére egy Információbiztonság tervezési és fenntartási szabályzatot építettem be (4.5 fejezet).

Kapcsolódó publikációim: [41] [66] [73] [79] [108].

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

Az információbiztonság kapcsolatainak, bevezetési módjainak és IT szolgáltatásmenedzsmentet támogató IBIR lehetőségeinek vizsgálata során megfigyeltem, hogy a szabványok közötti

összerendelések jellemzően szakterületenként történtek (2 fejezet). IBIR modellem megalkotása során a követelményeket szakterületenként csoportosítottam, ez lehetővé tette a projektek során a szabályzatok és eljárásrendek hozzárendelését a szervezetek szervezeti egységeiben működő szakterületekhez (4.3-4.5 fejezetek).

Kapcsolódó publikációim: [69] [79] [108].

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

Elméleti kutatásaim alapján megmutattam, hogy az információbiztonság folyamatlépésekbe építése biztosítja a folyamatok zavartalan működését és folyamatbiztonságot eredményez (2.3 fejezet). Ennek mentén megalkottam a folyamatszemléletű IBIR bevezetési módot. Ez az IBIR integrált bevezetésére épül, tartalmazza az IT szolgáltatásmenedzsment munkafolyamatokat az IT szolgáltatások biztonságos működtetéséhez, a bevezetés legvégén pedig beépíti az információbiztonsági követelményeket a szervezet munkafolyamataiba. Ez a bevezetési mód kiküszöböli az IBIR és szervezeti folyamatok ellentmondásait, ugyanakkor végrehajtása információbiztonsági, folyamatmenedzsment és IT szolgáltatásmenedzsment szaktudást igényel. A bevezetéséhez szükséges erőforrások mértéke függ a szervezet munkafolyamatainak számától és méretétől (2.4 fejezet).

Kapcsolódó publikációim: [19] [41] [66] [69] [90] [104]

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

Létrehoztam egy integrált incidenskezelési munkafolyamat modellt (5.6 fejezet) amely a különböző incidens típusok közötti átfedés esetén azonnali információáramlást biztosít, gyorsabb és hatékonyabb incidens kivizsgálást és reakciókészséget, ezáltal gyorsabb incidenselhárítást biztosít, mint az egymástól független IT szolgáltatási, biztonsági, adatvédelmi és információbiztonsági munkafolyamatok párhuzamos működtetése.

Kapcsolódó publikációim: [66] [115] [108]

## Ajánlások

Kutatási eredményeim általánosak, minden szervezetben alkalmazhatók.

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

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

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

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

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

# IRODALOMJEGYZÉK


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

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

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

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

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

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

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

[8] LEWIN, K., „Action Research and Minority Problems," *Journal of Social Issues*, vol. 2, no. 4., 1946., pp. 34-46. DOI:10.1111/j.1540-4560.1946.tb02295.x (Letöltés ideje: 2019.07.25.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[46] ISACA, COBIT 4.1., 2007.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[76] SHAMELI-SENDI, A., JABBARIFAR, M., DAGENAIS, M., SHAJARI, M., „System Health Monitoring Using a Novel Method: Security Unified Process," *Journal of Computer Networks and Communications*, vol. 2012. p. 20., DOI:10.1155/2012/151205 (Letöltés ideje: 2015.10.12.)

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

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

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

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

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

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

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

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

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

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

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

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

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

[91] AAGEDAL, Ø. J. et al., „Model-based Risk Assessment to improve Enterprise Security," in *Proceeding of the 6th International Enterprise Distributed Object Computing Conference (EDOC'02)*, 2002., pp. 51-54. DOI:10.1109/EDOC.2002.1137696 (Letöltés ideje: 2011.09.30.)

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

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

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

[96] RODRIGUEZ, A., FERNANDEZ-MEDINA, E., PIATTINI, M., "A BPMN Extension for the Modeling of Security Requirements in Business Processes," *IEICE TRANSACTIONS on Information and Systems*, vol. E90-D. no. 4. pp. 745-752, 2007., DOI:10.1093/ietisy/e90-d.4.745 (Letöltés ideje: 2016.10.05.)

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

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

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

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

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

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

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

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

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

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

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

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

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

## Saját publikációk

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Szabványok

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

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

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

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

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

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

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

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

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

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

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

## Jogszabályok

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

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

[31] Social Security Number Protection Act of 2011

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

[33] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[34] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[35] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

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

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

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

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

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

[56] 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

[57] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[58] 42/2015. (VII. 15) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

[59] 187/2015. (VII. 13.) Kormányrendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározás

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

[64] 2011. évi CXII. törvény Az információs önrendelkezési jogról és az információszabadságról

# TÁBLÁZATJEGYZÉK

# ÁBRAJEGYZÉK

# KÖSZÖNETNYILVÁNÍTÁS

Mindenekelőtt szeretném megköszönni témavezetőm, Prof. Dr. Michelberger Pál iránymutatásait a kutatási munka és az értekezés elkészítése során is.

Köszönöm Dr. Beinschróth Józsefnek, hogy folyamatos konzultációval segítette kutatási munkám elvégzését, Dr. habil. Velencei Jolánnak a módszertani útmutatást, Dr Horváth Zsolt Lászlónak, hogy szakmai írásaival és gondolkodásmódjával segítette munkámat.

Külön köszönettel tartozom lányomnak Melindának, aki nyelvhelyességi szempontból segített átnézni értekezésemet.

Köszönettel tartozom feleségemnek és gyermekeimnek a korlátlan türelmükért és folyamatos támogatásukért.

Köszönettel tartozom szüleimnek, hogy támogatták tanulmányaimat, lehetővé tették az egyetem elvégzését és a szakmai előrehaladásomat.