DIPLOMADOLGOZAT

Szabó József

2023

Magyar Agrár- és Élettudományi Egyetem
Szent István Campus
Műszaki Intézet
Műszaki menedzser mesterképzési szak

INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR) BEVEZETÉSE ÉS FENNTARTÁSA SZENZITÍV ADATOKAT KEZELŐ VÁLLALKOZÁSNÁL

Belső konzulens:	Dr. Kovács Imre mesteroktató
Intézete/Tanszék:	Műszaki Intézet, Műszaki Menedzsment Tanszék
Külső konzulens:	Bozi Péter nemzetközi igazgató
Készítette:	**Szabó József hallgató** **CQJVYQ**

Gödöllő

2023

MŰSZAKI INTÉZET
Műszaki menedzser mesterképzési szak
Termelés- és minőségmenedzsment specializáció

DIPLOMADOLGOZAT

feladatlap

Szabó József *(CQJVYQ)*

részére

A diplomadolgozat címe: INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR) BEVEZETÉSE ÉS FENNTARTÁSA SZENZITÍV ADATOKAT KEZELŐ VÁLLALKOZÁSNÁL

Feladatkiírás:

Tervezze meg az IBIR (MSZ ISO/IEC 27001:2014) szabvány szerinti irányítási rendszer bevezetésének és fenntartásának folyamatait egy adott vállalkozásnál, azok várható idő-költség és egyéb erőforrás szükségletét!

- Foglalja össze a minőségirányítási rendszerekkel és a kapcsolódó minőségmenedzsment technikákkal kapcsolatos ismereteket, mutassa be a vállalati adatvagyon szerepét, a vállalati erőforrástervező rendszerek kialakulását!
- Vizsgálja meg az ISO 27.000-es szabványcsalád és egyéb információbiztonsághoz kapcsolódó szabványok (ITIL, COBIT), előírások és eljárások közös elemeit, különös tekintettel az Európai Parlament és a Tanács (EU) 2016/679 rendeletére (GDPR- General Data Protection Regulation)!
- Elemezze az információhoz, adathoz és információtechnológiához kapcsolódó kockázati események főbb típusait, azok kezelésének lehetséges módjait!
- Dolgozza ki és mutassa be egy adott vállalatnál az IBIR bevezetésének lépéseit projektmenedzsment technikák alkalmazásával, tegyen további fejlesztési javaslatot a PDCA ciklusnak megfelelő belső folyamatok kialakítására!

Közreműködő tanszék: Műszaki Menedzsment Tanszék, Gödöllő
Külső konzulens: *Bozi Péter Nemzetközi Igazgató*, EMT Első Magyar Tanúsító Zrt., 2040 Budaörs, Muskátli utca 3.
Belső konzulens: *Dr. Kovács Imre mesteroktató,* MATE, Műszaki Intézet
A dolgozat beadási határideje: 2023. év november hó 6.nap
Kelt: Gödöllő, 2023. év szeptember hó 15. nap

Jóváhagyom		**Átvettem**
(tanszékvezető)	(szakfelelős)	Szabó József (hallgató)

A dolgozat készítőjének külső konzulense nyilatkozom arról, hogy a hallgató az előre egyeztetett konzultációkon megjelent.

Kelt: Budaörs, 2023.év október 27.

(külső konzulens)

Tartalom

1. Bevezetés

Adathalászat, zsaroló vírusok, online bankkártyacsalások, leállt egészségügyi intézmények, valamint „lehaló” kormányzati, oktatási és szolgáltatói weboldalak.

Mindennapjaink részévé váltak ezek a fogalmak, legtöbbünknek sajnos van már magánéleti, vagy munkahelyi tapasztalata ilyen események részeseként, áldozataként. Naponta adnak hírt a különböző médiumok levelező rendszerek feltöréséről, „kiszivárgott” kompromittáló fénykép és videofelvételekről, a magánéletünk legapróbb titkait feltáró hackerek által elkövetett cyber bűncselekményekről. Ezekre az ügyekre mindenki felkapja a fejét, a személyes érintettség lehetősége komoly figyelemfelhívó erővel bír.

Van azonban az **információbiztonsághoz** kapcsolódó **kockázatoknak**, sérülékenységeknek olyan területe, ami nagyságrendileg nagyobb károkozásra ad lehetőséget. Az ipar 4.0, a mesterséges intelligencia, az IoT (Internet of Thinks), adatbányászat és a Big Data, a virtuális és kiterjesztett valóság, valamint a teljes szellemi vagyon dematerializálódása korában, - megfelelő szabályozottság hiányában -, koncentrált és egymás hatását is felerősíteni képes kibertámadások áldozata lehet társadalmunk bármely szervezete, alanya. Ez pedig független attól, hogy az adott szervezet az iparban, a mezőgazdaságban, valamely szolgáltató ágazatban, kormányzati esetleg nonprofit társaságként látja el feladatát.

A „Just in Time” -ra időzített és LEAN-re karcsúsított termelési rendszerekben még csak szándékosság sem szükséges a teljes termelési lánc megakasztásához, elég hozzá az emberi gondatlanság, hanyagság, a rosszul tervezett és egymáshoz illesztett szoftverek és hardver eszközök, valamint a szabályozatlan munkafolyamatok.

Információtechnológia vezérli a tervezést - CAD-CAM rendszerek -, a gyártást, a logisztikát, a kereskedelmet, minden erőforrás és entitás kapcsolatban áll egymással, az anyagáramlással párhuzamosan pedig hatalmas mennyiségű adat áramlik át percről percre számítógépes és infokommunikációs hálózatokon.

Megtanultuk megvédeni a materiális formában rendelkezésre álló anyagi javainkat, de a robbanásszerűen felgyorsult technológiai fejlődés, a hihetetlenül lerövidülő termékéletciklusok, a marketing és a jóléti fogyasztói társadalmak által generált fejlesztési igények szinte leküzdhetetlen kihívások elé állítják a tervezőket, szoftverfejlesztőket, mérnököket és menedzsereket, legalábbis ami az információbiztonság kérdéskörét illeti.

Rövid időn belül szenzorok milliárdjai érzékelik majd környezetünket és nagy bonyolultságú rendszerek vezérlik a mezőgazdasági termelőeszközöket, az ipari robotokat, a logisztikai láncokat, de még lakóépületeinket is. Hamarosan digitálisan vezérelt közműhálózatok, erőművek, önvezető kamionok, mezőgazdasági vető, öntöző és betakarítógépek, ipari robotok állítják majd elő a megtermelt társadalmi és anyagi javak jelentős részét, minimális emberi beavatkozással.

Az ipari folyamatirányító és mérésadatgyűjtő rendszerekben a beavatkozás analóg relés vezérlését, - mágneskapcsolók, hő és időrelék, mágnesszelepek -, és szerepét a digitális programozott vezérléstechnika veszi át, a beágyazott ipari rendszerek programozott logikai vezérlői, PLC áramkörei pedig technikai belépési pontként jelennek meg az információtechnológiát érintő kockázati elemekben.

Claude E.S. (1948) matematikus és híradástechnikus információelméleti entrópia formulája óta tudjuk, hogy az **információ mennyisége mérhető**, az anyag és energia mellett a világegyetemet alkotó harmadik entitásként értelmezhető. Sajnálatos módon azonban van egy sajátos tulajdonsága az információnak: nem vonatkoznak rá a megmaradási tételek, korlátlanul sokszorosítható, veszteség nélkül továbbítható, de el is tűnhet a semmiben! [Komenczi, 2011]. És éppen ez a jellemzője az, ami miatt a napjainkban exponenciális ütemben növekvő elektronikus jelek, adatok, adatbázisok, majd az adatok tárolásából és feldolgozásából kinyerhető információk hatékony és biztonságos menedzselése egészen más eszközrendszert igényel, mint a materiális formában megjelenő egyéb vagyonelemek.
Diplomadolgozatom írásának időpontjának napi híreként jelent meg, hogy világszerte leállt a teljes Volkswagen csoport gépkocsi gyártó üzemei, a probléma a győri Audi gyárat is érintette, a leállás okaként pedig egy közelebbről meg nem nevezett informatikai problémát neveztek meg [Index.hu 2023]: *„A Reuters hírügynökség jelentése szerint Németországban a wolfsburgi, emdeni, osnabrücki, hannoveri, drezdai és zwickaui üzemeken kívül a braunschweigi, kasseli, chemnitzi és salzgitteri alkatrészgyárak is érintettek voltak a problémában.”* Rendszerinformatikusként és minőségmenedzsment szakirányú műszaki menedzserként, valamint munkahelyem pénzügyi és minőségbiztosítási vezetőjeként, kiemelt vállalti vagyonelemként tekintek a vállalkozások szellemi, pénzügyi, humánerőforrás, szervezeti és kapcsolati tőkéje mellett a céges **adatvagyonra**.

Ennek az immateriális tőkeelemnek a menedzseléséhez, a hatékony vezetői döntéstámogatáshoz, az üzletmenet folytonosságának biztosításához, valamint a vállalati reputáció védelméhez elengedhetetlennek tartom a minőségmenedzsmentnek az adatbiztonság, adatvédelem területén, - de facto ágazati szabványaként elterjedt -, Információbiztonsági Irányítási Rendszer szerinti működtetését.

Célom bemutatni munkahelyemnek az ISO 27 000 (továbbiakban IBIR) bevezetési folyamatát, ennek során felmérem a vállalati adatvagyont, elkészítem a vagyonleltárt. Mindezek alapján kockázatelemzést, kockázatkezelést végezek, a szabványkövetelmények mentén pedig kialakítom az információbiztonsági rendszer folyamatait. Az erőforrások tervezéséhez és az IBIR bevezetéshez bemutatok egyes projekttechnikákat, majd a tanácsadói felkészítési és külső audit tanúsításának költségelszámolásához javaslatot teszek azok számviteli kezelésére. A bevezetést követő fenntartás és fejlesztés területét érintően az információtechnológiában használatos teljesítménymutatókat, - KPI- Key Performance Indicator -, vezetek be. Kialakítom a hatékony IBIR szervezeti struktúráját, egyértelmű feladat és felelősségi körök meghatározásával.

Az információtechnológia széleskörű elterjedésének egyik alapfeltétele volt a szabványosítás, ennek a technikai, technológiai vonatkozásai mentén kialakultak a különböző információbiztosági szabványok, melyek közötti eltérés nagyjából összefoglalható abban, hogy melyik szabvány hová fekteti a fő hangsúlyt, a folyamatokra, a technológiára, vagy a szervezésre helyezi elsősorban a fókuszpontját.

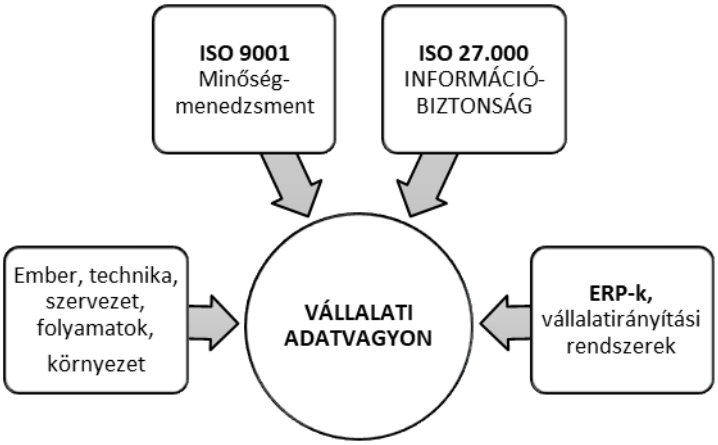
2023. június 1-én jelent meg a 2014.-évi 27 001-es követelményszabvány újabb kiadása, az MSZ ISO/IEC 27001:2023 szabvány, **Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek.** Jelentős módosítások történtek, haladva a kor követelményeinek megfelelően, ezeket is érintem dolgozatomban. Az adatvédelem kérdésköréhez kapcsolódóan bemutatom az ISO 27 001-es szabvány és a lassan szitokszóvá váló GDPR, az Európai Unió adatvédelmi rendeletének lehetséges kapcsolódási pontjait.

2. A hazai és a nemzetközi szakirodalom áttekintése

„Muszáj törődnöm vele. Valóságos fizikai fájdalmat okoz nekem, ha látom, hogy valamit rosszul csinálnak, amikor pedig olyan könnyen lehet jól is csinálni.” (Kurt Vonnegut)

Vállalatirányítás, minőségmenedzsment és információbiztonság. Látszólag egymástól távol álló fogalmak, mégis az üzleti élet egyre komplexebbé válása életre hívta az **információmenedzsment** területét kezelő, a Nemzetközi Szabványügyi Testület által kiadott ISO/IEC 27001:2005 szabványt, ami a minőségügy általános 9000-es szabványcsaládjának informatikai, egyben technikai vonatkozású, első széleskörűen elterjedt követelmény szabványa lett. Modern **vállalatirányítás** nem létezne **minőségmenedzsment** nélkül, vállalatirányítási szoftver rendszerek pedig nem léteznének **informatikai támogatás** nélkül. Ennek összefüggését szemléltetem az 1. ábrán.

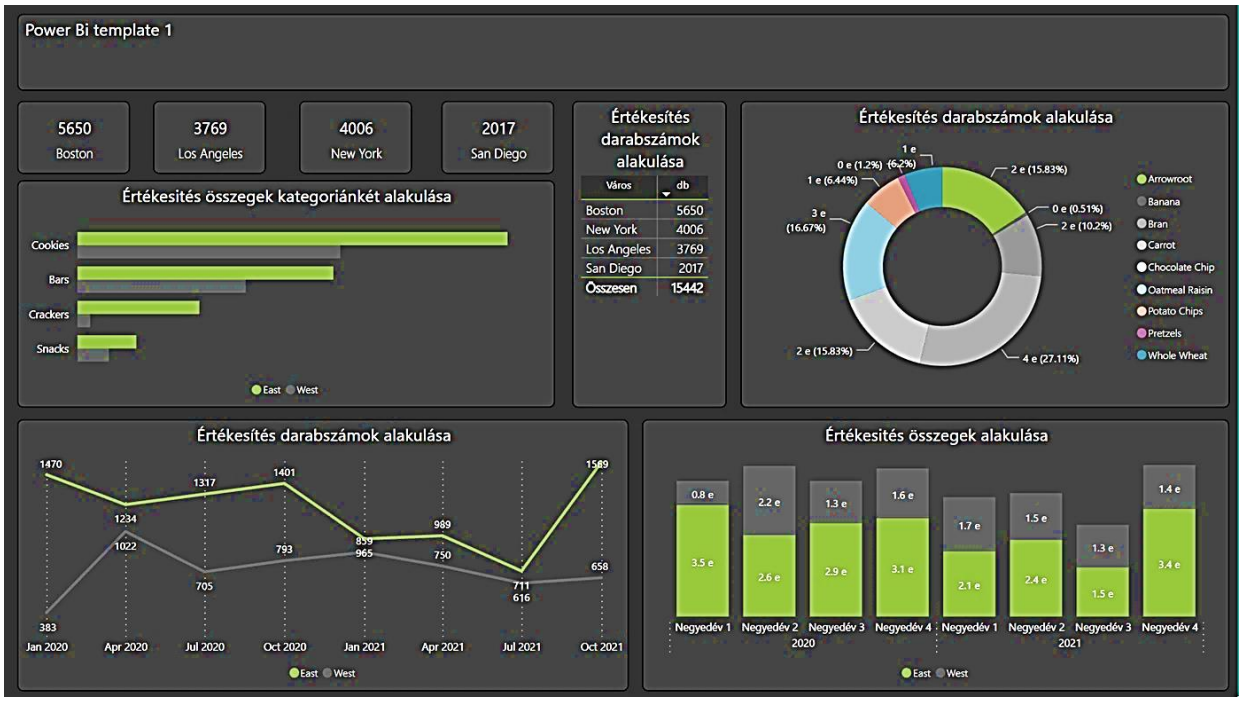
1. ábra: A vállalati adatvagyon menedzselése
(Forrás: Saját szerkesztés)



Egymásba kapcsolódó fogalmak ezek, ezért bemutatom ezen módszerek és menedzsment eszközök közös jellemzőit, kialakulásukat, mivel nem értelmezhető az információbiztonság pusztán technikai előírások összességeként. Szabványosítását megelőzte a sikeres vállalatok működésének minden szegmensét átható minőségirányítás és a teljes körű minőségmenedzsment kialakulása, ezzel párhuzamosan pedig megjelentek és elterjedtek a vállalati erőforrástervező rendszerek (**ERP**-Enterprise Resource Planning). Jelenleg pedig már az üzleti intelligencia és adatbányászati funkciókkal felvértezett komplex vezetői döntéstámogató és dokumentummenedzsment (**DMS**-Document Management

System) rendszerek korát éljük. Napjainkban a döntéshozók számára csak pontos, időszerű, teljeskörű és érvényes, valamint sértetlen alapadatokból készülhet **döntést támogató** anyag. Hatalmas mennyiségű adathalmazból kell kinyerni és a vezető számára vizuálisan megjeleníteni bonyolult matematikai és statisztikai műveletek eredményeként azokat a jellemzőket, amelyek számára az adott pillanatban fontosak, erre alkalmas az adatvizualizáció módszere. Power BI szoftverrel készült 2. számú ábrán szemléltetem az adatok megjelenítésének nagyon hatékony módját, ami ráadásul nem statikus, hanem különböző paraméterek változtatásával azonnal megjeleníti az összes kapcsolt és változó értéket.

2. Ábra Adatvizualizáció
(Forrás: www. https://ilovedata.hu/power-bi/)



Az információmenedzsment és a **tudásmenedzsment** egymásra épülésének folyamata során a fizikai jelsorozatból adat, azok feldolgozásából információ, kognitív képességünk segítségével tudás, abból pedig bölcsesség és intelligencia származtatható.

A világgazdaság ellátó rendszereiben nem működhetne a termelés és a logisztika **termelési erőforrástervezési rendszerek** nélkül, mértani pontossággal tervezve és prognosztizálva a termelés időbeli lefutását, az alapanyagrendelés ütemezését, a készletgazdálkodást és a raktározást.

A biztonsági készletekben, feleslegesen alapanyag vagy késztermék raktárakban álló fel nem használt termék olyan lekötött tőke, ami komoly finanszírozást és végső soron versenyhátrányt jelent az adott vállalkozásnak. Az értékesítés ügyfélkapcsolatokat kezelő rendszere, a vevőrendelések lekezelési folyamata egészen a kiszállításig, majd utána a vevőkövetésig, valamint a gazdasági eseményeknek a pénzügyi analitikus és szintetikus nyilvántartásba történő átvezetése szintén bonyolult és komplex információtechnológiai és minőségmenedzsment támogatást igényel. A termelési lánc, valamint a vállalati stratégiai részterületek ökoszisztémája akkor működik jól, ha biztosított a folyamatos termelés, szolgáltatás, kiesések nélkül, megfelelő katasztrófavédelmi tervekkel. Ez pedig már az üzletmenet folytonosságát és rendelkezésre állást érintő kérdéskör, ami az IT-szektorban az egyik fő bázis mutató. Eddig azonban el kellett jutnunk…..

2.1. Minőségmenedzsment és vállalati erőforrástervező rendszerek kialakulása

2.1.1. A minőségügy fejlődéstörténete

Mi is a minőség? Mire vonatkozik? Hogyan érzékeljük? Már Arisztotelész (Kr. e. 384-322) meghatározta a minőségkomponensek akkori halmazát, ami tíz elemből állt: 1. állag; 2. mennyiség; 3. minőség; 4. viszony; 5. hely; 6. idő; 7. helyzet; 8. bírás; 9. cselekvés; 10. szenvedés. Georg W.F H. (1812) német filozófus a saját minőségelméletében a minőséget, mennyiséget és mértéket egymással nagyon szoros kapcsolatban álló, egymásba korlátlanul átalakítható természeti jellemzőknek írt le. Fontos fogalmak a minőség filozófiai definíciójában a minősítő értékrendje és az értékalapú elemzés, továbbá a vizsgálati szempontok, mérések, és ezek eredményeinek összevetése egy másik objektummal. A minőség egyik lefontosabb tulajdonsága az, hogy általa az egyes termékek, a szolgáltatások megkülönböztethetőek, megmutatja az egyik egyobjektum másik objektummal való hasonlóságát, különbségét.

Az emberiség történelmi fejlődésének kezdetén, az ókorban, a minőség a méréssel, számolással, mértékegységrendszerekkel - Sumérok, Babilóniaiak -, később a kor akkori eszközeinek, termékeinek a szavatosságával és azonosíthatóságával kapcsolatosan jelent meg.

Az Egyiptomiak a halottak balzsamozásának folyamatát a „A halál könyvében”, az első dokumentált minőségirányítási rendszerben szabályozták. Már a Bibliában is találunk a minőséggel kapcsolatos építészeti előírásokat. A Kínaiak agyaghadseregük minden egyes tagját azonosító jellel látták el, a kézműves és mesteremberek azonosító védjegyhasználata, a rómaiak építészeti és útépítési korai szabványai pedig a minőség fogalmának ókori megjelenési formája. Az ókori és középkori arany, ezüst tárgyak tanúsítására fémjelzést vezettek be. A papírkészítés során a XIII. században vízjelet, az építészetben pedig a kőépületeknél a kőművesek azonosító jelét alkalmazták.

Az anyagvizsgálati módszerek elterjedésével, valamint a középkori törvényekben és rendeletekben szabályozott **mérőeszköz hitelesítésben** a forgalombahozatal követelményei jelennek meg. A kialakuló céhek és manufaktúrák megjelenésével a hangsúly a termelés egyes munkafázisainak szabályozására helyeződött át, ami az ipari forradalom termelésének tömegszerűvé válásával, később a világháborúk hadiipari gazdálkodásában a hadiipari beszállítókkal szemben támasztott követelményekkel, a hatékonyabb vállalatirányítási és válallatmenedzsment modellek megjelenése mellet a minőség-**ellenőrzés**, majd minőség **szabályozás** kialakulását, később a minőség **irányítást** és végül a teljes körű **minőségmenedzsment** rendszerek megjelenését is elhozza.

A minőség integratív tulajdonsága miatt magába olvasztja a menedzsment, a mérnöki, műszaki és pénzügyi-gazdasági tevékenységet, statisztikai, folyamatirányítási, esztétikai, ergonómiai vetületei is vannak. Komoly felhatalmazással bír a szervezetekkel és vállalati kultúrával kapcsolatos kérdésekben, hiszen az értékelőállítási folyamat során minden olyan szereplőre hat, aki a minőségre bármilyen hatással van, vagy lehet. Jelentheti a minőség továbbá az állandó fejlődésre, kiválóságra törekvést is, létezik olyan minőségmenedzsment modell, ami pont ezekre a tényezőkre fókuszálva vezeti le önnön lényegét. A minőséget több aspektusból vizsgálva bonthatjuk le összetevőire, de valamennyi lényege, hogy érték és hasznosság alapú és a folyamat eredményeként a vevő választásában jut kifejezésre, aki preferálja a tartósat, használhatót, esztétikusat, megbízhatót.

A minőségirányítás egyszerre jelent igazgatási és műszaki tevékenységet is. A minőség értelmezhető egy **termék**, objektum, egy **folyamat**, vagy egy egész **rendszer** jellemzőinek együtteseként.

Termékjellemzők leírásához a minőségügyben a **minőségkomponensek** fogalmát használjuk, ezek az ötlet, a funkcionalitás, konstrukciós, kivitelezési, megjelenés-esztétikum, használati és információs összetevőkben jelennek meg [Bartos 2010].

Egy termék újdonságfoka, funkcióinak és a vevői elvárásoknak összhangja, a kivitelezés technikai és konstrukciós szintje, ez előírt tűréshatároknak való megfelelése, megjelenési esztétikuma, valamint a biztonsági követelményeknek való megfelelése, továbbá a termék élettartama, javíthatósága és újrahasznosíthatósága jelenik meg a termék fizikai megjelenési formájához kapcsolódó minőségügyi elvárásokban. Egy termék/szolgáltatás minden esetben hordoz gazdasági és technikai funkciókat, pszichológiai funkciókat, szociológiai funkciókat. Ezek halmazát a költségek viszonyában vizsgálva **értékelemzéssel** határozhatjuk meg.

A minőségügy fejlődéstörténeti lépései során az áruk egyszerű **végellenőrzésétől** kezdve, később tervezéssel, **hiba megelőzéssel**, folyamat közbeni **visszacsatolásokkal**, **méréssel**, **felügyelettel**, **auditokon** alapuló működéssel és a teljes szervezetet átható szemlélettel eljutottunk a **teljes körű** minőségmenedzsmenthez. Ellenőrzés-szabályozás-biztosítás-irányítás, végül TQM a minőségügy evolúciós lépéseinek fő fejezetei, eltérő utat bejárva, de egymáshoz jelenleg már közeledve alakultak ki a minőségügy őshazájában, Japánban, majd az Egyesült Államokban és Európában. [Kövesi-Topár 2006].

Ahogy a minőségügy hatásköre a termék fizikai jellemzőiről kiszélesedett a termék teljes életciklusán át, -melyet minőséghuroknak nevezünk, - valamennyi érdekelt fél, tehát az egész termelő szervezet, a menedzsment, a szállítók, partnerek, a természeti környezet, majd a társadalom elvárásaira is, úgy jelent meg a minőségügyben a **folyamatszemlélet**, valamint az egyes **problémamegoldó technikák**. A termelési folyamatokban statisztikai jellemzőket kezdtünk figyelni, a komplexitás növekedésével pedig az egyváltozós, statikus és determinisztikus jelenségektől eljutottunk a többváltozós, dinamikus és sztochasztikus folyamatokig. A termelésben ezt a kérdéskört a Statisztikai Folyamatszabályozás vizsgálja, ami a LEAN menedzsment egyik minőségügyi módszertanát képezi.

Az alábbi, 1 számú táblázat a jelenségek komplexitását és annak lehetséges matematikai kezelési módját mutatja be, ez a Howard féle problématér [Enyedi, 1997].

1. Táblázat a Howard féle problématér
(Forrás: Enyedi, 1997)

	Tartalma	**Példa**	**Matematikai modell**
1.	Determinisztikus, statikus, egyváltozós	Adott kerülethez tartozó, téglalap terület (kerítés)	Elemi matematika eszközei
2.	Determinisztikus, dinamikus, egyváltozós	Elemi automatikus szabályozás	Differenciál egyenletek, transzformáció számítás
3.	Sztochasztikus, dinamikus, egyváltozós	Egyszerű biztosítási ügyletek	Valószínűség számítás
4.	Determinisztikus, statikus, sokváltozós	Hozzárendelési problémák, termelésprogramozás	Mátrix algebra
5.	Sztochasztikus, dinamikus, egyváltozós	Készletezési problémák	Sztochasztikus folyamatok elmélete
6.	Sztochasztikus, statikus, sokváltozós	Új termék bevezetése	Keverékeloszlások matematikája
7.	Determinisztikus, dinamikus, sokváltozós	Bonyolult szabályozási és vezérlési problémák	Szabályozás-vezérlés elmélete
8-	Sztochasztikus, dinamikus, sokváltozós	Iparvállalatok fúziója	Markov-folyamatok, ezzel kapcsolatos matematikai eljárások

A minőségügyben egyesül a vevők kimondott, kimondatlan és látens **igényeinek kielégítése**, egy terméknek, szolgáltatásnak, folyamatnak, vagy magának a minőségirányítási rendszernek az a képessége, hogy kielégítse a vevők és más érdekelt felek igényeit. Ez pedig a szabvány alapú megközelítése a minőségirányításnak [ISO 9001 2015]. Eredménye a vevői megelégedettség, a visszatérő vásárló, a termék vagy szolgáltatás kimeneti paramétereinek stabilitása, ingadozástól való mentessége. Minőségkövetelmény, megfelelőség, képesség és megbízhatóság, ezek azok a fogalmak, melyek köré a minőségügy szerveződött.

A **fejlődés** és a **fejlesztés** mindegyik minőségirányítási, folyamatfejlesztési rendszer központi elemeként jelenik meg, hiszen nincs hibamentes emberi tevékenység, tökéletes munka és technológiai folyamat. Folyamatosan változó környezetünk változásra képes szervezeti, tervezési és gyártási környezetet igényel. Ennek a fejlesztési folyamatnak a módszertana az ISO 9000-es szabványcsaládban a **PDCA (plan-do-check-act) ciklus**.

Minden termék, folyamat vagy eljárás rendelkezik számszerűsíthető és nem számszerűsíthető jellemzőkkel, néhányat a 2. számú táblázatban mutatok be.

2. Táblázat Számszerűsíthető és nem számszerűsíthető jellemzők
(Forrás: Saját szerkesztés)

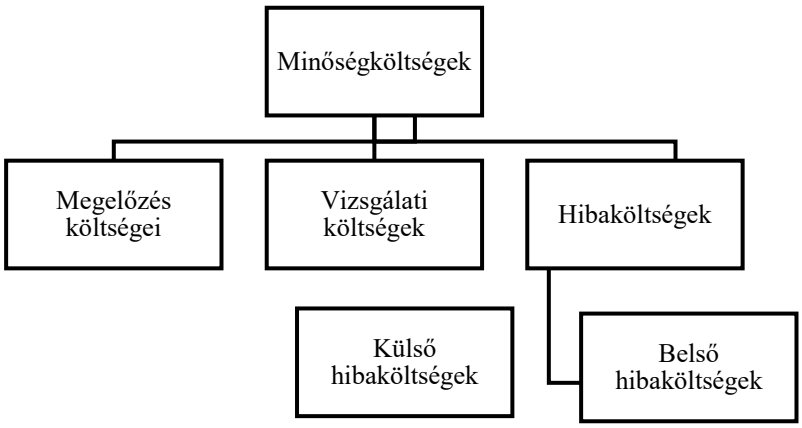
Számszerűsíthető jellemzők	Nem számszerűsíthető jellemzők
Vegyi összetétel, fizikai jellemzők	Esztétikai és ergonómiai jellemzők
Technológiai jellemzők, hőkezelés, megmunkálás	Szerelési előírások
Funkcionális jellemzők teljesítmény, sebesség	Üzembe helyezési előírások
Megbízhatósági jellemzők-szavatosság, jótállás	Használati előírások
Élettartam jellemzők	Karbantartási előírások
Biztonságtechnikai jellemzők	Javítási előírások
Geometriai jellemzők-méretek, tűrések	Hulladékkezelési előírások

Általánosságban elmondható, hogy a minőségbiztosítás a legtöbb esetben igyekszik a szubjektívet objektívvá, a nem mérhetőt pedig mérhetővé alakítani, Ennek eszközei a **minősítéses és méréses méréstechnikai eljárások** a minőségügy alapvető folyamatfelügyeleti eszközei:

Fontos területe a minőségügynek, magának a **minőségügyi költségeknek** a feltérképezése, hiszen egyrészt a minőségirányítási rendszer üzemeltetetése és a minőség biztosítása egy szervezet erőforrásait felhasználva történik, ami a vállalatvezetés rövid távú gazdasági tervével és érdekeivel ütközhet. Ennek feloldásához **minőségköltség modell** elkészítése szükséges, ami egyrészt igazolja a tulajdonosok és a menedzsment felé az irányítási rendszer működési költségeinek hatékony és optimális felhasználását, rámutatva olyan összefüggésekre, hogy a be nem következett veszteségek, az el nem szenvedett minőséghibák komoly megtakarítást eredményeznek egy cég gazdálkodásában.
A megelőzési költségek a minőségirányítási rendszer tervezésével, bevezetésével és fenntartásával kapcsolatos költségelemek összessége, - például a rendszeres adatgyűjtések, elemzések költsége, a mérőeszközök felügyeletének költsége **(R&R vizsgálatok**), **hitelesítés** és **kalibrálási** költségek -, de ide tartoznak az **oktatások, képzések** költségei is, valamint a folyamatszabályozási tevékenységek egyes ráfordításai.

A vizsgálati költségek közé tartoznak a **beérkező termékek és idegenáru vizsgálati költségek** - Acceptable Quality Level – AQL szintek figyelése -, beszállítók minősítésének költsége, **gyártásközi** és **végellenőrzések**, minőségellenőrzési eszközök költségei. Belső hibaköltségek a kiszállítás előtt észlelt költségek, - például selejt, esteleges javítási költségek, áruleértékelés veszteségei, a korrekciós intézkedések és az újbóli vizsgálatok költségei -, míg a külső hibaköltségek a kiszállítás után keletkezett költségek, ezek a visszahívás, jótállás és garanciális költségek. A minőségköltségek összetevőit a 3. számú ábra tartalmazza

3. Ábra Minőségköltségek összetevői
(Forrás: Medina, 2019)



Az összesített minőségköltségek függvényének alakja kádgörbe alakú, ami a jól szemlélteti a meghibásodási arány változását az alkalmazás időtartamának függvényében.

2.1.2. A minőségügy „gurui", minőségmenedzsment eljárások és technikák

„Nem muszáj ezt tenni. A túlélés ugyanis nem kötelező." Deming

A minőségügy „felfedezőinek" közös jellemzője, hogy mindegyikük saját filozófiát, egyéni megközelítésmódot alkalmaztak és munkáik során különböző módszertani eljárásokat dolgoztak ki a minőség fogalmi körében. Fontos megemlíteni, hogy a minőségmenedzsment technikák közül számosat az IBIR-ben is használunk, erre a későbbiekben példákat fogok mutatni. A minőségmenedzsment technikák egy része pedig a projektmenedzsmentből eredeztethető, egy IBIR bevezetési folyamata pedig nem más, mint egy összetett projekt, így ezek szintén megemlítésre kerülnek dolgozatomban.

Az Egyesült Államok első nagy minőség guruinak 1930-as években történő megjelenését megelőzte 1901-ben **Frederick W. Taylor** (1856–1915) amerikai mérnöknek a termelési módszerek forradalmi változására tett erőfeszítése. A Bethlehem Steel Co. acélműben folyó tevékenység során elválasztja a tervezési, termelési és a független ellenőri, minőségfelügyeleti tevékenységet. 1911-ben kiadja a „A tudományos irányítás alapelvei" című művét, amiben alapelveket fogalmaz meg a termelés irányítására vonatkozóan. 1907-ben **Henry Ford** (1863–1947) futószalagja a tömegtermelés kialakulásának jelentős lépcsőfoka, de 161 szabadalma a közlekedést és az USA iparát is forradalmasította. 1947-ben létrejön az ISO (International Organization for Standardization), a Nemzetközi Szabványosítási Szervezet.

Az amerikai minőségiskola képviselői közé tartozik **Walter A. Shewhart** (1891–1967), aki a termelésben tapasztalható ingadozásokat statisztikai módszerekkel elemezte, azokat pedig grafikonokon ábrázolta. **Dr. W. E. Deming** (1900–1993) lett a japán minőségügy megalapítója, tanácsai és 14 pontból álló menedzselési elvei a menedzserek minőségért való felelősségét hangsúlyozza. Előadássorozatai a PDCA ciklusról és a statisztikai módszerekről, valamint a teljes körű minőségirányításról mérföldkő lett a japán minőség megteremtésében. **Joseph M. Juran** (1904–2008) a minőségtervezés „térképének" megalkotója, véleménye szerint a minőség tervezésének, ellenőrzésének-szabályozásának és javításának hármas egysége biztosít elfogadható minőségszintet, a minőségspirál elmélete pedig a vevői igények figyelembevétele és a folyamatos termékfejlesztés kapcsolatát modellezi. **Armund V. Feigenbaum** (1920-2014) a TQC (Total Quality Control), a teljes körű minőségszabályozás koncepciójának megalkotója, kiterjeszti a minőségért való felelősséget a teljes szervezetre, továbbá véleménye szerint bármely tevékenység induló pontjában figyelemmel kell lenni a minőségre, nem elegendő az utólagos ellenőrzés. Ő egyben a minőségköltség fogalmának bevezetője is [Turcsányi 2014]. **George Stanley Radford** -The control of quality in manufacturing - A minőség ellenőrzése a gyártásban című könyve a 20. századelő jelentős hatású minőségbiztosítási szerzeménye.

A japán minőségiskola jelentősen hozzájárult a második világháborút követően a lerombolt gazdaságuk újjáépítéséhez, melyhez amerikai tőkére és modern menedzsment ismeretekre is szükségük volt. Az amerikai minőségiskola japán kulturális közegbe történő átültetése során a hangsúly áthelyeződött a kollektív felelősségre, a minőségügybe az alkalmazottak minden rétegét bevonva jött létre az ő „minőségi iskolájuk".

Az amerikai típusú individualista, felülről lefelé építkező, egyéni sikerorientált, a menedzsment teljes felelősségét hangsúlyozó kultúrával szemben itt az alulról jövő kezdeményezéseké, az alázaté, valamint a korfüggő bérezésen túl az élethosszig tartó foglalkoztatásé az a vállalati kulturális közeg, ahol a japán minőségiskola kialakult.

Kaoru Ishikawa (1915–1989) a dolgozók teljes körű bevonásának, a statisztikai technikák alkalmazásának és a minőségkörök megalkotójának atyja. A halszálka diagram használatának bevezetője [Kaoru I., 1991]. **Genichi Taguchi** (1924–2012) nevéhez a minőségveszteség fogalmának bevezetése kapcsolódik, aki a veszteséget nem csak a vállalat, hanem a társadalom egésze vonatkozásában értelmezte. A Taguchi féle kísérleti modell egy sokváltozós környezetben teszi lehetővé a kombinációk minimalizálásával a helyes matematikai modell megalkotását és a kísérletek számának jelentős csökkentését. **Masaaki Imai** (1930–2023) a KAIZEN (Kai=változás, Zen=harmónikus) filozófia legelismertebb szakértője. Nézete szerint egy olyan gondolkodásmódot kell képviselni, ami azt képviseli, hogy az életben minden dolgot jobbá lehet tenni, bármilyen tevékenységet lehet fejleszteni. A szervezet tagjainak teljes elköteleződése és bevonása mellett a vevői igények minél magasabb szintű kielégítése a célja, költségcsökkentésen, minőségfejlesztésen, a vevőkiszolgálás pontosságán és a rugalmasságon keresztül. Ez a gondolkodásmód nagymértékben megjelenik a LEAN menedzsmentben és a Total Productive Maintenance (TPM)-ben [Dévai, Fésüs, Kosztolányi, Kővári, Nika, 2020]. A Gemba séták gyakorlójaként azt az elvet vallotta, hogy helyszíni adatgyűjtés nagyon fontos a folyamatok jobbá tételében, a “Menj, nézd meg, kérdezd meg, miért, és tanúsíts tiszteletet!” jelmondat fontosságát hangsúlyozta. **Shigeo Shingo** (1909-1990) japán mérnök, a POKA-YOKE - véletlenszerű hibák kiküszöbölése ,- rendszer megalkotója és a Toyota Termelési Rendszer szakértője. A technológiai folyamatok és a szerelési hibák megelőzésére helyezi a hangsúlyt. **Taiichi Ohno** (1912-1990) a Toyota Termelési Rendszer megalkotója, a Just in Time és a Lean menedzsment előfutáraként nevéhez fűződik a veszteségtípusok hét csoportba sorolásának kategorizálása, ezek: anyagmozgatásból, készletfelhalmozásból, mozdulatokban rejlő, várakozásból fakadó, túltermelésből adódó, felesleges tevékenységek végzése miatti, javításból eredő veszteségek. **Shoji Shiba** japán professzor a Total Quality Management (TQM) módszerek kidolgozásáért, nem mellesleg a hazai minőségügy meghonosítójaként és a hét lépéses problémamegoldás kifejlesztésével vált ismertté. [Fehér

2023]. A problémamegoldás hét lépésének és a PDCA ciklusnak a kapcsolatát a 3. számú táblázat tartalmazza:

3. Táblázat: PDCA ciklus és a hétlépéses problémamegoldás kapcsolata
Forrás: Leanforum.hu alapján saját szerkesztés

PDCA	**7 minőségjavítási lépés**	**7 hagyományos minőségeszköz**
PLAN	1. A téma kiválasztása 2. Adatgyűjtés és elemzés 3. Az okok elemzése	<u>Ötletgyűjtő technikák:</u> • Brainstorming (ötletroham) • Brainwriting • 635 módszer • Philips 66 módszer • Delphi módszer • K-J diagram vagy affinitás diagram. • Nominális csoport technika <u>Adatgyűjtés és elemzés technikái:</u> • Adatgyűjtés az 5W + 1H módszerrel • Adatgyűjtő lapok alkalmazása • Pareto elemzés • Hisztogram, vagy kumulatív görbe rajzolása • folyamatábra • szórásdiagram • Ishikawa (Ok-okozati) diagram <u>Ok-okozati elemzés módszerei:</u> • regressziós, korrelációs és kovariancia elemzések • Ishikawa diagram • Valószínűségi elemzés, hibafa felrajzolása • Fadiagram, kapcsolati diagram • Flow-chart (folyamatdiagramm)
DO	4.Ellenintézkedések megtervezése és a megoldás bevezetése	• Hálótervezési módszerek, (Gantt-diagram, PERT, CPM, RAMPS)
CHECK	5. Az eredmények értékelése	• Ellenőrző diagram, Adatgyűjtő lapok, hisztogram, szórásdiagram, Ishikawa diagram
ACT	6. A megoldás szabványosítása 7. Visszacsatolás a folyamatról és a következő problémáról	

Shoji Shiba vezette be a **hét új vezetői eszközt**, melyekkel az adatok elemzése, valamint a folyamatok ábrázolása és a döntéshozatali problémák kezelhetőek [Drégelyi, Farkas, Galla, Tóth 2013]. Ezek felsorolásszerűen:

1. **Affinitás, vagy KJ diagram** (Kawakita Jiro): adatokat csoportosítunk benne a közöttük lévő kapcsolatok alapján,
2. **Kapcsolati diagram**: Ok-okozati kapcsolatok feltárására alkalmas,
3. **Fa diagram**: egy esemény okait a gyökérokig vezeti vissza, hibafa és eseményfa változatát használjuk. Utóbbiban az egyes események bekövetkezésének valószínűségével is számolunk,
4. **Mátrix diagram**: problémák jellemzőinek mátrix elrendezésben történő szemléltetése, a kapcsolatok szorosságának feltárása,
5. **Nyíl diagram**: a feladatok sorrendjének meghatározására használjuk, tulajdonképpen egy egyszerű Gantt diagramként is értelmezhető,
6. **PDCP ábra**: segítségével meghatározhatjuk, hogy mi mehet rosszul egy folyamatban, egy folyamatsor valamennyi kimeneti eseményének megismerésére szolgál, rokonságban van az FMEA-val és az eseményfával,
7. **Mátrix adatelemzés ábra**: adatokat rangsorolunk és szemléltetünk benne.

Takashi Osada az **5S módszerével**, ami a japán megnevezések kezdőbetűiből alkotott mozaikszó vált ismertté. Segítségével a munkahelyi hatékonyságot, eredményességet és biztonságot lehet növelni, ráadásul egy végtelenül egyszerű módszer. A japán szavak szó szerinti fordítása a szelektálás, szervezés, szépítés, szabványosítás és szinten tartás. Elsősorban a munkakultúrát javítja. Japán eredetű, elterjed és széleskörűen használt minőségmenedzsment módszereket dolgozatom *10.1 számú melléklete* tartalmazza. Az információbiztonsági keretrendszerekben ezek közül többet alkalmazunk, a KANBAN például a szoftverfejlesztésben is megvetette a lábát.

Végül a minőségguruk harmadik csoportját alkotják az „újhullámos” képviselők. Közülük említést érdemel **Philip B. Crosby** (1926–2001) a „nulla hiba” program megalkotója és számos minőségmenedzsment könyv szerzője. Nulla hiba programja felkeltette a hadiipar és a kormányzat érdeklődését is, a vevői igények felmérésére, jobb megértésére és a minőség átfogó definíciójára adott válaszai pedig napjaink minőségmenedzsment rendszereire is nagy hatást gyakorolnak. **James Harrington** üzleti folyamatok 5 lépéses fejlesztése, valamint a gyakorlati minőségi módszertanok és üzleti folyamatfejlesztési koncepciók alkalmazásának világszerte elismert képviselője. **John Oakland** a Teljes Körű

Minőségmenedzsment, a TQM modell kidolgozásával lett ismert, mely a vevőközpontúság, folyamatos javítás, a vezetőség minőség melletti elköteleződése és az alkalmazottak felhatalmazásának elveire épül.

Hazai képviselőik közül kiemelném **Fehér Norbert** munkásságát, aki a minőségmenedzsment szakértőjeként számos könyv szerzője, Lean és Six Sigma specialista.

A termék, gyártás és gyártmánytervezés, valamint a teljes termelés vertikumában megjelenő, minőséghez is kapcsolódó módszertanok és technikák szintén részét képezik a vállalatok minőségirányítási rendszerének, ezek közül a fontosabbak:

- **QFD (Quality Function Deployment):** a minőségkövetelmények és a vevői elvárások, valamint a mérnöki, műszaki, technológiai termékjellemzők, azok közötti korrelációt vizsgáló, továbbá a konkurencia már piacon jelenlevő termékei közötti kapcsolatot megteremtő módszer. Először Yoji Akao japán mérnök mutatta be, vizuálisan egy kapcsolat mátrix elrendezésű alakzatban, -ez a minőség háza-, jeleníti meg a piaci igények (MIT) és a termékjellemző (HOGYAN) közötti összefüggéseket. Olyan cégek alkalmazták először, mint a Mitshubishi, Toyota, Kodak, továbbá vezető elektronikai és autóipari cégek, pl. a Ford. [Koczor 2010].
- **DOE: (design of experiment):** kísérlettervezéshez kapcsolódó módszertan, egy folyamat bemenetei és kimenetei közötti függvényszerű kapcsolat feltárásával (transzferfüggvény), a szükséges kísérletek számának jelentős csökkentésével tudja a fejlesztési időt lényegesen lerövidíteni. A Six Sigma rendszer DMAIC - define, measure, analyze, improve and control -, modelljében az improve szinten lép be a fejlesztési folyamatba.
- **FMEA (Failure Mode and Effect Analysis, hibalehetőség és hatáselemzés):** hibaok, hibahatás és annak megjelenése közötti összefüggéseket vizsgáló, kockázatelemző módszertan. A kockázatokat nagyágát súlyozással (RPN, Risk Priority Number), a hiba felismerhetőségének, gyakoriságának és a következmény súlyosságának szorzataként állítja elő, az információbiztonsági kockázatkezelésben is használt módszertan.

Ma már széleskörűen alkalmazzák, nem csak az autóiparban. Felhasználási területe alapján beszélhetünk rendszer, üzemeltetési, konstrukciós, vagy folyamat FMEA-ról. [Fehér 2018].

- **TPM (Total Productive Maintenance - Termelékenységközpontú Karbantartás)** AZ 1960-as években Japánban kialakuló, átfogó műszaki és menedzsment elemekből álló, elsősorban a termelő berendezésekhez köthető, felesleges állásidők kiküszöbölését célzó és a selejtgyártást megelőző rendszer.
- **HEP (Human Error Probability-Emberi hibavalószínűség):** Az emberi megbízhatóság számszerűsítésére, matematikai modellezésére kidolgozott módszertan, a bekövetkezett hibák és a hibalehetőségek arányából következtet a megbízhatóságra. Vezérlőtermi, irányítótermi, légiközlekedés légiforgalmi és a pilóták munkavégzéséhez, kockázatelemzéséhez kiváló eszköz.
- **Radar diagram:** több változós adathalmazból a mérhető mennyiségeket több tengely mentén felvéve egy pókháló képét kapjuk, a kapott síkidom alakja és mérete megmutatja a követelmények kielégítésének szintjét, mértékét.

A minőségtechnikák legújabb tagjai, melyek napjaink komplex minőségmenedzsment módszereit képezik, egyes elemeit a projektmenedzsmentből vette át a minőségügy:

- **5 miért módszer**: 5 kérdés feltevésével keresi a probléma okait.
- **Erőtér elemzés**: ható és fékezőerők szemléltetésére alkalmas.
- **CEDAC** módszer: Ok-okozat diagram kiegészítése üzenő kártyákkal, a hiba kijavításának is célja ennek a módszernek a használata.
- **Run Chart** és **Multi var Chart** ábra: a statisztikai folyamatszabályozás szabályozó kártyáira hasonlító módszer, vizuálisan szemlélteti a termelési darabszám és a változékonyság időbeli változását.
- **Szabályozatlanság 8 kritériuma** módszer: folyamat stabilitását a normális eloszlás mellett a mérési pontsorozat trendjét is figyelembe veszi.

- **Potenciális Probléma elemzés módszere (PPA):** a probléma megelőzésének lehetőségére fókuszáló módszer, tehát nem csak okokat vizsgálja.
- **Prioritási és Döntési Mátrix módszerek**: a tevékenységek fontossági sorrendjét állítja középpontba, a megtett erőfeszítés (idő-költség), az elért hatás függvényében.
- **Tevékenység hálózat diagram**: a projekt tevékenységeinek, feladatainak, időbeli lefutásának tervezésére és szemléltetésére alkalmas módszer, már a kritikus út meghatározására is képes.
- **PERT** módszer (Programme Evaluation Review Technique): bizonytalan végrehajtási idejű, ezért valószínűségszámítási és statisztikai alapú módszertan a projektfolyamatok mérföldköveinek és végrehajtási idejének meghatározására.
- **CPM (Critical Path Method) háló** módszere: tevékenységtípsusú és feladatorientált, gráfelméleti alapokon nyugvó, idő és költségoptimalizálásra alkalmas projektmenedzsment technika [Daróczi 2019].
- **Logframe mátrix**: (logikai keretmátrix rendszer): problémafelvetés, célok kijelölése, az eredményességi mutatók meghatározása és objektív módon történő méréséből jelöli ki a projekt tevékenységi lépések sorozatát, a hatás és cél, valamint az eszközök mutatóinak felhasználásával.

Az általános menedzsment módszerek között pedig meg kell említeni a versenytársak és saját teljesítményünk összehasonlítására kidolgozott, Japánból származó **Benchmarking-ot**, ami termék, versenytárs, vagy folyamatok összehasonlító elemzése a legjobb gyakorlat átvételére, egyben a saját folyamtok és szervezeti struktúra fejlesztésére. Az **üzleti folyamatok újratervezése (BPR - Business Process Reengineering)** az áttöréses, radikális változások stratégiai menedzsmentet érintő módszertana. Jelentheti egyetlen üzleti folyamat, egy technológia, vagy egy teljes szervezet újjáalakítását is. Régi szabály-új szabály és szabálytörő technológia vagy folyamat mentén, a felesleges, értéket nem termelő vállalati tevékenységek elhagyásával, radikális költségcsökkentéssel, szervezeti karcsúsítással és ezek kombinációjával ér el eredményt ez a módszertan. A mutatószámok világában, melynek IT vonatkozásai is vannak, **a kiegyensúlyozott teljesítmény-mutató rendszer (BSC - Balanced Scorecard)** az**,** ami a pénzügyi-számviteli mutatószámok múltra vonatkozó

információi mellett, a jövőre vonatkozó terv-cél kontrolling és a teljesítménymutatószámok rendszerének jelenre vonatkozó elemeit kapcsolja össze.

2.1.3. A vállalati adatvagyon és az erőforrástervező rendszerek

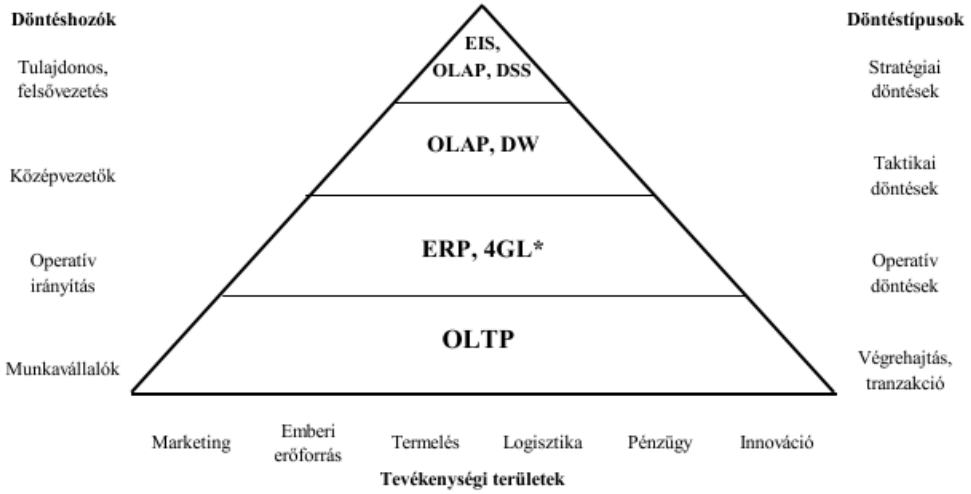
Az információbiztonság-minőségmenedzsment-vállalati adatvagyon összefüggésében szükséges a vállaltirányítási rendszerek kialakulását és jelenlegi helyzetét bemutatni, hiszen ez az egyik olyan dimenziója a vállalati működésnek, aminek megfelelő védelméhez, folyamatainak javításához az IBIR nagymértékben hozzájárul. Hatalmas szakirodalom, megannyi szabvány és ajánlás jött létre a vállalti adatvagyon menedzselésére, az alább látható szófelhő mutatja ennek a témakörnek az összetettségét:

4. Ábra: Szófelhő a vállalati adatvagyon menedzselésére kialakult renszerekből, fogalmakból *(Forrás: Saját szerkesztés)*

Jelenleg a **vállalti erőforrástervező rendszerek** (ERP- Enterprise Resource Planning) hordozzák a maguk komplexitásában és ma már centralizáltságában szinte a teljes vállalati adatvagyont. Ha valami centralizált, annak számos előnye mellett megvan az a hátrányos tulajdonsága, hogy a központi részének kiesésével azonnal megakasztja a kliens egységek működését, Az INTERNET kialakulásában nem véletlenül játszott szerepet egy szimulált katonai támadás az USA információs infrastruktúrája ellen, a teljes decentralizált struktúra egy átfogó atomcsapás esetén is biztosította volna a létfontosságú rendszerek további működését. A vállalati információs rendszerek kialakulása szinte egyidőre tehető a számítástechnika széleskörű elterjedésének kezdetével.

Egy vállat rendszerként értelmezhető, input és output elemekkel kapcsolódik környezetéhez, belső folyamatai vannak, különböző szintjein pedig döntéshozók állnak, akik megfelelően szervezett, tárolt és feldogozott adatokból, adatbázisokból, - ideális körülmények között-, releváns, pontos, időszerű, teljeskörű és könnyen érthető adatokat kapnak, melyek a döntéshozási folyamatban az egyes cselekvési alternatívák közötti választásban segít [Kovács 2011]. Az üzleti élet egyre komplexebbé válásával, a megfelelő adatbáziskezelő matematikai modellek fejlődésével párhuzamosa a menedzsment információs rendszerek alkalmazási területe kiszélesedet, és ma már a cégek teljes funkcionális tevékenységét lefedik. Az első, **elektronikus adatfeldolgozó rendszerek** (Electronic Data Processing - EDP) az 1950-es években jöttek létre, csupán adatok egyszerű bevitelére és tárolására voltak alkalmasak. Alig tíz évvel később már az adatok kötegelt feldolgozását támogató, adatok nagy mennyiségben történő feldolgozását elősegítő **tranzakció feldolgozó rendszerek** (Transaction Porcessig System -TPS) jöttek létre, ezeket a valós idejű tranzakciókezelést végző **OLTP rendszerek** (Online Transaction Processing) váltják. A számítástechnikai rendszerek teljesítményének, a megfelelő matematikai és adatmodellek adaptálásával, a programozási nyelvek és fejlesztői környezetek szélsebes fejlődésével, **a gyártási erőforrástervező rendszerek** mellett a vezető döntéstámogatást segítő **felsővezetői információs** (Executive Information System) és **szakértői rendszerek** (Expert System -**ES**) is elterjednek. A tranzakció alapú rendszereket **az analitikus rendszerek** (**OLAP** Online Analytical Processing) váltják, az adatmodell matematikai alapját pedig a Codd féle relációs algebra adja, az adatok tárolásának és lekérdezésének szabványos nyelve az SQL (Structured query language) lett. [Michelberger 2017]. A vezetői döntéstámogatás informatikai támogatásának különböző szintjeit szemlélteti az 5. számú ábra:

5. Ábra: Információtechnológiai piramis
(Forrás: Michelberger 2017.)



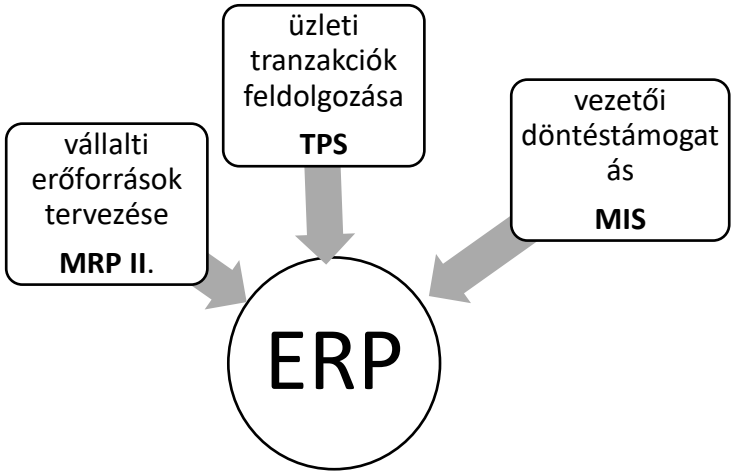
Jól látszik, hogy az operatív tevékenység elemi tranzakcióit feldolgozó OLTP rendszer, a problémakör egyre bonyolultabb válása során, a jól strukturált adatokat átadja az analitikus rendszereknek, melyek képesek rosszul strukturált adatokból is, több változós, és sztochasztikus rendszerekben egyaránt hatékony vezetői döntéstámogató funkciót nyújtani.

A gyártásban **az anyagigény tervezési rendszerekből** -Material Requiment Plannig , kiegészülve a **kapacitásszükséglet tervezési rendszerekkel** létrejön a **gyártási erőforrások tervezési rendszere**, a Manufacturing Resources Planning -MRP II. [Husti 2020]. Az irodai munkát pedig az **irodaautomatizálási** – Office Automation System -OAS – és **dokumentum menedzsment** -DMS- rendszerek segítik, széleskörű szoftveres és hardveres támogatással.

6. Ábra ERP rendszerek funkciói
(Forrás: Innolog Kft 2023)

Az ERP rendszerek funkcióit a 6. ábra szemlélteti. Valamennyi ERP, kiszereléstől, fejlesztőtől függetlenül az alábbi három alapfunkciót minden esetben biztosítja, melyet a 7. ábrán szemléltetek:

7. Ábra ERP rendszer három alapfunkciója
(Forrás: saját szerkesztés)



Az ERP rendszerinek jellemzője, hogy moduláris felépítésűek, de az integrált felépítéséből adódóan a vállalati funkciók szinte minden elemét képesek támogatni:

- gyártás, termelés tervezés/irányítás és minőségbiztosítás,
- teljes ellátási lánc és beszerzés menedzsmentje (SCM, SRM),
- kutatás fejlesztés és mérnöki tevékenységek,
- vállalati eszközmenedzsment (EAM),
- pénzügy, könyvelés, Controlling és Terasury funkciók,
- emberi erőforrásmenedzsment,
- értékesítés, marketing és disztribúció, és ügyfélkapcsolatok (CRM),
- termék életciklus menedzsment funkciók (PLM).

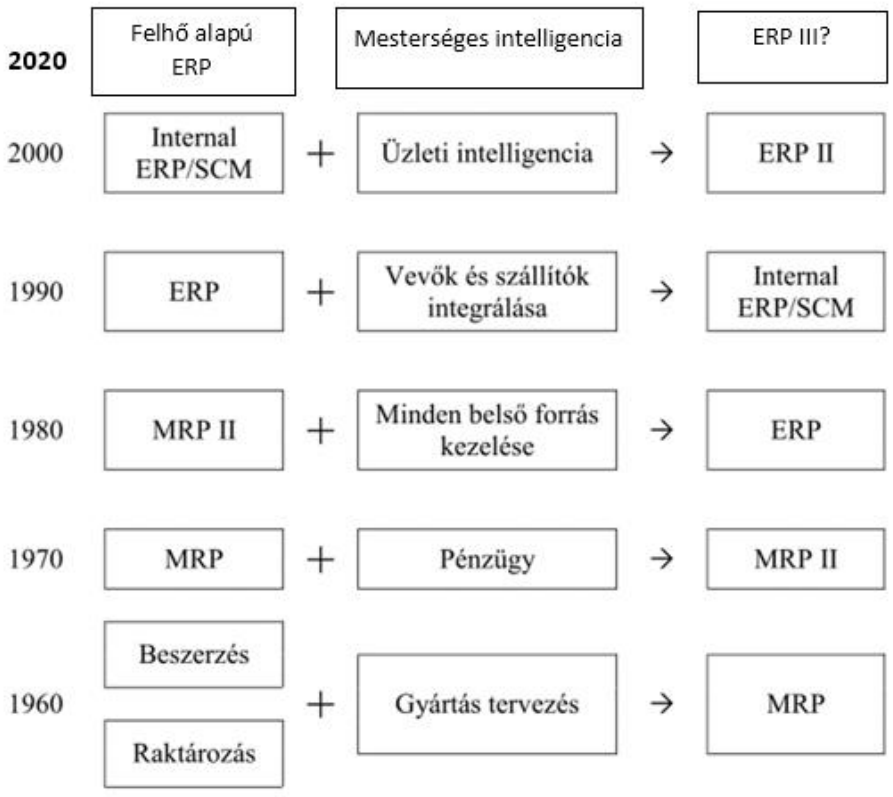
Mérnököknek, tervezőknek készültek a termék, gyártás és gyártmánytervezésben elterjedt **CAD/CAM rendszerek**, melyek nagyon erős információtechnikai támogatást kaptak (olyannyira, hogy ma már nagyon ritkán készülnek például kézi tervrajzok). Ezek fejlesztését úgy valósították meg, hogy illeszkedjenek az előbbi bekezdésben bemutatott informatikai megoldásokhoz, ERP-hez, EAM- Enterprise Asset Management-vállalati eszközgazdálkodó

rendszerekhez, elkerülve a szigetszerű működést. A következő moduljai ismertek [Michelberger 2017]:

- gyártmánytervezés (CAD – Computer Aided Design),
- gyártási folyamatok tervezése (CAPP – Computer Aided Process Planning),
- termeléstervezés és irányítás (PPS – Production Planning System)
- gyártás (CAM – Computer Aided Manufacturing),
- anyagszállítás és tárolás (CAST – Computer Aided Storage and Transport),
- minőségszabályozás (CAQ – Computer Aided Quality).

Az ERP-k fejlődése során az adat alapú rendszereket, melyek az adatok gyűjtésére és tárolására fókuszálnak, felváltja a szakirodalomban a C-ERP megnevezéssel illetett újabb korszak, amelyek már a folyamatok fejlesztésére és optimalizálásra helyezik a fő hangsúlyt, mivel az adatgyűjtés és tárolás funkciót a fejlett informatikai algoritmusok és a mesterséges intelligencia emberi beavatkozás nélkül is megfelelő minőségben tudja elvégezni. Ezt a fejlődési folyamatot mutatom be a 8. ábrán.

8. Ábra Az integrált vállalatirányítási rendszerek evolúciója
(Forrás: Turban et al (2002) alapján saját szerkesztés)



ERP-k piaca rendkívül kompetitív, jelenleg a legfontosabb szállítói és fontosabb termékeik [Elevatiq 2023]:

1. Oracle: Netsuite és Oracle Cloud ERP
2. SAP: S/4 HANA Suite, SAP Business One
3. Microsoft: Microsoft Dynamics 365 Business Central
4. Infor: több termék,
5. Sage: Sage X3 Business Cloud
6. Epicor: Epicor Resource Planning

A 2000-es években megjelentek a rosszul strukturált adatok kezelésére képes, már a mesterséges intelligencia előfutáraként kezelhető **intelligens üzleti informatikai megoldások**, -pl. az **adatbányászat**- ami napjainkban a **neurális hálózatok** és **nyelvi modellek** elterjedésével a tanulási képességekkel felruházott mesterséges intelligencia széleskörű megjelenésénél tart. A CHATGPT, a Google Bard, Microsoft Bing Chat, OpenAI, a virtuális és kiterjesztett valóság korát éjük, ezek pedig a modern vállalatirányítási rendszerekben is megjelentek, például az adatvizualizációban, adatbányászatban.

Az üzleti szoftverek kiválasztását nagymértékben segítő Capterra honlapján jelenleg több mint 400 ERP termék rövid ismertetője és elérési útvonala található. Jellemző erre a nemzetközi piacra, hogy a felhasználók száma és a szoftver robusztussága, méretezhetősége és skálázhatósága, valamint a bevezetés időigénye alapján **Tier 1-2-3** csoportba sorolják őket.

- Tier 1: Oracle, SAP, MS Dynamics 365 Business Central, Infor
- Tier 2: Abas, Netsuite, Deltek, Sage Intacct
- Tier 3: a kisebb rendszerek csoportja, rengeteg ERP található itt, kifejezetten a kisméretű vállalkozások számára kifejlesztve.

A hazai piacon a Cégmenedzser vállaltirányítási rendszere, a Revolution Deep Erp-je, a dlmsolution DLM TruMES rendszere, és persze a régebbi temékek, az Abas, Libra11, Cobra, az Infosys, exPanda a legismertebbek, de nagyon sok kisebb és új feljlesztőcég jelent meg a piacon, modularitást, alacsonyabb fejlesztési és bevezetési költségeket és egyéb pénzügyi konstrukciókkal, - például tartós bérlés -, támogatva az ERP-k széleskörű hazai elterjedését.

ERP-t használó hazai cégek 2022-es iparági megoszlásának táblázatát, az XAPT Hungary Kft. kivonatos felmérése alapján -dolgozatom 10.*2. számú melléklete* tartalmazza.

2.2. Információtechnológiához, információbiztonsághoz kapcsolódó szabványok, irányítási és projektmenedzsment rendszerek

2.2.1. Szervezetek, szabványok és ajánlások

Az ISO 27.000-es szabványcsalád mellett az információbiztonságot érintő technológiában rengeteg szabvány, ajánlás jött létre, melyek a mai napig sem egységesek. Mindegyikük fogalmaz meg azonban követelményeket műszaki leírásokra, ellenintézkedésekre, folyamatokra és kockázatkezelésre. A **szabványok kiadásáért felelős szervezetek** alapján nemzetközi, nemzeti és regionális szabványokat különböztetünk meg. A közismert Nemzetközi Szabványügyi Testület (ISO) mellett az alábbi szervezetek foglalkoznak elektronikus, IT szabványok kiadásával, gondozásával:

- ANSI: American National Standards Institute,
- IEC: International Electrotechnical Commission,
- IEEE: Institute of Electrical and Electronics Engineers Computer,
- Society Software Engineering Standards Committee,
- CEN: Comité Européen de Normalisation,
- CENELEC: Comité Européen de Normalisation Électrotechnique,
- ITU-T (CCITT): International Telegraph Union,
- EIA: Electronics Industry Alliance,
- TIA: Telecommunications Industry Association,
- ETSI: European Telecommunications Standards Institute,
- ICANN Internet Corporation for Assigned Names and Numbers.

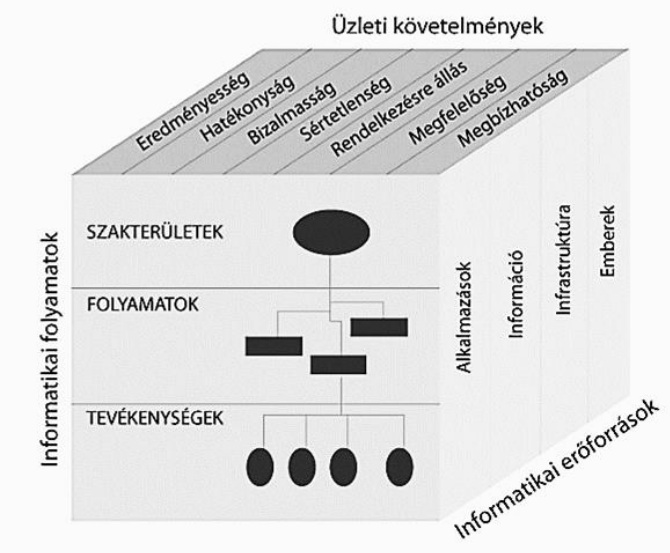
Az információtechnológia szakmai szervezetei közül az **ISACA** (Information Systems Audit and Control Association) az egyik legismertebb, az egyesület 180 országban 140 ezer taggal képviselteti magát.

Az információbiztonsági auditorok, minőségbiztosítási, kockázatkezelési és IT szakemberek szövetségeként a **COBIT** (Control Objectives for Information and related Technologies) módszertant dolgozta ki, elsősorban a nagyvállalati informatika támogatásában játszik szerepet. Négy területen végez szakemberek számára minősítési programot:

- a CISA az auditorok,
- a CISM az információ biztonság területén tényked̋ők,
- a CGEIT az IT szervezeti vezetők,
- a CRISC pedig a kockázatkezeléssel foglalkozók.

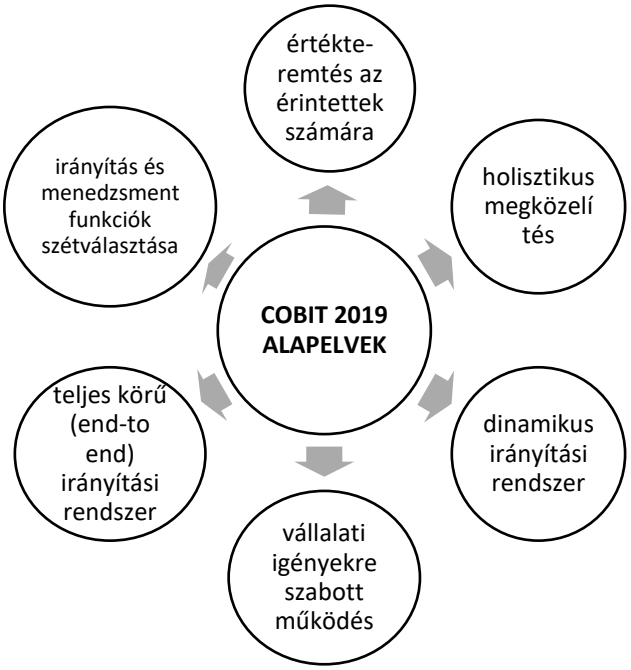
A COBIT, mint nemzetközileg elismert informatikai irányítási **keretrendszer** az üzleti és szervezeti céloknak az informatikai kockázatkezelésnek, a kialakítandó kontrolloknak és stratégiának legjobb gyakorlataira ad módszertant, nyílt szabványnak tekinthetjük. Jelenleg a 2019-es a legfrissebb verziója. Hat folyamatképességi szintet határoz meg érettségi modellek alapján, a kockázatokra adott „ne tegyünk semmit” megközelítésből öt fokozatú skálán jut el az „emberi tűzfal” szintjére, ahol a biztonságtudatosság legmagasabb fokára a rendszeres képzéseken, tájékoztatásokon keresztül jutnak el a szervezet munkatársai. [TARJÁN GÁBOR doktori értekezés 2020]. Üzleti követelmények-folyamatok-IT erőforrások dimenzióiban ad megoldást az IT Governance (IT-menedzsment tervezésének és működtetésének váza) támogatására és üzemeltetésére. Ez a Cobit kocka. (Szádeczky 2014), amit a 9 ábrán mutatok be.

9. Ábra: COBIT kocka
(Forrás: Szádeczky 2014)



A COBIT 2019 hat alapelvet tartalmaz az irányítási kerethez:

10. Ábra: COBIT 2019 alapelvei
(Forrás: Saját szerkesztés)



További ismert szabványok, ajánlások, módszertanok gyűjteményei:

- **TCSEC** Trusted Computer System Evaluation Criteria, Orange Book of DoD (1985), USA védelmi minisztériuma által készített szabvány a számítógépes rendszerek biztonsági szintjének meghatározásához.
- **ITSEC** Information Technology Security Evaluation, a TSEC európai megfelelője, szintén védelmi szinteket határozott meg a biztonsági követelményekben.
- **COMMON CRITERIA** for Information Technology Security Evaluation part, (ISO/IEC 15408). Az informatikai termékek és rendszerek biztonsági értékelésének standardját jelenti, röviden CC-ként említve. Ez a rendszer meghatározza azokat a követelményeket, amelyek alapján értékelhetők és minősíthetők az informatikai termékek és rendszerek, gyakorlatilag egyfajta szabványok, követelmények gyűjteménye a biztonság tekintetében. A Nemzetközi Szabványügyi Szervezet ISO/IES 15408 számon adta ki, Magyarország pedig az MSZ ISO/IEC 15408:2002 számon honosította

- **ITIL**: (Information Technology Infrastructure Lirary) kialakulásában nagy szerepe volt annak, hogy szükségessé vált egy olyan gyakorlati módszertan és modell kidolgozása, amely elsősorban a felhasználók és ügyfelek igényeire összpontosít a technológia orientált szervezési kérdések helyett. Eredetileg brit szabványként (BS 15.000) és kormányzati ajánlásként jött létre. Később az IT Service Management Forum International segített az elterjedésében és az egységes maradásában. 2005-ben az ISO/IEC 20.000 szabvány kialakításához is hozzájárult. Az ITIL azóta más informatikai szolgáltatáskezelési megközelítésekkel is összekapcsolódott, mint például a Microsoft Operation Framework (MOF), a CMMI módszertan és a COBIT. [Muha, Krasznay 2014]: A Magyar Szabványügyi Testület is honosította a szabványt, amelynek pontos megnevezése: "Az informatikai szolgáltatás irányítási rendszerek, jelenlegi hatályos változata az **MSZ ISO/IEC 20000-1:2018**. Az ITIL a PDCA (Plan-Do-Check-Act) elvet alkalmazza a minőségi és megbízható, költséghatékony IT szolgáltatások támogatásához. Az ITIL-ben meghatározva vannak mind a kulcsfontosságú folyamatok, mind a folyamatok közötti kapcsolatok. Az ITIL beilleszti az üzleti folyamatokba a szolgáltatási szintű megállapodásokat (SLA-k), és holisztikus megközelítést alkalmaz az üzleti informatikai, az üzleti kulcsfolyamatok és a vevői igények kielégítésében. Nemzetközi és hazai képzések és vizsgák segítik a szakemberek minősítését. (ITIL® 4 Foundation akkreditált vizsgák)

Az **ISO 31000:2018 Vállalati Kockázatkezelési Rendszer Tanúsítvány**, amely nem kontroll, hanem célkitűzés alapú, tanúsítható szabvány, a vállalat teljes tevékenységére ír elő kockázatmenedzsment szintű eljárásokat, integrálható az egyéb minőségirányítási rendszerekkel, egyre több haza vállalkozás alkalmazza működése során. Fontos felismerése a kockázatkezelési modelljének, hogy a hagyományos kockázatkezelési eljárások során a kockázat állapotának meghatározása során, a költség haszon elemzés utáni válaszintézkedéseknek - ezek lehetnek az elfogadás, kezelés, áthárítás, megszüntetés -, a maradványkockázatok elfogadási tartományában a gyakoriság a valószínűség és a következmény szorzataként még mindig maradhatnak olyan lehetőségek, melyek kezelése szükséges.

A kockázati térkép a hagyományos modellben nem jeleníti meg a ritkán előforduló, soha meg nem történt eseményeket, az események bekövetkezési láncolatát, valamint az audit figyelmét is inkább a nagy hatású és magas bekövetkezési valószínűségű eseményekre irányítja. A **kockázatkezelési technikákat**, módszertanokat tartalmazó szabvány az **IEC 31010:2019** számon került bevezetésre.

Az információbiztonság kockázatmenedzsmenttel foglalkozó szabványa az **ISO/IEC 27005:2018** szabvány, amely részletes iránymutatásokat és eljárásokat tartalmaz az **információbiztonság kockázatkezelésére** vonatkozóan. A követelményrendszer segít az információbiztonsági kockázatok azonosításában, értékelésében, kezelésében és felügyeletében, pl. IT vagyonelemek, fenyegetések, meglévő folyamatszabályozások, sérülékenységek, és azok következményei.

ISO/IEC 38500:2015 (Information technology Governance of IT for the organization) a **vállaltirányítás és az informatikai irányítást** szabályozza irányelvek és jó gyakorlatok meghatározásával. A vezetők szerepét és felelősségét jelöli ki és meghatározza azokat az alapelveket, hogy hogyan kell az informatikai tevékenységeket a vállalatirányítás szempontjából összehangolni és felügyelni.

ISO/IEC 15504 folyamatfelmérési és irányítási képesség vizsgálati szabvány, valamint az **ISO 55000:2014 vagyongazdálkodási szabvány** szintén tartalmaz az információbiztonság témakörében hasznosítható követelményeket, módszertanokat. [Nemzetközi Szabványügyi Testület, ISO.org 2023].

A tanúsítások, kockázatkezelés, ellenintézkedés szabványai mellet olyan IT-t érintő terméktervezéshez, gyártáshoz szükséges műszaki szabványok is léteznek, melyeket szinte lehetetlen felsorolni, csoportosítva feltüntetek néhány szabványt, ajánlást:

- biztonságtechnikával, vagyonvédelemmel és infokommunikációs hálózatokkal kapcsolatos termékek, eljárások szabványai,
- távoli hozzáférést szabályozó eljárások,
- digitális aláírásokat szabályozó módszerek,
- autentikációval, időbélyegzéssel kapcsolatos leírások,
- hálózati eszközök hardveres és szoftveres követelményeit szabályozó szabványok,
- információbiztonsági incidensek kezelésének módját előíró szabványok,

2022. -ben megjelent az **ISO/IEC 27001**-es szabvány **új kiadása**, valamint ennek „A” mellékletében található kontrollok értelmező és magyarázó szabványa az **ISO/IEC 27002:2022** A követelmények leírását tartalmazó rész kis mértékben, míg az „A” melléklet kontroll melléklete jelentős mértékben változott. A technika, technológia változása indukálta a felülvizsgálatot és az új kiadást. Ezek közül a legjelentősebbek:

- a kibertér használatának jelentősége, a felhő alapú szolgáltatások rohamos és széleskörű elterjedése,
- a virtualizáció (hypervisor), és konténerek (docker) alapú informatikai megoldások,
- a home office-ban történő munkavégzés széleskörű növekedése,
- maradt a HLS (High Level Structure), ami az ISO irányítási rendszerek fő jellemzője, az egységes felépítés nagyban megkönnyíti az integrált irányítási rendszerek kialakítását és auditálását,
- az ellenintézkedések száma a korábbi 114-ről 93-ra csökkent, négy tématerületben:
  - technológiai intézkedések, 34 db,
  - fizikai védelemmel kapcsolatos intézkedések, 14 db,
  - szervezeti intézkedések, 37 db,
  - humán erőforrásokkal kapcsolatos intézkedések, 8 db.
- bevezetésre került **11 új információbiztonsági témakör,** a 4. táblázatban mutatom be őket, jól látszik, hogy az adatvédelmi és felhőszolgáltatással kapcsolatos követelmények már hangsúlyosabb szerepet kapnak.

4. Táblázat Új témakörök és kontrollok
(Forrás: Horváth, Horváth 2023)

Témakör	Kontroll neve	Terület
5.7	Fenyegetettségi információk	szervezeti
5.23	Információbiztonság a felhőszolgáltatások használatakor	szervezeti
5.30	IKT felkészülés az üzletmenet folytonosságához	szervezeti
7.4	Fizikai biztonság felügyelete	fizikai
8.9	Konfigurációkezelés	technológiai
8.10	Információk törlése	technológiai
8.11	Adatmaszkolás	technológiai
8.12	Adatszivárgás megelőzése	technológiai
8.16	Monitoring tevékenységek	technológiai
8.23	Webszűrés	technológiai
8.28	Biztonságos fejleszté	technológiai

- Az új kontroll szabvány pedig bevezeti az **attribútumok** fogalmát, ezzel az egyes intézkedéseket lehet kategorizálni a megelőző, felderítő, javító, bizalmasság, integritás, rendelkezésre állás stb., kategóriákba.
- Az információk törlése, adatmaszkolás, adatszivárgás megelőzése kontrollok beemelése a személyes adatok védelmi szintjének növelését segíti elő, a GDPR megfeleléssel összhangban [Horváth, Horváth 2023.]

A 27 000-es szabványcsalád tagjai **65 publikált tagból állnak, 13 jelenleg is fejlesztés alatt van,** - Big Data Security, IoT security and privacy -, számozásuk a 27 000-től kezdődően 27 799-ig tart, ennek bemutatása meghaladja a dolgozatom terjedelmét, de jelzi, hogy mekkora méretű szabályozási területhez ad követelményrendszert és módszertani útmutatót. Tagoltságát tekintve a következő részekből áll: [Alan, Steve 2019].

- Áttekintés és szótár,
- Követelmények,
- Útmutatók: gyakorlati útmutatók a bevezetéshez,
- Auditok, követelmények a tanúsítóknak, auditálási útmutatók,
- Biztonsági területek és ágazatok: mérés, kockázat és incidensmenedzsment szabályozása, üzletmenet folytonossága, hálózati biztonsági kérdések, telekommunikáció és egészségügy irányítási rendszerei,
- ágazatonkénti biztonság, mint pl. pénzügy, telekommunikációs cégek, energiaipar, publikus felhőszolgáltatók, IS Governance.

Fontos megemlíteni, hogy az információbiztonsági keretrendszerek kialakítása nem elszigetelten történt, ezek nagy része több ponton, - akár a stratégiai tervezésben, a kockázatkezelésben, a kontrollokon, vagy az ellenintézkedésekben -, szorosan kapcsolódnak egymásba, több helyen átfedésekkel. Egy szervezet információbiztonsági stratégiájának kialakítása során ezekből a szabványokból, keretrendszerekből a számára legoptimálisabb, tevékenységéhez, szervezetéhez vagy a követelményekhez leginkább illeszkedőt érdemes választania. Gondoljuk a közbeszerzésekre, vagy akár az élelmiszerbiztonsági szabványok HACCP és ISO 22000 közötti választáshoz.

Meg kell említeni továbbá, hogy léteznek más, széleskörben, elsősorban az Egyesült Államokban meghonosodott keretrendszerek, csak felsorolásszerűen néhány:

- **COSO ERM 2017 és COSO Integrált Kontroll keretrendszer,** (Committee of Sponsoring Organizations of the Treadway Commission), átfogó, integrált **kockázatkezelési keretrendszer,** a pénzügyi, tőkepiaci területről származó, ma már széleskörűen, a kiberkockázatok kezelésében, felhő alapú számítástechnikában, agilis szervezeteknél is alkalmazott keretrendszerré vált [COSO 2023].
- **CIS Controls** (Center for Internet Security) IT biztonsággal kapcsolatos **legjobb gyakorlatok védelmi készlete**, irányítási keretrendszer is egyben. A CIS-vezérlőket IT-szakértőkből álló közösség fejlesztette ki, akik kibervédőként szerzett tapasztalataikat alkalmazzák ezeknek a globálisan elfogadott biztonsági legjobb gyakorlatoknak a megalkotására. A CIS-vezérlőket fejlesztő szakértők számos szektorból származnak, beleértve a kiskereskedelmet, a gyártást, az egészségügyet, az oktatást, a kormányzatot, a védelmet és más területeket. Basic, Foundational és Organizational csoportokban, 20 kontrollt alkalmaz, erősen technikai jellegű a módszertana. [The Center for Internet Security, Inc. 2023].
- **NIST Cybersecurity keretrendszer**, az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete által létrehozott, széles körben használt **kiberbiztonsági keretrendszer**, mely több szériából áll, a kiadásoknak és a célzott IT területnek megfelelően. [Muha L., Krasznay 2014].

Végezetül dolgozatom *10.3. számú melléklete* néhány vizuális példát tartalmaz a szabványok, keretrendszerek és ajánlások egymásba épülésére a nemzetközi szakirodalom alapján:

2.2.2. Szoftverfejlesztés projektmenedzsmentje és szabványai

Az információbiztonság tárgyalásakor nem kerülhetjük meg a szoftverfejlesztés szabványait és projektmenedzsment eljárásit.

Szerte a világon használják szoftvertervezési és fejlesztési projektekben **a SPICE** (Software Process Improvement and Capability Determination) modellt. Az ISO 15504 szabványként a szervezetek **szoftverfejleszési folyamatainak** méréséhez, fejlesztéséhez, értékeléséhez egy referenciamodellt hozott létre, ami gyakorlati ajánlásokat fogalmaz meg, **érettségi szintek bevezetésével**. A SPICE a CMMI, - képesség-érettségi modell-integráció -, kiterjesztésének tekinthető, és szorosan kapcsolódik más folyamatkeretrendszerekhez, például az ISO 9001-hez.

A **CMMI modell** (Capability Maturity Model Integration) fejlesztésének fő célja az volt, hogy egyetlen modellbe integrálja a korábban a **szoftverfejlesztésben, rendszerfejlesztésben és termékfejlesztésben** legelterjedtebben használt modelleket és megközelítéseket. Ez a modell lehetővé teszi bármely szoftverfejlesztő vagy más szervezet számára, hogy javítsa a teljes szervezet érettségét és/vagy egyes folyamatainak képességét [Visure Solutions 2023].

A szoftver minőségbiztosítás szabványai speciális előírásokat, követelményeket fogalmaznak meg a programkód és funkcionális tervezés, fejlesztés, programtesztelés és a dokumentáltság vonatkozásában, hiszen a szoftver egy speciális terméknek tekinthető. A fejlesztési fázis életciklus modellje alapján ez egyes fejlesztési lépések sorrendjének, a folyamat és projektmenedzsment támogatásának függvényében jöttek létre a:

- **Vízesés modell,**
- V-modell,
- Spirál modell,
- A **SCRUM keretrendszer és az AGILIS módszertan,**
- **DevOps módszertan.** Ez a Development, fejlesztés és az Operations, üzemeltetés csapatok tevékenységének egyesítésével a fejlesztési, üzemeltetési és egyéb fejlesztői szerepköröket kapcsolja össze, szoros együttműködésre kényszerítve őket, a felhasználói igények és azok változásának gyors feldolgozására.

- **PMBOK-**a Project Management Institute által létrehozott, projektmenedzsment technikákat és eszközöket tartalmazó gyakorlati útmutatója, a projektmenedzsment „Bibliája”, ma már a szoftverfejlesztésben is széleskörűen használják.

Napjaink népszerű, lassan a vízcsapból is folyó **SCRUM-AGILIS képzések** hirdetései tulajdonképpen jelzik az Agilis módszertant a szoftverfejlesztésen kívüli egyre szélesebb körű elterjedését a projektmenedzsment világában.

Segítségével könnyebben kezelhetővé válnak a fejlesztés során bekövetkező váratlan események, ügyfélközpontúbb, lényegesen alacsonyabb költségű és kisebb kockázatú fejlesztési módszertan, -persze ha helyesen alkalmazzák-, mint mondjuk a vízesés technika. Ebben a rendszerben különböző területeken jártas csapattagok dolgoznak együtt meghatározott szerepkörökben, vezetőjük a Product Owner és a Scrum Master, tagok az Agile/Lean szakértő, Facilitátor, Coach, Akadálymentesítő, Tanár és a Mentor. Átalában kis létszámú, 3-9 főből álló csapatokban dolgoznak, az egyes munkafázisokat pedig **sprint**-ekre bontják. Az alábbi táblázat a két módszertan közötti különbséget mutatja be:

5. Táblázat Agilis és Vízesés modell összehasonlítása
(Forrrás: Székely 2022)

AGILIS MODELL		**VÍZESÉS MODELL**
Kisebb egységeket, sprinteket használ	Projekt ütemezés	A projektet nagyobb mérföldkövekre bontja
Rugalmasan kezeli a változásokat	Változások kezelése	Rugalmatlan, a scope változásait igyekszik elkerülni
Az ügyfél elégedettség és a megvalósítási folyamat van a középpontban	Fókusz	A sikeres projektre fókuszál
Rendszeres, akár sprintenként is megváltozhat	Követelmények változása	A követelményeket a projekt kezdetekor határozzák meg
Folyamatosan történik a fejlesztés során	Tesztelés	Az egyes mérföldkövek elkészültét követően történik a tesztelés
Az ügyfél igénynek legmegfelelőbb termék készül el		

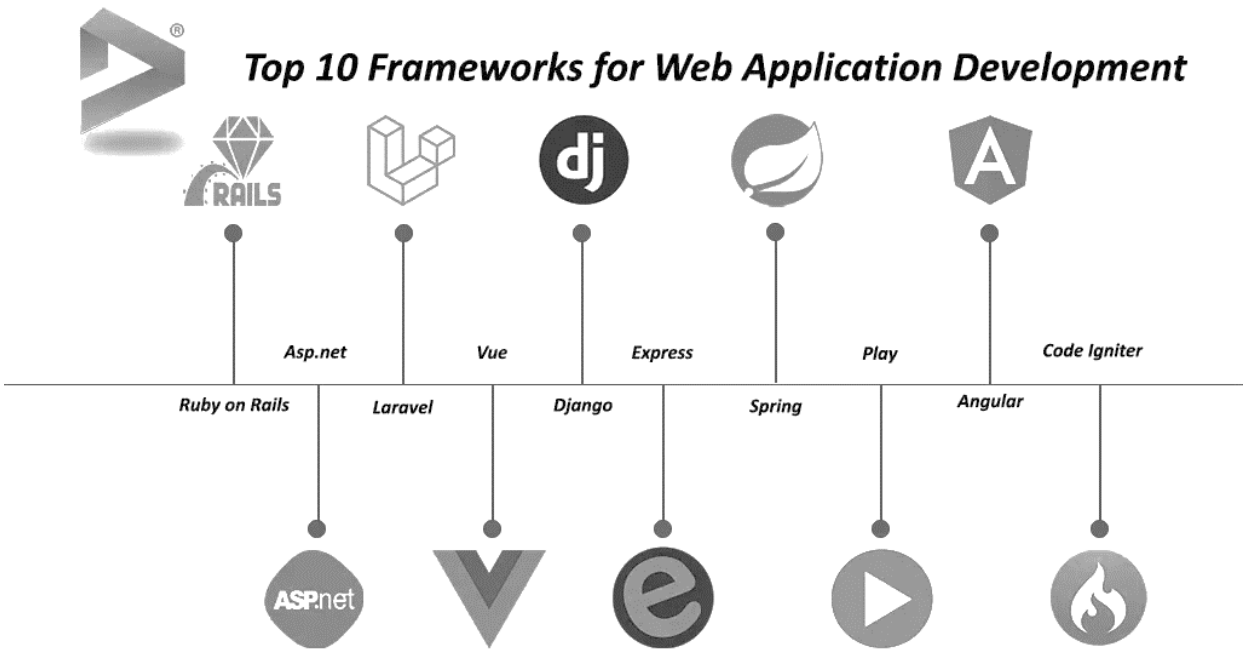
A szoftverek, fejlesztésük és használatuk minden fázisában minőségbiztosítási követelményeknek kell megfelelniük, a legjobb forráskód is az idő előrehaladtával megkopik, ez biztonsági kockázatot hordoz, ezért a teljes életciklusra vonatkozóan szükséges a felügyelet biztosítása, ennek szabványa az **ISO/IEC 25010:2011**, illetve ennek hamarosan helyébe lépő, jelenleg még fejlesztés alatt álló újabb kiadása és az **ISO/IEC DIS 25002**.

A szoftverek fejlesztésére (**SDLC-Software Development Life Cycle**) számos keretrendszer létezik, néhányuk rendelkezik kiterjed **projektmenedzsment** funkciókkal, ezek közül a fontosabbak:

- Jira Software, Agile, Scrum és Kanban táblákkal segíti a projektmunkát,
- Back-End Web keretrendszerek: Django (Python) és Rails,
- Front End Web keretrendszerek: Angular, ReactJS (JavaScript), Bootstrap,
- Mobil fejlesztési keretrendszerek: Flutter, React Native, jQuery Mobile (JavaScript)

A Decipher Zone 2022-es felmérése alapján a következőek voltak a TOP 10 legjobb, legnépszerűbb webfejlesztő keretrendszerei, melyeket a logóikkal az alábbi ábra szemléltet:

11. Ábra Legnépszerűbb webfejlesztő keretrendszerek és logóik 2022-ben
(Forrrás: Decipher Zone Technologies 2023)



3. Anyag és módszer

3.1. A Safety Sector Kft. bemutatása

A Safety Sector Biztonsági Tanácsadó és Szolgáltató Kft. húsz évvel ezelőtti jogelődjének alapítása óta, többszörös átalakulás következményeként ma már igen sokrétű, komplex szolgáltató tevékenységet végez, a hazai piacon 2 Mrd Ft körüli árbevételével és 80 fő saját alkalmazottal, továbbá kb. 300 fő alvállalkozónál bejelentett munkavállalóval közepes méretű hazai vállalkozásnak minősül.

Fő szolgáltatásaink és alaptevékenységeink:

- Vállalkozásbiztonsági tanácsadás, üzleti kockázatkezelés,
- Követeléskezelés és követelés érvényesítés,
- Partnervizsgálat, humán háttérellenőrzés,
- Információvédelem, komplex informatikai auditok elvégzése,
- Élőerős őrzésvédelem, fegyveres és fegyver nélkül, áruházi detektív szolgáltatás,
- Magánnyomozás és vagyonkutatás tevékenység,
- Versenypiaci információszerzés, elemzés és értékelés,
- Biztonságtechnikai szolgáltatások és ingatlan üzemeltetés, valamint biztonsági takarítás,
- Technikai mentesítés, védett tárgyalók kialakítása, lehallgatásmentesítés,
- Üzleti hírszerzés (Business Intelligence).

Cégünk alapvető küldetése, missziója, hogy a magyarországi magán biztonsági igényeket kielégítő, komplex és értékarányos szolgáltatások nyújtásával támogassuk a gazdálkodó szervezetek mindennapi, biztonságos értékteremtő folyamatait, a vállalati vagyon gyarapodását, a stakeholderek érdekeit és céljait, hosszú távon hozzájárulva ezzel a magyar gazdaság fejlődéséhez, munkahelyeket teremtve, nem utolsó sorban védve a természetes személyek biztonságos munkavégzéshez fűződő jogait

A hivatkozott szolgáltatások a vállalkozások szabad alapításának követelményeivel összhangban, azonban egy „átlagos” tevékenységet folytató céggel szemben, **jóval szigorúbb hatósági kontroll alatt állnak.**

Vagyonvédelemhez és magánnyomozáshoz kapcsolódó tevékenységünket külön ágazati jogszabályok, a Személy- és Vagyonvédelemről szóló 2005. évi CXXXIII. törvény, továbbá a 2011. évi CXII. törvény az Információs Önrendelkezési Jogról és az Információszabadságról, illetve kötelező kamarai tagság is szabályozza. 2018. május 1-től pedig az eddiginél is szigorúbb jogszabály válik Magyarországon is kötelezővé, az Európai Parlament új adatvédelmi szabályokat szavazott meg, melyek által 2016/679/EU számon megszületett az EU Általános Adatvédelmi Rendelete.

Követeléskezelés területen MNB kötelező ajánlásai, továbbá a Ptk. és a Btk. megfelelő részei szabályozzák tevékenységünket. (pl. önbíráskodás veszélye.)

Lő (tűz) fegyverekkel, valamint **kábítószer anyagmaradványok** kutatásával kapcsolatosan szintén külön jogszabályok, illetve az engedélyezés és ellenőrzést folyamatosan végző Rendőrhatóság, Kormányhivatalok felügyelete alatt állunk.

Technikai mentesítést pedig **haditechnikai eszközökkel** végzünk, ennek engedélyezését, importját a Magyar Kereskedelmi és Engedélyezési Hivatal végezte, nemzetbiztonsági ellenőrzéssel egybekötve.

A vállalkozásunk által végzett tevékenységi terület hazánkban lényegében a rendszerváltást követően jött létre, az évek során jelentős átalakulásokon ment át, cégek alakultak és szűntek meg. Ma a fő szolgáltatásaink területén cégünk az iparágat meghatározó szervezetek közé tartozik. Meggyőződésünk, hogy ennek oka megrendelőink igényeihez történő rugalmas alkalmazkodás, a jól működő ellenőrzési rendszerünk, kiváló üzleti folyamataink, munkatársaink alapos szakmai felkészültsége, melyet az igényeknek megfelelően folyamatosan fejlesztünk, s utoljára, de nem utolsósorban menedzsmentünk szakértelme és tapasztalata. Tagjai vagyunk a Magyar Biztonsági Fórumnak.

A hazai jogszabályi környezet az érintett területeket pontatlanul, sokszor ellentmondásosan szabályozza, ezért működésünkkel kapcsolatos **jogi és adatvédelmi kockázatok** kezelésére kiemelt figyelmet vagyunk kénytelenek fordítani, tekintve a sokszor ellentmondó bírói és ügyészi gyakorlatot. Nem könnyíti meg ez a közállapot az integrált minőségirányítási rendszerünk hatékony működtetését sem, mivel a személyes adatok és dokumentumok kezelése, az egyes eljárások kompatibilissé tétele a hatósági előírásoknak sok esetben ellentmondásos helyzetet idéznek elő, még akkor is, ha a 9001-es irányítási rendszer 2015. évi módosítása könnyít és egyszerűsít bizonyos adminisztrációs feltételeken, követelményeken.

Olyan szolgáltatások nyújtására törekszünk, amely teljesen kielégíti megrendelőink elvárásait, s minden minőségi, környezetvédelmi és információ biztonsági követelménynek megfelel. E célkitűzések érdekében hoztuk létre már 2004-ben minőségirányítási rendszerünket, melyet 2010-ben a környezetvédelmi irányítási rendszerrel, majd 2014-ben a munkahelyi egészségvédelem, 2022-ben pedig **Információbiztonsági Irányítási rendszerrel bővítettü**k, továbbá egyes technikai eszközeink és néhány állami megrendelésünk, közbeszerzéses követelményrendszer előírása, továbbá a **NATO Beszállítói** státuszunk is indokolttá tették **Katonai Minőségirányitási Rendszer** bevezetését is. Egységes irányítási rendszerünket eddig sikeresen működtettük, melyet a külső auditok is igazolnak és tanúsítottak. Ennek biztosítása céljából felső vezetésünk belső és harmadik fél általi aduitok, vezetőségi átvizsgálások, és egyéb eljárások mentén folyamatosan ellenőrzi irányítási rendszerünk alkalmasságát, megfelelőségét a követelményeknek, és annak hatékonyságát.

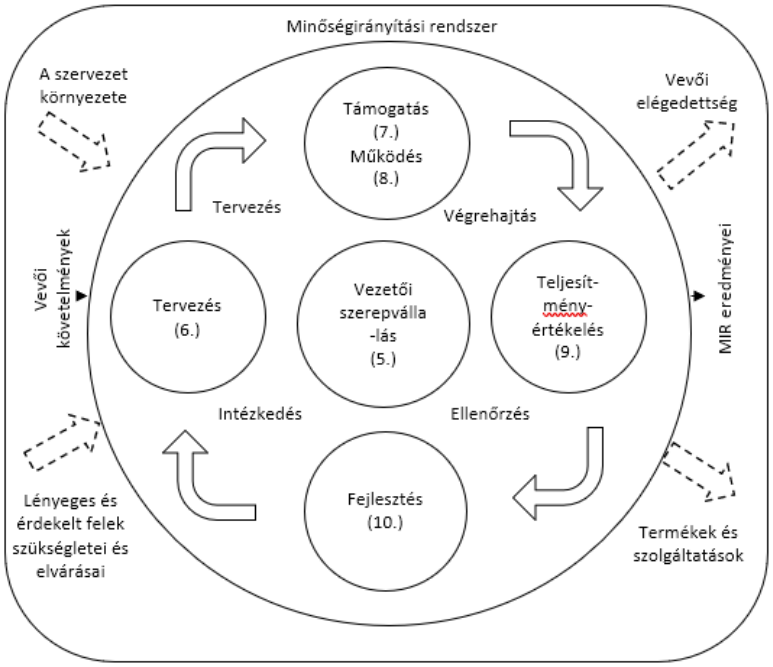
Integrált irányítási rendszerünkben megfogalmazott előírásokat az MSZ EN ISO 9001:2015., az MSZ EN ISO 14001:2015., az MSZ ISO/IEC 27001:2014., és az MSZ 45001:2018. nemzetközi szabványok követelményeinek megfelelően dolgoztuk ki, melybe beépítettük az AQAP-2120 (Edition 3) normatív dokumentum követelményeit is.

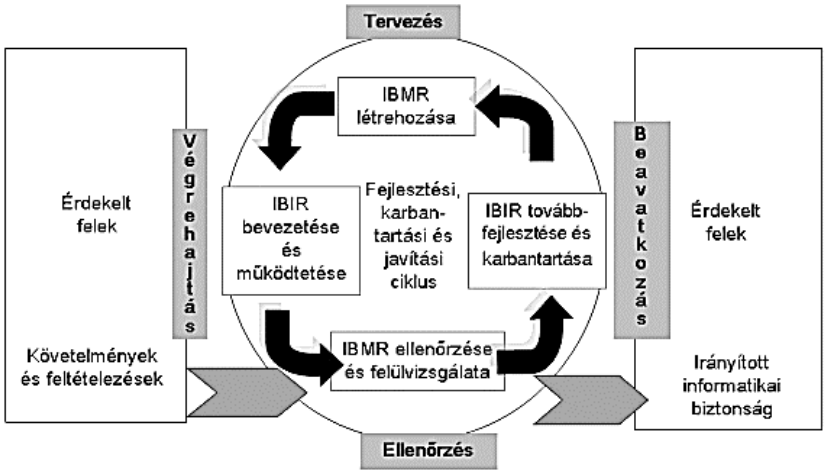
Cégünk legnagyobb vagyoneleme az immateriális és dematerializálódott formában megtestesülő **vállalati adatvagyon**, ennek védelme pedig mind technikai, mind folyamatszervezési, továbbá szervezeti oldalról indokolt és szükségszerű. Mivel az IBIR-nek, mint egy erősen technikai jellegű szabványnak a bevezetése az integrált irányítási rendszerünk már működő három szabványa mellett történt, ezért bevezetési folyamatát, az auditokat, a külső felkészítő tanácsadó cég tevékenységét teljesen elkülönítetten kezeltük. Későbbi terveink szerint sem szándékozom ezen változtatni, csupán arra törekszem, hogy mind az ISO szabványok, mind az **AQAP és a NATO beszállítói** követelményeknek való megfelelés egységes felépítésű, **HLS dokumentációs rendszerben** valósuljon meg, meghivatkozva a dokumentumok között azokat a fejezeteket, amelyek olyan előírásokat szabályoznak, melyeket máshol már részletesen szabályoztunk.

3.2. Az alkalmazott módszerek

Az IBIR bevezetése során, már a tervezései és bevezetési szakaszt is a PDCA folyamatmodell mentén valósítottam meg, ebben az ISO 9001-es szabvány minőségcéljai, továbbá a PDCA logika információbiztonsági rendszerrel kapcsolatos folyamatszemlélete is segítségemre volt. A 9001-es szabvány minőségcéljai (a szabvány fejezetszámaival összerendelve) és a 27001-es IBIR megvalósulása közötti összhangot az alábbi ábrákkal szemléltetem:

12. Ábra ISO 9001 és IBIR szabályozott területek és fejezetszámok
(Forrás:: ISO 9001:2015 és Muha, Krasznay 2014)





A bevezetési folyamatot az ISO 27001-es szabvány megfelelő fejezeteivel összerendelve mutatom be, egyfajta struktúrát adva a tevékenységeknek és bemutatva azt a módszertant, amivel egy ilyen rendszer bevezetési folyamata tervezhető.

A TERVEZÉS - Érintett szabvány fejezetek: 4.-5-6.

A szervezet környezete, Vezetői szerepvállalás, Kockázatkezelés, IBIR célok

A tervezés első lépéseként meghatároztam a szervezeti működés tágabb környezetét, szerződéses és hivatalos kapcsolatainkat az érintett felekkel, felmértem továbbá az információbiztonság jelenlegi helyzetét, majd kijelöltem az IBIR alkalmazási területét. A helyzetelemzés során **adatgyűjtő lapokat** alkalmaztam, melyeken különböző csoportosítás mentén gyűjtöttem össze azokat az eseményeket, melyeknek az IBIR bármely részére hatásuk lehet. Ehhez korábbi jegyzőkönyvek, email-ek, eseményjelentők, kivizsgálási jelentések szolgáltattak adatot, továbbá megkérdezéses kérdőívek is kiküldésre kerültek a munkatársaknak., Felhasználtam továbbá a már működő integrált irányítási rendszerünkben fellelhető dokumentált információkat, audit bizonyítékokat.

Technikai oldalról az információbiztonsági események számítógépes LOG fájljai kerültek elemzésre. A továbbiakban létrehoztam a vállalkozás Információbiztonsági Stratégiáját és Politikáját, valamint kidolgoztam a kockázatkezelési modellt. Ebben a fázisban történt a vagyonleltár feltérképezése is.

Az IBIR bevezetését magában foglaló erőforrás és időtervezéshez a **projektmenedzsment Gantt diagramját**, valamint a kritikus tevékenységek, út és átfutási idő meghatározásához a **CPM (Critical Path Method** - kritikus út módszere) módszertant alkalmaztam, ami a határozott időtartamú, determinisztikus projektek projektmenedzsment módszere. Szoftveres segítségként a nyílt forráskódú GanttProject 2.8.5 Pilsen (build 2179) program 3 változatát használtam.

A kockázatkezelési modell kialakítása során kerültem a túlbonyolított értékelési és számolási módszereket, **Kockázat (R) = Hatás (I) × Bekövetkezési valószínűség (P)** alapján, valamint 5-5 minősítési kategória mentén alakítottam ki az elfogadás, beavatkozás vagy áthárítás intézkedéseket. A 6. táblázat szerinti modellt hoztam létre szakirodalmi források alapján, jelentősen átalakítva azt a saját szervezetünkre igazítva:

6. Táblázat Kockázatkezelési folyamat lépései
(Forrás: Saját szerkesztés)

A kockázatértékelés lépései és modellje			
Lépés	**Leírás**	**Oszlop**	**Érték**
1.	Információs vagyon elemek azonosítása	D	szöveges
2.	Az azonosított vagyontárgy csoportokra vonatkozó fenyegetések megállapítása	B	szöveges
3.	A vagyontárgy csoportra jellemző a fenyegetés szempontjából releváns sérülékenység megállapítása	C	szöveges
4.	A fenyegetés megvalósulásának a hatása kerül megállapításra.	E	szöveges
5.	Az érvényben lévő kockázat csökkentő intézkedés Iso 27001 kontrollok szerinti számbavétele	F	szöveges
6.	A hatás nagyságának az értékelése (meglévő kontrollokkal csökkentve)	J	1-5 -ig értékelve
7.	A bekövetkezés valószínűségének az értékelése (meglévő kontrollokkal csökkentve)	K	1-5 -ig értékelve
8.	A kockázat kiszámítása Risk=ImpactxProbability	L	1-25 -ig kiszámítva
9.	A kockázat elfogadása/kezelése döntés indoklás	M	határérték 6
10.	A kockázat elfogadási határt meghaladó esetben a kockázat kezelésre javasolt intézkedés meghatározása	N	szöveges
11.	A javasolt kockázatkezelési intézkedés megvalósulása után a fenyegetés bekövetkeztének a hatása	O	1-5 -ig értékelve
12.	A javasolt kockázatkezelési intézkedés megvalósulása után a bekövetkezés valószínűségének értékelése	P	1-5 -ig értékelve
13.	A javasolt kockázatkezelési intézkedés megvalósulása után megmaradó kockázat kiszámítása	Q	1-25 -ig kiszámítva
14.	A javasolt intézkedések és a maradék kockázat elfogadtatása a vezetőséggel	R	igen/nem
15.	A javasolt kockázatkezelési intézkedés megvalósításának javasolt határideje	T	dátum
16.	A javasolt kockázatkezelési intézkedés megvalósításáért felelős megnevezése, feladatok kiadása	U	név
17.	A megvalósítás nyomonkövetése, eszkaláció, vezetőség tájékoztatása	V	szöveges

Az egyes események bekövetkezési valószínűségét és hatását az alábbi táblázat alapján soroltam kategóriákba:

7. Táblázat: Események bekövetkezési valószínűsége és hatása
(Forrás: Saját szerkesztés)

Értékelési kategória meghatározások			
Bekövetkezési valószínűségek			
kategória	**érték (pont)**	**P**	**leírás**
kritikus	5	>95%	A bekövetkezés minden percben várható
magas	4	50>95%	A bekövetkezés valószínűbb, mint a nem bekövetkezés
közepes	3	25>50%	A kockázat már konkrét, a bekövetkezésre számítani lehet
alacsony	2	5>25%	A meglévő állapotok, körülmények alapján a bekövetkezés elképzelhető
nagyon alacsony	1	>5%	A lehetőséget azonosították, de a bekövetkezése valószínűtlen
Hatások			
kategória	**érték (pont)**	**érték ezer Ft I**	**leírás**
kritikus	5	>=100M	nagy számosságú különleges személyes adat sérülhet, a hatás a vállalaton túlterjed, további magas besorolású hatásokat indukál, súlyos jogi következményekkel jár, a vállalat reputációját nagyban rontja, az üzletmenet folytonossága sérül
magas	4	>=50M	a hatás az egész vállalatra kiterjed, a folyamatokban tartós fennakadások, helyreállítás több mint 1 napos, jogi következmények, jelentős pénzügyi veszteségek lehetnek
közepes	3	>=5M	különleges személyes adatok, vagy nagy mennyiségű személyes adatok sérülhetnek a hatás több egységre kiterjed, a károk elhárítása 1 napot igényelhet, a folyamatokban jelentős fennakadásokat okoz, esetleg jogkövetkezmények
alacsony	2	>=1M	személyes adat sérülhet, a hatás egy egységen belül érzékelhető, egyes folyamatok végrehajtásában múló fennakadások, a kárelhárítás 4 órán belül lehetséges, nincsenek jogkövetkezmények.
nagyon alacsony	1	<50	A személyes adatok nincsenek veszélyeztetve. A problémák kezelése a szervezet határain belül oldhatóak meg. A közvetlen és közvetett anyagi kár minimális a szervezet költségvetéséhez és erőforrásaihoz képest.

Az alábbi kockázatkezelési táblázat szerint úgy döntöttem, hogy a kockázat elfogadható szintje a 6 alatti értékek, míg a 7 felett beavatkozásra, 20 felett pedig azonnali beavatkozásra van szükség.

A VÉGREHAJTÁS, BEVEZETÉS - Érintett szabvány fejezetek: 7.-8

Támogatás, Működés

Elkészítettem a vonatkozó biztonsági szabályzatokat, a dokumentált információkezelés követelményeit, valamint az intézkedéseket (szabályozó környezet), az IBIR felügyeletének és mérésének módszereit, meghatároztam a kritériumokat, a mutatószámokon nyugvó objektív értékelési elveket. A menedzsment támogatásával átalakítottam a vállalkozás szervezeti struktúráját. A felelős személyek körének kijelölése, megfelelő hatásköri jogosultságok kiosztásával valósítottam meg. Az intézkedések érintették továbbá a teljes IBIR alkalmazási területet, beleértve a fizikai környezet biztonságát is.

AZ ELLENŐRZÉS - Érintett szabvány fejezet: 9.

Teljesítményértékelés

A teljesítményértékelés kialakításához meghatároztam a belső ellenőrzés és a vezetőségi átvizsgálások, auditok rendjét, a folyamatos felügyelethez szükséges szervezeti és folyamatkontrollokat.

A BEAVATKOZÁSI FÁZIS - Érintett szabvány fejezet 10.

fejlesztés

Bevezettem a folyamatkontrollokból, auditokból és felülvizsgálatokból származó adatok alapján történő megelőző és korrigáló és fejlesztő intézkedéseket, valamint a továbbfejlesztéshez szükséges erőforrások allokálásának, a technikai eszközbeszerzések és folyamatos oktatásoknak és a képzéseknek a rendjét.

A szabvány „A” mellékletében, a kontrollok 7.7 pontjának Tiszta asztal és tiszta képernyő követelményének alkalmazásához a minőségmenedzsment módszertanok közül az **5S modellt** alkalmaztam.

A folyamatok mérésének és felügyelet alatt tartásának objektív értékeléséhez, valamint a fejlesztéshez a szervezetünkhöz igazodó egyszerűsített **mutatószámok** rendszerét dolgoztam ki.

Az ISO/IEC 27004:2016 szabványa azzal foglalkozik, hogy hogyan mérjük az Információbiztonsági Menedzsment Rendszer hatékonyságát és teljesítményét. Ebben a szabványban a mérések bevezetéséhez, a mutatószámok rendszeréhez és az ezekre alkalmazott értékelési kritériumokhoz adnak iránymutatást. A szabvány kiemelten foglalkozik a mérési módszer kialakításával, az alap- és származtatott adatok létrehozásának módjaival, az adatok gyűjtésének és elemzésének módszereivel, valamint az eredmények prezentálásával a döntéshozatalhoz szükséges információk biztosításával.

Az összetettebb és bonyolultabb információbiztonsági rendszerek, nagyobb szervezetek esetében a **KPI** (key performance indicator) rendszerét tovább bontja, e megközelítés szerin kockázati mutatókat (Key Risk Indicator - **KRI**), kulcsfontosságú területi mutatókat (Key Result Areas - **KRA**), teljesítményterületi mutatókat (Key Performance Area - **KPA**), valamint a környezeti kockázatok mérési szintjét jelző kulcs ellenőrző indikátort (Key Control Indicator - **KCI**) hoznak létre az adatokból. Ezekből pedig indexálással készítenek teljesítménymutató indexet (**KPX** - Key Performance Index). Ilyen bonyolultságú mutatószám rendszerre a mi szervezetünknél nem volt szükség, mindazonáltal egy olyan jelzőrendszer létrehozására igen, ami igazolja, vagy cáfolja a következő felvetéseket:

- a rendszer képes észlelni a biztonsági eseményeket az üzleti folyamataink működése során,
- a védelmi intézkedések elég hatékonyak a fenyegetések kezeléséhez,
- a dolgozók a napi rutintevékenységük során megvalósítják az IBIR követelményrendszerében foglaltakat,
- üzemszünet, katasztrófa esetén a meghatározott szintidőn belül képes-e az irodai működés helyreállni,
- új és azonosítatlan fenyegetések megjelenése esetén a rendszer képes azt jelezni a folyamat vagy adatgazdának.

A **belső auditok rendszere** szintén támogatást nyújt a folyamatok szabályozottságának igazolására, azonban az kizárólag utólag képes igazolni, vagy cáfolni a rendszer működésének szabványkövetelményeknek és IBIR céloknak való megfelelését, operatív, azonnali jelzések adására a megfelelően kialakított mutatószámok rendszere képes. Ezeknek a mutatószámoknak a képzési ideje a céltól függ, vannak olyan technológiai jellegű mutatók, amit a rendszerből a rendszergazda akár percenként is lekérdez, monitoroz, - megfelelő szoftverrel természetesen -, és vannak olyan mutatószámok, melyeket elegendő évente egyszer kiszámolni, mert abból is lehet a rendszer egészére vonatkozóan teljesítményszintet meghatározni.

Más szakirodalmi források (Védelem és Tudomány 2019.) **megelőző és követő típusú indikátorokra** csoportosítják a mutatószámokat, azokon belül például:

- a műszaki állapot nyomonkövetésére alkalmas indikátorokat – például karbantartás,
- személyi erőforráshoz kapcsolódó mutatókat – például sikertelen oktatási vizsgák aránya,
- technológiai leírások, utasítások indikátorai – például folyamatleírással nem rendelkező technológiai vagy egyéb biztonság szempontjából kritikus folyamatok száma,
- bekövetkezett események kivizsgálásával kapcsolatos mutatók, - például a javító intézkedések átlagos késési ideje,
- Az olyan események számossága, amelyek bekövetkezése nem került előzetes elemzésre a veszély-kockázatelemzések során,

Ezekből a mutatószám csoportokból és típusokból néhányat használunk, ezeket a dolgozatom 10.4 számú mellékletében tüntettem fel.

4. Saját feldolgozás

A továbbiakban bemutatom az irányítási rendszer létrehozási folyamatának egyes lépéseit, a bevezetéshez szükséges tervezési elemeket, a szükséges idő és erőforrástervezési lépéseket, továbbá a folyamatos működésfelügyeleti eljárásokat és a fejlesztési lehetőségeket.

4.1. Az IBIR létrehozása és a fejlesztések bevezetése

4.1.1. Helyzetfelmérés

A bevezetés előtti információbiztonsági kultúra, az akkori rendszer gyenge és szabályozatlan pontjainak meghatározásához a szervezet átvilágítása során a következő területeket tekintettem át, és azok az alábbi eredményekre jutottam:

8. Táblázat: Helyzetfelmérés területei és eredményei
(Forrás: Saját szerkesztés)

Átvizsgált terület	Eredmény
Szabályozási környezet	Sem információbiztonsági politika, sem stratégia nem található a szervezetnél. Egy egyszerű informatikai szabályzaton kívül semmiféle magasabb vagy alacsonyabb szintű előírás nem foglalkozik az információbiztonság kérdésével. A munkavállalók napi munkavégzése során követelményekkel és IT vonatkozású munkavégzési előírásokkal nem találkoznak.
Szervezeti biztonság	A vezetőség információbiztonsági elkötelezettsége kinyilvánítva nem jelenik meg. A szervezeti struktúrában az IT rendszergazda hatásköre alacsony, az információbiztonságot senki nem képviseli a súlyának megfelelően a szervezetben.
Vagyontárgyak biztonsága	Vagyonleltár nincs, kockázatkezelési rendszer nem létezik. A vagyontárgyak használata szigetszerűen történik, közöttük a védelmi szintre vonatkozóan sem besorolás, sem osztályozás nincsen. A kiadott eszközök leltározási követelményeit sem teljesítik az akkori folyamatok, ami számviteli problémákat is felvetett.

Fizikai környezet biztonsága	A dolgozók irodai munkavégzésének rendje nem szabályozott és nem felügyelt. A számítógépes erőforrásokhoz és az ügyviteli nyilvántartásokhoz való hozzáférés szintén hiányos.
Emberi erőforrásokhoz kapcsolódó kockázati elemek	Sem a felvételi eljárás, sem a munkaviszony megszüntetésekor nincs szabályozva a kiadott IT eszközök, létrehozott jelszakvak, jogosultságok kezelésének folyamata, a jogosultságok visszavonása, valamint a megfelelő titoktartási megállapodások munkajogi iratokban való megjelenítése nem történt meg. Biztonságtudatossági képzés és egyéb technikai jellegű oktatások nem voltak.
A kommunikáció és az üzemeltetés biztonsága	Az alkalmazott információtechnológia szoftveres és hardveres megvalósítása elavult, a szenzitív adatok védelmének titkosítási követelményrendszere pedig nem létezett. Az elektronikus levelezés és a webhelyek, webszolgáltatások használata során a szervezet adatai nem voltak védve semmilyen alkalmazási és technikai protokollal.
Incidenskezelés	A szervezet nem határozta meg az információbiztonsági és adatvédelmi incidens körébe eső eseményeket, azokra semmiféle intézkedési terv nem létezett.
Üzletmenet folytonosságának biztosítása	Sem katasztrófavédelmi és helyreállítási tervvel, sem annak begyakorolt folyamatával nem rendelkezett a szervezet, biztonsági mentések pedig csak esetszerűen, nem pedig mentési stratégia mentén valósultak meg.
Jogszabályi, törvényi és egyéb szervezetek által megkövetelt kritériumrendszernek történő megfelelés	A személyes és különleges személyes adatok, valamint az üzleti titkok védelme nem történt meg teljesen jogszabály konform módon, különösen igaz volt ez a kép és hangfelvételek esetében.
Fejlesztés, karbantartás	Az információtechnikai eszközök beszerzése és karbantartása ad hoc jellegű és stratégia nélküli volt. A karbantartás az első meghibásodási eseményhez kapcsolódott, tartalék eszközök és rendszerek nélkül.

Amint az eredmények mutatják, a szervezet nemhogy a szabványkövetelményeknek nem felet meg, de még jogszabályi hiányosságok is voltak a működésben. A COBIT érettségi modellje alapján, - ami hat fokozatra osztja a szervezet információbiztonsági szintjét, -, **az 1-es, kezdeti, ad hoc jellegű érettségi szintnek feleltünk** meg, az alábbi jellemzőkkel:

- a menedzsment hozzáállása az információbiztonság kérdéséhez ellentmondásos, kaotikus,
- nincsenek szabályozott biztonsági folyamatok, kialakult módszerek,

- hiányzik a szervezeti struktúrában az információbiztonság hangsúlyos megjelenítése,
- feladat, felelősség és hatásköri hiányosságok mutatkoznak a szervezetnél,
- a vállalati teljesítmény és információbiztonság kapcsolatát a menedzsment nem ismerte fel, az egész szervezet működésében folyamatosan zavarok keletkeznek szabályozatlanság és az információbiztonsági tudatosság teljes hiánya miatt,
- informatikai, technikai jellegű lemaradás figyelhető meg a hálózati infrastruktúrában, a korábbi fejlesztések elmaradása miatt.

Célul tűztem ki, hogy a szervezetet a tanúsító audit időpontjára legalább a **4-es COBIT szinte, az irányított és mérhető IBIR rendszert** alkalmazók szintjére hozzuk. Itt már a kialakult gyakorlat után az egész szervezet irányítási rendszerébe integrálódott az IBIR, az informatikai eljárások tisztázottak, a felelősségi körök kialakultak, az IT tevékenység teljes vertikuma folyamatos felügyelet alatt ál, a kockázatokat folyamatosan mérik és kezelik, a biztonságtudatosságot pedig állandó képzésekkel segítik.

A pillanatnyi helyzet felmérése után az Információbiztonsági Stratégia részeként döntés született egy célállapot megfogalmazására, ami magában foglalta a szervezeti kultúra megváltoztatását, szabályozási környezet kialakítását, védelmi és kontroll intézkedések bevezetését, oktatást és képzést, valamint az ehhez szükséges erőforrások biztosítását.

A kiindulási állapotot **felülvizsgálati jelentésbe** foglaltam, mely tartalmazta mindazon hiányosságokat, melyek az IBIR kialakításához szükségesek voltak.

4.1.2. Vagyonleltár elkészítése

A vagyonelemek **bizalmasságának, sértetlenségének és rendelkezésre állásának** kritériumai alapján minden szervezetnek vagyonleltár kell készítenie, a védendő fizikai, szoftver és információs vagyonelemek védelme érdekében. Ehhez a könyvelésből és a fizikai leltározásból átemelt adatokkal, valamint az egy számítógépekre telepített, szoftver és hardverkörnyezetet pontosan meghatározó felügyeleti programokból vettem az adatokat.

A vagyonleltár felvételével egyidejűleg az egyes vagyonelemeket **biztonsági osztályokba** soroltam, ezzel a védendő elemmel kapcsolatos fenyegetések eredetét, a védendő információkkal kapcsolatos sérülés esetén a bekövetkező kár valószínűsíthető nagyságát és az esetleges kiesési időt tudtam meghatározni.

Az adatvagyonleltár elkészítéséhez bevontam a folyamat és adatgazdákat, mivel a folyamatok által használt adatok és információk megjelenési formájáról, fellelhetőségéről, az adathordozó típusáról, továbbá a jelenleg beállított hozzáférési jogosultságokról ők rendelkeztek a legtöbb információval. Az adott vagyonelem minden esetben kapcsolatban állt egy létrehozó, vagy működtető, felügyelő tulajdonossal, a szabályozott folyamatok kialakításához elengedhetetlenül szükséges volt az adatgazdák, tulajdonosok és felelősök kijelölése.

A vagyonleltárt az informatikai irányítás, de facto sztenderdje, a COBIT alapján az alábbi csoportosítások mentén végeztem el:

9. Táblázat COBIT szerinti vagyonelem fő csoportok
(Forrás: Saját szerkesztés)

Fő csoportok	Vagyonelem
infrastruktúra	hardver eszközök: szerver, munkaállomás, laptop, mobiltelefon, tablet, adathordozó eszközök, adatbeviteli és megjelenítő eszközök, videokamerás megfigyelő rendszerek elemei szoftverek: operációs rendszerek, virtuális számítógépek, adatbáziskezelők, video szerkesztő programok, felhasználói kommunikációt megvalósító programok (Outlook, Teams, Skype) hálózati eszközök: NAS, router, switch, tűzfal, UPS szünetmentes tápegység
információ hordozó	dokumentációs rendszer, IT rendszerre vonatkozó kézikönyvek, utasítások, leírások
alkalmazói rendszerek	komplex ügyviteli, pénzügyi rendszer
emberi erőforrások	folyamatgazdák, projektmenedzserek, ügyviteli alkalmazottak, pénzügyi munkatársak, menedzsment, külső érintettek, partnerek, beszállítók munkatársai

A vagyonleltár kivonatát, terjedelmi okok miatt a dolgozatom 10.5 *számú melléklete* tartalmazza.

4.1.3. Kockázatfelmérés, kockázatelemzés és kockázatkezelés

Az adatvagyonleltár elkészítését követően a lehetséges **fenyegetések és sérülékenységek, sebezhetőségek** azonosítása következett. A fenyegetéseket csoportosítottam az eredetük jellege szerint, például humán veszélyforrás, természeti veszélyforrás, fizikai veszélyforrás stb. Olyan kérdésekre kerestem a válaszokat a kockázatkezelési folyamat során, hogy az adott vagyonelemet:

- Mitől kell védeni? Hol keletkezhet a kár?
- Mi teszi lehetővé a kár bekövetkezését?
- Mi a kár bekövetkezésének valószínűsége?
- Tudom-e ezek alapján kvantitatív módszerrel meghatározni a kockázat számszerű értékét?
- Mekkora a kárbekövetkezés hatása a szervezetre vonatkozóan?
- Milyen típusú a bekövetkezett kár?
- Milyen lépéseket tegyek ennek elkerülésére?
- Kockázatkezelés után mekkora a maradványkockázat elfogadhatósági szintje?

Mindezek, valamint felhasználva az Információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt, a biztonsági osztályokba sorolást az alábbi táblázat szerint végeztem el:

10. Táblázat Bizalmassági osztályok kialakítása
(Forrás: Saját szerkesztés)

BIZALMASSÁGI **Biztonsági osztályok**	**Jogszabállyal, belső szabályozóval szabályozott,** **vagy védett adat**
1. **Nyilvános**	Az az információ, vagy az információt tartalmazó papír vagy elektronikus dokumentum, amit mindenki számára elérhetővé kívánnak tenni, és amit egy erre feljogosított szervezeti egység vezetője nyilvánosnak minősített, az információ megjelenéséhez hozzájárult. Ilyenek például a nyilvános weblapok tartalma, a hirdetések, a médiának tett nyilatkozatok.

2. **Belső használatra**	Gyakorlatilag minden, ami nem esik a többi kategóriába. Alaphelyzetben egy dokumentum „belső használatra” állapotú, amíg nincs osztályozva. Jellemzően olyan anyagok, ahol nem lehet, vagy nem kell pontosan előre meghatározni a „címzettek” teljes körét. Az információk nyilvánosságra kerülése csak elhanyagolható kárt vagy biztonsági sérülékenységet fog okozni.
3. **Minősített adat**	Az olyan információk vagy azokat tartalmazó dokumentumok, amiket egy jól behatárolható, de sok személyből álló csoportnak, (jellemzően közép és felsővezetőkből), valamint az általuk személy szerint meghatározottan bevonandó alkalmazottak körének szólnak. (például minden projektvezető és helyetteseik). Amennyiben külső felek kezébe kerülne, akkor az érezhető versenyhátrányt, kimutatható pénzügyi veszteséget, elmaraszталó jogi következményeket okozhat, vagy rosszindulatú cselekmények (támadások) megvalósítását elősegítheti. Ilyenek lehetnek például szerződések, műszaki tervek, programok forráskódjai, az IT rendszer dokumentációja, auditjelentések, üzletmenet folytonossági tervek, katasztrófahelyzeti tervek, árkalkulációk, a vezetőség számára készült jelentések, fizetési listák, valamint az adatvédelmi törvényben meghatározott védendő személyes adatokat tartalmaznak.

A változtatásokat, a hivatkozott szabályozó dokumentumok létrehozása utána átvezettem az **Adatvédelmi Szabályzatunkba** és az **Ügyviteli és Iratkezelési Szabályzatunkba** is. Az Ügyviteli és Iratkezelési Szabályzatban részletesen meghatároztam az információvédelemmel és osztályozással kapcsolatos szabályokat, a következők szerint:

- az információk besorolási irányelvei között a **bizalmassági szint** szerinti osztályozás szabályai kerültek kifejtésre, a fenti táblázatnak megfelelően,
- a **rendelkezésre állás** szerinti besorolásban az alábbi kategóriákat határoztam meg: alacsony rendelkezésre állás, rövid időn belüli rendelkezésre állás, azonnali és folyamatos rendelkezésre állás,
- **információk osztályba sorolásának irányelveit** külön pontokba szedve, taxatíve határoztam meg, ebbe a védelmi osztályba sorolás felelőse, az adat gazdájának szerepe, valamint az adatokkal történő műveletek szabályai kerültek részletesen kifejtésre. (felhasználás, tárolás, továbbítás, kivonat készítés, megsemmisítés stb).

Az információk és az információkezelő rendszerek besorolását az üzleti hatáselemzés eredményeivel és az üzletmenet folytonossági, valamint a helyreállítási tervekkel is egyeztettem. Külön szabályoztam a papír alapon és az elektronikus formában megjelenő tárolt adatokat, azok eltérő technikai kezelési módja miatt.

A kockázatfelmérés során részletesen feltártam az alábbi területek sérülékenységeit és fenyegetettségi állapotát:

- Az informatikai infrastruktúra fizikai biztonságával kapcsolatos, továbbá az IT rendszer technológiai hiányosságait,
- A fizikai környezet, beleértve a szerverszoba, irodahelyiségek biztonságtechnikai vonatkozású hiányosságait,
- Az erőforrásokhoz való hozzáférés logikai biztonsággal kapcsolatos hiányosságait,
- A szabályozatlan folyamatok, hiányzó szabályozó környezet hiányosságait,
- Az elégtelen személyi és tárgyi feltételek, az oktatások és képzések hiányosságait, valamint a vezetőknek a biztonságtudatosságra történő elkötelezettségének a teljes hiányát.

A **kockázatelemzés** során meghatároztam a kapcsolatokat a feltárt sérülékenységek és a lehetséges fenyegető tényezők között, a sebezhetőségek pedig ezek alapján megmutatták, hogy egy esetlegesen szándékos rosszindulatú, vagy véletlen tevékenység során az hogyan képes kifejteni hatását. A korábban már bemutatott kockázatelemzései módszertan alapján elkészítettem a **kockázatkezelési tervet**, melyben az elfogadhatatlan méretű kockázatokat, kockázatkezelési döntés alapján, megfelelő ellenintézkedésekkel, felelős, és határidő kijelölésével a vállalt kockázati szintre redukáltam. Az **azonnali biztonsági intézkedések mellett**, tudatos döntés alapján a következő alternatívák között választhattam:

- egyes folyamatok, eszközök, eljárások kiiktatásával **a kockázatot elkerülöm,**
- a kockázatot valamilyen módszerrel (biztosítás, szerzősé) **áthárítom** valamelyik szerződéses partnerre,
- a kockázatot, beavatkozás nélkül, az eredeti szinten **elfogadom.**

A kialakított kontrollok esetében megvizsgáltam azok jellegét (hibamegelőző kontroll, hibaérzékelő kontroll, hibajavító kontroll), a bevezetéséhez szükséges idő és pénzbeli ráfordításokat, a kockázatok mérséklésének **költséghatékonyságát**, a maradványkockázatok további kezelésének esetleges szükségszerűségét, valamint a védelmi intézkedések közötti fontossági rangsort állítottam fel.

Terjedelmi okokból az IBIR bevezetési folyamat, vezetőségi átvizsgálás időpontjáig előírt kockázatkezelési tervnek és a kockázati elemzésnek csak néhány sorát tudom bemutatni. A kockázatelemzési táblázatban (11. táblázat) eltérő színnel azonnal megjelennek az intézkedés alá vont vagyonelemek. A **kockázatkezelési terv** (12.táblázat) pedig **feladat, felelős és határidő** kijelölésével mutatja meg a sérülékeny vagyonelemekkel kapcsolatos intézkedéseket.

11. Táblázat Kockázati elemzés és kezelési táblázat
(Forrás: Saját szerkesztés)

Sorszám	Vagyonelem	Fenyegetések	Sérülékenységek	Hatások	Meglévő ellenintézkedések (ISO27001 szerint)	Hatás	Valószínűség	Kockázat	Kockázat elfogadása/kezelése döntés és indoklás	Kockázatkezelés	Hatás	Valószínűség	Maradék Kockázat	Intézkedés szükséges?	Határidő	Felelős	Monitoring
1	Bizalmas információk	Bizalmas információk kiadása	titoktartási megállapodás hiánya, nem megfelelő felek/szintek között megállapodás, hiányos megállapodás	adatok kiszivárgása, károkozás ügyfélnek	Titoktartási megállapodások	3	1	3	Kockázatcsökkentő intézkedés szükséges	Aktualizálás, éves felülvizsgálat, ellenőrzés	3	1	3	nem			Végrehajtva
4	Elektronikus dokumentumok, adatok	Bizalmas információk nem	a dokumentumok, dokumentum tárak bizalmasságának hiányos vagy téves megjelölése	adatok kiszivárgása, károkozás ügyfélnek, hátrányos jogi	Az Információk jelölése és kezelése	2	2	4	Kockázatcsökkentő intézkedés nem szükséges	további intézkedés nem szükséges	2	2	4	nem			elvégezve
5	Elektronikus dokumentumok, adatok, papíralapú dokumetumok	adatvédelmi szabályok megsértése, hátrányos jogi következmények	személyes adatok szabálytalan vagy hanyag kezelése	hátrányos jogi következmények	Adatvédelem és a személyes adatok titkossága, GDPR adatmegfelelőség, NAIH felügyelet	5	1	5	a meglévő kockázat elfogadva	további intézkedés nem szükséges	3	1	3	nem			Folyamatban
6	Elektronikus dokumentumok, adatok, papíralapú dokumetumok	adatok kiszivárgása, bizalr	információk hibás-, hanyag kezelése, szabálytalan levelezés, faxolás, file küldés, nyomtatás	adatvesztés, adatok kiszivárgása	Információkezelési eljárások (IT szabályzat)	5	1	5	a meglévő kockázat elfogadva	további intézkedés nem szükséges	5	1	5	nem			elvégezve
7	Elektronikus levelezési rendszer	e-mail rendszer szabálytalan használata	az email használat szabályozására és annak ismeretének, ellenőrzésének hiánya	adatok kiszivárgása, vírusok behatolása, rendszer túlterhelése, levéltitok megsértése, hátrányos jogi következmények	Elektronikus üzenetek küldése/fogadása	4	1	4	Kockázatcsökkentő intézkedés szükséges	Csak megfelelő átirányítás okkal, céges domain-es tartományban, illetve a Főügyelet esetében 1 db Microsoft tartományban létrehozott email-ek forgalma	4	1	4	nem			elvégezve
8	Hálózati aktív elemek, Szerver számítógépek	adatok elvesztése, vagy a működés megszakadása	elégtelen, vagy hibás mentések, mentési állományok keveredése, azonosíthatatlansága, mentési ütemezés hiánya, mentés megőrzési idők hibás beállítása,	adatvesztés, rendszerek üzemképtelensége, BCP/DRP tevékenységek lehetetlenné válása	Információk biztonsági mentése	5	1	5	a meglévő kockázat elfogadva	további intézkedés nem szükséges	5	1	5	nem			Folyamatban
9	LAN, WAN, Desktop számítógépek	szabálytalan internet használat	szabályok, tudatosság, védelmi megoldások hiánya vagy elégtelensége	munkaidő kiesés, információ kiszivárgás, hátrányos jogi	Hálózati szolgáltatások használatára vonatkozó szabályzat	3	1	3	a meglévő kockázat elfogadva	további intézkedés nem szükséges	3	1	3	nem			Folyamatban
10	Mentési adathordozók	Adatok kiszivárgása	adatmentesítés elmaradása	adatok kiszivárgása, jogi következmények	Berendezések biztonságos selejtezése, illetve újrafelhasználása	3	1	3	a meglévő kockázat elfogadva	további intézkedés nem szükséges	3	1	3	nem			Folyamatban
15	Minden vagyonelem	Bizalmas információk nem	az osztályozási elvek hiánya, következetlensége, vagy hiányos ismerete	adatok kiszivárgása, károkozás ügyfélnek, hátrányos jogi következmények	Osztályozási elvek	3	2	6	az osztályozási elvek gyakorlati alkalmazása hiányzik	gyakorlatban alkalmazni kell az osztályozási elveket (pl. iratmegsemmisítés esetén ennek megfelelően kell eljárni)	3	1	3	igen	2022.12.31	projektvezetők, adatvédelmi tisztviselő, rendszergazda	Folyamatban
16	Mobil adathordozók (pendrive, cd, dvd, ...)	Adatok kiszivárgása	adathordozók engedélyezetlen kivitele	adatok kiszivárgása	Vagyontárgyak eltávolítása	3	3	9	információk kiszivárgása, visszaélések	mobil adathordozók használhatóságának korlátozása műszaki	3	3	9	igen	2023.12.31	Vezetők, Irodavezető, rendszergazda	Folyamatban
18	Mobil számítógépek és mobiltelefonok	mobil eszközök sérülése, elvesztése, ellopása	a mobileszközök védelmének hiányos vagy hibás szabályozása, tudatosság hiánya	adatok elvesztése, adatok kiszivárgása	Berendezések biztonsága a telephelyen kívül	4	1	4	notebook lopások adatok kiszivárgása Kockázatcsökkentő	mobil adathordozók használhatóságának korlátozása műszaki eszközökkel (titkosítás)	3	1	3	nem			elvégezve

12. Táblázat Kockázatkezelési terv
(Forrás: Saját szerkesztés)

	Változások, érintett vagyonelem	Feladatok	Érintett szervezeti vezető	Határidő
1.	Jelszavak tárolása és kezelése	Központi jelszószéf létrehozása, jelszó adatbázis biztonsági mentése	Rendszergazda, ügyvezető	2022.12.31
2.	Kockázatelemzés aktualizálása	December 31-i határidejű feladatok elvégzése	Rendszergazda	2022.12.31
3.	IT Vagyonleltár aktualizálása	Laptop beszerzések, telefon beszerzések, szoftverek, licenszek, jelszavak, verziókövetés	Rendszergazda	2022.12.31
4.	Weboldal	SSH tanúsítványok beszerzése megtörtént, új weboldal aktualizálása folyamatban	Rendszergazda	2022.12.31
5.	Szoftverek	Verziókövetés, előfizetések	Rendszergazda	2022.12.31
6.	Szerver	karbantartás, adatmentési policy aktualizálása, vészhelyzeti próba, virtuális gépek, Internetkapcsolat duplikálása	Rendszergazda	2022.12.31
7.	Tárolás	NAS beszerzése, aktív és archív adatok költöztetése, Veracrypt kikapcsolása, elektronikus dokumentumok éves archiválása	Rendszergazda, valamennyi vezető	2022.12.31
8.	Telefonok	ESET felügyeleti funkciók bekapcsolása valamennyi készüléken, Vagyonvédelmi ágazatban Life360 GPS alapú helyzetmeghatározás aktiválása	Rendszergazda, ügyvezető	2022.12.31
9.	Elektronikus felületek, hozzáférések	EKR, Ügyfélkapu, Cégkapu, NAV köztartozásmentes portál	Rendszergazda	2022.12.31
10.	Dokumentumkezelés	Irodai dokumentációs rendszer, iktatási rend felülvizsgálata, iratok fizikai elhelyezésének szakszerű biztosítása, archív iratok raktározása és biztonságos megsemmisítésének felülvizsgálata	Rendszergazda, irodavezető	2022.12.31
11.	Érintésvédelmi vizsgálat	Érintésvédelmi éves ellenőrzés, jegyzőkönyv készítése	Rendszergazda, munkavédelmi felelős	2022.12.31
12.	Zárt láncú irodai kamerarendszer ellenőrzése	Felvételek törlése, szükség esetén archiválása, műszaki ellenőrzés	Rendszergazda, technikai munkatárs	2022.12.31
13.	Elektromos áramellátás zavartalanságának biztosítása	Szünetmentes tápegység akkumulátorának cseréje	Rendszergazda	2022.12.31

4.1.4. Alkalmazhatósági nyilatkozat elkészítése

Az MSZ ISO/IEC 27001:2014-es szabvány által **kötelezően előírt dokumentumok** egyike az alkalmazhatósági nyilatkozat. (6.1.3 d pont szerint). Tulajdonképpen ebben igazoljuk, hogy a szabvány „A” mellékletében lévő kontrollokat megfelelő intézkedésekkel végrehajtottuk. A rendszer működtetéséért felelős vezető, valamint az auditor munkájának „mankójaként” szolgál, tartalmazza a szabályozási célokat, kontrollokat, azok indoklását, valamint a szabályozásból kizárt területeket. Szintén terjedelmi okokból ennek a több tízoldalas dokumentumnak csupán első két oldalát tudom bemutatni.

Alkalmazhatósági nyilatkozatunk tartalmazza a következőket:

- Kockázatkezelési szabályozási célok és intézkedések
- ISO/IEC 27001:2013 szabvány „A” melléklet óvintézkedései, valamint a vonatkozó szabályozások közötti összefüggéseket
- Az ISO/IEC 27001:2013 szabvány „A” mellékletben felsorolt szabályozási célok és intézkedések bármelyikének kizárását, valamint a kizárás indoklását.:

13. Táblázat Alkalmazhatósági nyilatkozat
(Forrás: Saját szerkesztés)

MSZ ISO/IEC 27001:2014 Alkalmazhatósági nyilatkozat SAFETY SECTOR VAGYONVÉDELMI Kft.

Szabvány követelmény			Hivatkozás	Megjegyzés
A5. Információbiztonsági irányelvek			-	-
A5.1. Az információbiztonság vezetői irányítása			-	-
Cél: Biztosítani a vezetői irányítást és támogatást az információbiztonság számára az üzleti követelményekkel és a vonatkozó törvényekkel és jogszabályokkal összhangban.				
A5.1.1.	Információbiztonsági irányelvek	*Intézkedés* Információbiztonsági irányelveket kell meghatározni, a vezetés által jóváhagyni, közzétenni, valamint a munkatársak és a fontos, külső érdekelt felek felé kommunikálni.	Komplex MIR/IBIR dokumentáció IBSZ	Ellenőrizve, rendelkezésre áll
A5.1.2.	Az információbiztonsági irányelvek átvizsgálása	*Intézkedés* Az információbiztonsági irányelveket tervezett időközönként vagy jelentős változások esetén át kell vizsgálni, hogy a folyamatos alkalmasságuk, megfelelőségük és eredményességük biztosítva legyen.	Vezetőségi átvizsgáláskor	A többi irányítási rendszer elem felülvizsgálatakor fog megtörténni
A6. Az információbiztonság szervezete				
A6.1. Belső szervezet				
Cél: Létrehozni egy vezetési keretrendszert az információbiztonság megvalósításának és működtetésének kezdeményezésére és felügyelet alatt tartására a szervezeten belül.				
A6.1.1.	Információbiztonsági szerepek és felelősségek	*Intézkedés* Minden információbiztonsággal kapcsolatos felelősséget meg kell adni, és ki kell osztani.	*IBSZ, IBSZ 2. melléklet 2. fejezet*	*Munkaköri leírások kiegészítése szükséges.*
A6.1.2.	Feladatkörök szétválasztása	*Intézkedés* Az egymással ütköző kötelességeket és felelősségi területeket szét kell választani annak érdekében, hogy csökkenjen a lehetősége a szervezeti vagyonelemek jogosulatlan vagy nem szándékos módosításának, illetve az azokkal történő visszaélésnek.	*Eljárásokban; Munkaköri leírásokban*	*Kézikönyv módosítása szükséges.*
A6.1.3.	Kapcsolat a hatóságokkal	*Intézkedés* Megfelelő kapcsolatokat kell fenntartani az illetékes hatóságokkal.	*Értékelések; Vezetői beszámoltatások, IBSZ 2. melléklet 2.1.6. fejezete*	*Havi szintű kapcsolattartás*
A6.1.4.	Kapcsolat szakmai csoportokkal	*Intézkedés* Megfelelő kapcsolatot kell fenntartani szakmai csoportokkal vagy más specializálódott biztonsági fórumokkal és szakmai egyesületekkel.	*IBSZ 2. melléklet 2.1.7. fejezete*	
A6.1.5.	Információbiztonság a projektvezetésben	*Intézkedés* Az információbiztonsággal foglalkozni kell a projektvezetésben - tekintet nélkül a projektek típusától.	*IBSZ 2. melléklete*	*A projektvezetők folyamatainak egységesítése szükséges. Policy kidolgozása javasolt*
A6.2. Mobil eszközök és távmunka				
Cél: Biztosítani a távmunka és a mobil eszközök használatának biztonságát.				
A6.2.1.	Irányelv mobil eszközökre	*Intézkedés* Irányelvet és azt támogató biztonsági intézkedéseket kell bevezetni a mobil eszközök használatával járó kockázatok kezelésére.	*IBSZ 3. melléklet IBSZ 7. melléklet*	*Az összes mobil eszközt rendszergazdai felügyelet alá kell vonni. ESET beszerzése. Munkaköri leírások kiegészítése is szükséges ennek*

Szabvány követelmény			Hivatkozás	Megjegyzés
Cél: Védeni a szervezet érdekeit a munkaviszony megszüntetésének vagy megváltoztatásának folyamatában.				
A7.3.1.	A munkaviszony megszüntetéséhez vagy megváltoztatásához kapcsolódó felelősségek	*Intézkedés* A munkaviszony megszűnése vagy megváltozása után is érvényben maradó információbiztonsági felelősségeket és kötelességeket meg kell határozni, közölni kell az alkalmazott vagy a szerződéses munkatárs felé, és ezeket érvényesíteni kell.	*IBSZ 5. melléklet 4.1. fejezete Munkaköri leírások*	*A megszűnő munkaviszonyok esetén alkalmazni kell az előírásokat. Dokumentumok visszaszolgáltatás át szabályozni kellene. Körbejáró papír elkészítése.*
A8. Vagyonelemek kezelése				
A8.1. A vagyonelemekért viselt felelősség				
Cél: Azonosítani a szervezeti vagyonelemeket és meghatározni a megfelelő védelmi felelősségeket.				
A8.1.1.	Vagyonleltár	*Intézkedés* Az információs vagyonelemeket és az információfeldolgozó eszközöket azonosítani kell, ezeknek a vagyonelemeknek egy leltárát kell kialakítani, és azt karban kell tartani.	*IBSZ 3. melléklet 2 fejezet Kockázatelemzés részes*	*Informatikai felügyeleti szoftver beszerzése javasolt. SpiceWorks pl. szoftver és hardver nyilvántartás folyamatban. Iroda zárás, szekrények bezárása, dokumentumok védelme, stb.*
A8.1.2.	A vagyonelemek felelősei	*Intézkedés* A vagyonleltárban szereplő vagyonelemek esetében be kell tölteni a gazdaszerepet.	*IBSZ 3. melléklet 2 fejezet Kockázatelemzés része*	
A8.1.3.	A vagyonelemek elfogadható használata	*Intézkedés* Az információk, valamint az információkkal és információfeldolgozó eszközökkel kapcsolatos vagyonelemek elfogadható használatára vonatkozó szabályokat azonosítani kell, dokumentálni kell és be kell vezetni.	*IBSZ 3. melléklet 2 fejezet Kockázatelemzés része*	
A8.1.4.	A vagyonelemek visszaszolgáltatása	*Intézkedés* Minden alkalmazottnak és a külső felek felhasználóinak vissza kell szolgáltatniuk a birtokukban lévő, összes szervezeti vagyonelemet, ha megszűnik a munkaviszonyuk, szerződésük vagy megállapodásuk.	*IBSZ 5. melléklet 4.2 fejezet*	*A külső felek esetén hogyan járunk el?*
A8.2. Információosztályozás				
Cél: Biztosítani, hogy az információk a szervezetben betöltött fontosságukkal összhangban kapjanak védelmet.				
A8.2.1.	Az információk osztályozása	*Intézkedés* Az információkat osztályozni kell a jogi követelmények, az értékük, a kritikusságuk, valamint a jogosulatlan nyilvánosságra hozásra és módosításra való érzékenységük szerint.	*Komplex MIR/IBIR Kézikönyv IBSZ 4. melléklete 2.1. fejezet*	*Az előírások alkalmazása szükséges. Informatikai oldalról és dokumentumok kezelési oldalát is meg kell vizsgálni.*
A8.2.2.	Az információk megjelölése	*Intézkedés* Megfelelő eljárásokat kell kialakítani és bevezetni az információk megjelölésére a szervezet által elfogadott információosztályozási módszerrel összhangban.	*Komplex MIR/IBIR Kézikönyv IBSZ 4. melléklete 3. fejezete*	

4.1.5. Szabályozási környezet kialakítása

Az IBIR, mint jól dokumentált irányítási rendszer szabályozási környezetének létrehozása során, a 9001-es minőségirányítási rendszer **dokumentumhierarchiájának** megfelelő struktúrában, az információvédelem célitűzéseinek és folyamatainak megfelelő formában és tartalommal hoztam létre, a fizikai és logikai védelmi szint mellett a harmadik pillérként, amit **adminisztratív védelemnek** nevezünk. A hierarchia legfelső szintjén az **Információbiztonsági Politika és Stratégia** áll, mely dokumentumban a szervezet egészére vonatkozóan nyilvánítjuk ki a menedzsmentnek az információbiztonsági iránti elkötelezettségét, valamint ebben a dokumentumban jelöltem ki a legfontosabb IBIR céljokat:

1 Az információbiztonsági politika meghatározása, célkitűzése, tárgyköre, kiterjedése a szervezet egészére vonatkozóan.
2 Az IBIR szervezet létrehozása, a szervezeti struktúra bemutatása.
3 A társaság informatikai környezetének zavartalan és folyamatos működésének biztosítása, figyelemmel a szervezet külső környezeti tényezőire, valamint a vállalti kultúrára.
4 Az adatvédelem és adatbiztonság szabályozásának fontossága a szervezeti célok elérése érdekében.
5 Az adatok hitelességének, integritásának, sértetlenségének és rendelkezésre állásának biztosításának a vállalat működésére gyakorolt hatásának bemutatása.
6 Az informatikai rendszert fenyegető veszélyek megelőzése, elhárítása, az informatikai és információ- és adatbiztonsági incidensek kezelésének indokai.
7 Az informatikai és információtechnológiai rendszerek és eljárások tervezése, kivitelezése, megvalósítása és fejlesztése, ehhez a menedzsment és tulajdonosi támogatás kinyilvánítása.
8 A társaságban az információ szabályozott és hatékony áramlásának szervezési és technikai eszközökkel történő támogatásának bemutatása a szervezeti céloknak megfelelően.

Mivel a túlbonyolított dokumentációs rendszer a véleményem és a gyakorlati tapasztalataim szerint bármilyen rendszernek inkább a működési gátjává, mint elősegítőjévé válik, ezért a szakirodalomban ajánlott Információbiztonsági Stratégiát a politikával összevontam, az eggyel alacsonyabb dokumentációs szintre kerülő Információbiztonsági Irányítási Rendszer Szabályzatot, vagy Informatikai Biztonsági Szabályzatot pedig be sem

vezettem. Helyette a Biztonsági Politika, illetve a közvetlenül felhasználói szintre tervezett Informatikai, ügyviteli, vagyonvédelmi és biztonságtechnikai szabályzat került részletesebb terjedelemben bevezetésre. A hierarchikus felépítésű dokumentációs rendszert a 13. ábra tartalmazza.

13. Ábra: IBIR dokumentációs rendszer
(Forrás: Saját szerkesztés)

Amint látható, a legalsó szinten találhatók a szabványban kötelezően előírt bizonyítékok dokumentumai, míg a felső három szint az előírásokat és követelményeket tartalmazó dokumentumokat tartalmazza.

Az informatikai szabályzatban rögzítettem az IBIR szervezet érintett szereplőinek beosztását, feladatait, hatáskörét és felelősségét, bemutattam a működtetés folyamatait, a kapcsolódó infrastruktúrát, a biztonsági követelményeket és hivatkozva a kapcsolódó szabályok rendelkezéseit.

Két részből álló Informatikai Szabályzatot készítettem, ez első, **Általános Rendelkezések** rész a fentebb felsorolt, **technológiafüggetlen részeket**, míg a második rész, az **Informatikai Kézikönyvet** tartalmazza, ahol a felhasználók részletes leírásokat, gyakorlati útmutatásokat kapnak az IBIR folyamatok és technológiai elemek összekapcsolásából eredő követelményekről, a szoftver és hardver eszközök szakszerű és biztonságos működtetéséről.

Az Általános Rendelkezések technológiafüggetlen területeket szabályozó részeit a következő táblázat mutatja be, a teljesség igénye nélkül.

14. Táblázat IT szabályzat technológiafüggetlen területeket szabályozó részei *(Forrás: Saját szerkesztés)*

Általános Rendelkezések – technológiafüggetlen eljárások	
Szabályozott területek	**Szabályozott területek**
Információ biztonsági irányelvek, belső szervezet, felelősségi körök	Kockázatértékelés, kockázatkezelés
Általános óvintézkedések	Az információs vagyon osztályozása és ellenőrzése
Tudatosság, képzés, vezetőségi felelősség és átvizsgálás, belső audit	A szabályzat szervezeti és tárgyi hatálya
Személyek, valamint az egyes munkakör meghatározásának és erőforrással való ellátásának folyamata	A felhasználók oktatása, képzése
Biztonsági események és incidensek kezelésének indoklása	A fizikai és környezeti biztonság
Az informatikai és biztonságtechnikai eszközök biztonsága	Az információbiztonsági, informatikai rendszer tervezése és üzemeltetése
A Rendszergazda munkakör	A kommunikáció biztonsága
Hozzáférés-ellenőrzés és szabályozás	Támogató folyamatok, üzletmenet folytonosság.
Munkajogi követelmények	Felülvizsgálatok, auditok

Az informatikai szabályzat technikai jellegűmunkautasításait az alábbi táblázat tartalmazza, szintén a teljesség igénye nélkül:

15. Táblázat IT szabályzat technikai munkautasításai
(Forrás: Saját szerkesztés)

Informatikai Kézikönyv technikai jellegű utasítások	
Szabályozott területek	**Szabályozott területek**
Munkaállomások és a számítógépes hálózat erőforrásainak, az operációs rendszer használata	Az operációs rendszer állományainak védelme
Az adathordozók kezelése és biztonsága	Belépés, hitelesítés, egyéb autentikációs eljárások
Fájlműveletek, Dokumentumkezelés, titkosítási intézkedések	Elektronikus levelezés
Multimédia, kép és hangfájlok, audiovizuális alkalmazások	Internet, böngészés biztonsága
Mobil eszközök használata, távmunka	Hordozható háttértárak
Biztonsági események és incidensek kezelése	Kapcsolódó dokumentumok
Felhasználókat érintő hacker támadások típusa, védekezés ellenük,	Adatmaszkolás, biztonságos adattörlés

Az Ügyviteli és Iratkezelési Szabályzat, a **Biztonságtechnikai és Vagyonvédelmi Szabályzat,** valamint az Informatikai Szabályzat több ponton kapcsolódnak egymáshoz, az egyik dokumentumban szabályozott területet a másik dokumentumban már csak meghivatkoztam, a felesleges duplikációk elkerülése és a verziókövetés egyszerűsítése érdekében. A dokumentációs rendszer harmadik szintjén lévő alkalmazásoknak, a szoftver és hardver eszközöknek a gyári használati útmutatói, manualok, gépkönyvek pdf formátumban a szervezet belső oktatási felületén megtalálhatóak, azok példányait a rendszergazda folyamatosan aktualizálja. Azokat a technikai dokumentációkat, amelyek a számítógépes hálózati rendszer logikai és fizikai szervezési rendjét rögzítik, a telepített szoftverek és hardver eszközök részletes technikai leírását tartalmazzák, már csak és kizárólag **a rendszergazda, a biztonságtechnikai és villamosmérnök munkatárs** érheti el közvetlenül. Itt kerülnek szabályozásra a kifejezetten szakembereknek készített **technikai intézkedések**, néhány közülük:

- Számítógépes tartományi erőforrásokhoz való hozzáférésvezérlés szabályozása, mint például a hálózati autentikáció, azonosítás tudás, birtoklás és tulajdonságalapú szervezési eljárásai,
- A biztonságos internetes tevékenységhez szükséges SSL tanúsítványok kezelése,
- Felhasználók jogosultsági rendszerének IT vonatkozású eljárásai,
- Hálózati forgalom figyelése, a hálózati protokollok felügyelete, a hálózati sérülékenységek folyamatos figyelése, tesztelése,
- Tartományi csoportházirendek kialakítása,
- Biztonsági mentések ütemezett elvégzése, a 3-2-1 szabálynak megfelelően az egyik mentési állomány szállítása egy másik földrajzi helyre,
- Tűzfalak konfigurálása, távoli hozzáférésvezérlés felügyelete,
- Az irodai vezeték nélküli hálózat folyamatos biztonsági felügyelete, a hálózati forgalom szoftveres eszközzel történő figyelése,
- Rendszeresített kriptográfiai eljárások végrehajtása,
- Elektronikus aláírásokkal és digitális tanúsítványokkal kapcsolatos intézkedések,
- Eszközbeszerzés esetén azok konfigurálása, titkosítása, visszavétel esetén azok biztonságos törlése, a kiadott felhasználói jogosultság megszüntetése,
- Vírusdefiníciós adatbázisok frissítése.

A szabvány és több esetben jogszabály is előírja, hogy a kapcsolódó **dokumentumokat felügyelet alatt tartsuk**, az események bizonyítékainak rögzítését és sértetlen megőrzését biztosítják a hierarchia legalsó szintjén található jegyzőkönyvek, naplók, vizsgálati jelentések. és elektronikus úton tárolt számítógépes LOG fájlok.

További intézkedésként, az irodai tevékenységet a **minőségmenedzsment 5S módszerének** alkalmazása szerint szabályoztam, ami véleményem szerint irodai, informatikai környezetben kiemelten fontos ezért a következő, munkakultúrát javító intézkedéseket vezettem be:

„Tiszta íróasztal" szabály

Mindenki köteles rendet tartani íróasztalán, a munkavégzés befejezését követően az íróasztalon irat, adathordozó nem maradhat, mindent a biztonsági osztályának megfelelően el kell zárni.

„Tiszta képernyő" szabály

Munkahelyet még ideiglenesen is elhagyni, csak a számítógép zárolását követően lehet.

A munkaállomásokat úgy állítottam be, hogy ha azokat hosszabb időre, több mint 3 perc, felügyelet nélkül hagyják, akkor a számítógép zárolja magát, és csak a felhasználó újbóli azonosítását követően lehessen azt használni. A számítógépek Asztal mappájában csak ideiglenesen lehet fájlokat tárolni.

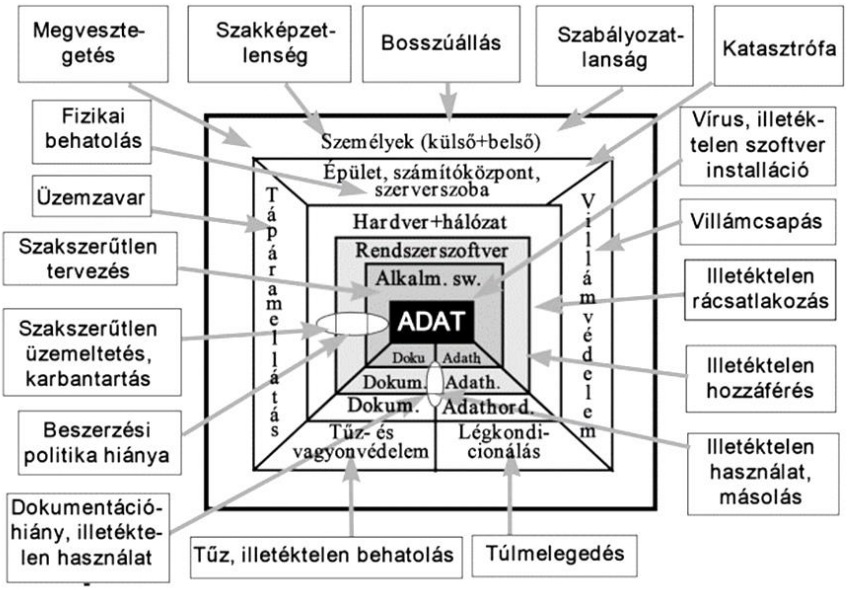
„Tárgyalók rendje"

Informatikai, kommunikációs eszköz nem maradhat a tárgyalóban, a kivetítőket ki kell kapcsolni a megbeszélés végén, a rajztáblákon lévő feliratokat pedig törölni kell. Különösen bizalmas megbeszéléseket csak védett tárgyalóban lehet lefolytatni.

4.1.6. Fizikai környezet biztonsága

A fizikai környezet vagyonvédelmi és biztonságtechnikai kritériumok szerinti biztosítása az IBIR három védelmi mechanizmusának egyik eleme. a **logikai védelem, és adminisztratív védelem** mellett**.** Az irodai és informatikai infrastruktúra védelmének megszervezése a vagyonvédelmi és biztonságtechnikai szakma kompetenciájába tartozik, de szerves elemét képezik az IBIR-nek is. Számtalan veszély fenyegetheti az infrastruktúrát, ennek tömör szemléltetését mutatja a 14. ábra.

14. Ábra: A fizikai biztonság logikai sémája
(Forrás: Muha, Krasznai 2014)



A biztonságtechnika által **hagymahéj elvnek** nevezett objektum helyiségeinek zónafelosztása, valamint a **mechanikai védelem**, **elektronikai betörésvédelmi jelzőrendszer**, és **élőerős őrzésvédelem** hármasa nyújtja azt az elfogadható védelmi szintet,

amit a mi szervezetünk megkövetel. Cégünk a legszigorúbb szabályozás alá esik, mivel lő és tűzfegyverek, maroklőfegyverek, valamint haditechnikai eszköznek minősülő rádiósugárázást felderítő eszközöket is tárolunk. Ennek érdekében, ahol szükséges a nyílászárókat rácsokkal, biztonsági üvegfóliával, valamint biztonsági zárakkal védjük. Többkörös riasztórendszer védi az irodai infrastruktúrát, az épületbe történő bejutás, az irodai beléptetőrendszer, valamint a fegyverszoba riasztórendszere egymástól függetlenül működnek.

Az élőerős őrzésvédelem mellett kivonuló távfelügyeleti szolgáltatóval is rendelkezünk. Irodáinkban a legszigorúbb védelmi szinttel rendelkező eszközöket, iratokat, MABISZ minősítésű lemez és páncélszekrényekben tároljuk. Az iroda védelmét megfelelően előkészített és begyakorolt **katasztrófa elhárítási tervben** rögzítettük, az infrastruktúrát ért kritikus támadás utáni haladéktalan helyreállítást pedig **üzletmenet folytonossági tervben** rögzítettük. A biztonságos körlet kialakításának érdekében az irodaépületbe történő be és kiléptetések rendjét, valamint az általános vagyonbiztonsággal kapcsolatos utasításokat és eljárásokat (kulcsfelvétel, épület riasztó használata, egyes irodahelyiségek használatának rendje, munka-tűz, érintésvédelmi és balesetvédelmi előírások), külön szabályzatban rögzítettem vagyonvédelmi szakember bevonásával.

Az információbiztonság informatikai rendszerének kritikus eszközeit (szerverek, hálózati eszközök, adattárolók, mobil eszközök) a szervezet külön helyiségekben, illetve kiemelten védetten tároljuk. Ezeknek a helyiségeknek a használatát a fizikai és környezeti biztonság általános előírásainál lényegesen szigorúbb szabályrendszer korlátozza. (belépési jogosultság a helyiségekbe, ezek adminisztrálása, tűzvédelem, érintésvédelem, valamint külön rácsos ajtó felszerelése). A berendezések megfelelő és biztonságos áramellátásának biztosítása, szünetmentes tápegység alkalmazása, leválasztó áramkörök és villámhárító beszerelése a megfelelő szabványoknak és villamossági előírásoknak megfelelően történt. Magasfeszültségű berendezés meghibásodása esetén annak szakszerű kezelését szakemberre bízzuk.

A Munkavédelmi Megbízottunk évente a rendszergazdával és az üzemeltetésért felelős belső munkatársakkal (gondnok, karbantartó) elvégzi a teljes irodai elektromos hálózat éritésvédelmi ellenőrzését, arról megfelelő kompetenciával rendelkező szervezettel, személlyel érintésvédelmi jegyzőkönyvet vesz fel.

Az energetikai és távközlési kábelek biztonságos elhelyezésének szabályzatát a technikai munkatárs készítette, villamosmérnök képzettségű szakember bevonásával. A berendezések rendszeres karbantartása, a gépek portalanítása, takarítása, vezetékek, aljzatok ellenőrzése, biztosítékok szükség szerinti cseréje az ajánlott szervizidőszakban, karbantartási ciklusokban történik.

4.1.7. Humánerőforrásokhoz kapcsolódó kockázatok

Mint minden ember által alkotott rendszer, az IBIR esetében sincs ez másképp: a rendszer leggyengébb pontja maga az ember. Az ember az IBIR számára a maga motivációs és emocionális tulajdonságaival fekete dobozként jelenik meg, amiből olyan kockázatok származnak, amelyek pusztán adminisztratív kezelése lehetetlen. Minden előírás, szabály annyit ér, amennyit betartanak belőle, a hanyagság és gondatlanság mellett a szándékos károkozás, vagy a hackerek, esetleg a versenytársak üzleti hírszerző alkalmazottai által elkövettet adatlopások elleni védelem technikai és folyamatbeli szabályozást is igényelnek. Az állandó vezetői felügyelet és szisztematikus ellenőrzés, az éppen elégséges jogok kiosztásának elve, a megfelelő munkaszerződések, munkaköri leírások, pontosan kidolgozott hatásköri feladat és felelősségi körök jelenthetnek elegendő védelmet az információbiztonság szempontjából. Munkajogászokkal egyeztetve ezért a HR kérdésekben az alábbiakat vezettem be:

- Az új belépők kiválasztása meghatározott biztonsági protokoll mellett történik vetting tevékenység elvégzését követően, a kompetenciák és képességek ellenőrzésén túl munkavállaló csak biztonsági ellenőrzést követően kezdheti meg munkaviszonyát.
- A munkafelvételi, valamint a szerződéskötési eljárás során – törvényes keretek között – az IBIR vezető által meghatározott információbiztonsági szempontból fontos munkakörök betöltőinél felvételi folyamaton belül olyan további vizsgálatot, azaz átvilágítást kell lefolytatni, melyek pontos információt szolgáltatnak a jelentkező információbiztonsági alkalmasságáról, előéletéről, előző munkahelyein, valamint közösségi médiákban tanúsított magatartásáról.

- Cégünknél az HR kockázatok csökkentések érdekében az új munkatársaknak az alábbi dokumentumokat és a belépési ellenőrző listában meghatározott tájékoztató anyagokat kell megismerniük, továbbá az alábbi nyilatkozatokat, megállapodásokat kell aláírásukkal igazoltan elfogniuk:

16. Táblázat: Felvételi eljárás kötelező dokumentumai
(Forrás: Saját szerkesztés)

1.	Adatkezelési hozzájáruló nyilatkozat
2.	Munkaszerződés, tájékoztató és munkaköri leírás
3.	Információbiztonsági Politika
	Információbiztonsági képzés oktatási jegyzőkönyve
4.	Tűzvédelmi szabályzat kivonat. Munkavédelmi szabályzat kivonat
5.	Vagyonvédelmi és biztonságtechnikai szabályzat kivonat
6.	Titoktartási és adatvédelmi nyilatkozat
7	A foglalkoztatásnak megfelelő munkaköri speciális dokumentumok

Minden alkalmazottnak be kell tartania a Társaság információbiztonsági szabályait. Az információbiztonsági előírások szándékos és tudatos megsértéséből származó információbiztonsági incidensek szankcionálhatóak. Ilyen esetekben a fegyelmi eljárás módjának meghatározása a munkáltatói jogkörök gyakorlói, valamint az IBIR vezető felelőssége.

4.1.8. Mérés és felügyelet, oktatások és képzések

Mivel társaságunk korábban az információbiztonsági folyamatoknak objektív teljesítménymutató rendszerét egyáltalán nem alkalmazta, valamint mivel a szabvány kötelező dokumentumként tartja nyilván a megfigyelési és mérési eredmények bizonyítékait (9.1), ezért kiindulásként létrehoztam azokat a KPI-okat, valamint azok adatlapjait, melyek leginkább igazodnak mi szervezetünkhöz, továbbá összhangban vannak a kockázatelemzés során feltárt fenyegetésekkel és sebezhetőségekkel.

A Pareto elv 80-20-as szabálya, mely szerint a kialakult problémák 80 %-ért a tényezők 20%-a felel, úgy tűnik, hogy az IBIR-ben is nagyságrendileg pontos képet ad a fenyegetések, sérülékenységek és az esetlegesen bekövetkezett károkozás nagysága között, ezért olyan KPI-okat hoztam létre, melyekkel elsősorban a nagy számosságban előforduló, vagy nagy károkozásra lehetőséget adó eseményeket méri. A KPI lap aza alábbi táblázatban lévő adatokat tartalmazza:

17. Táblázat: KPI lap adattartalma
(Forrás: Saját szerkesztés)

KPI neve	rövid név, verziószám, sorszám
KPI státusza	kidolgozás, tesztelés, bevezetve, kivezetve
Leírás	a KPI rövid leírása, honnan vannak az adatok, milyen matematikai művelettel állítjuk elő a mutatószámot
Feladat	pontosan mit mér, miért fontos ez a mutató
Fontosság	3 fokozatú skála
Eszközök	A mérésbe bevont, vagy adatot szolgáltató eszközök
Gyakoriság	A mintavétel gyakorisága és a KPI előállításának gyakorisága
Megjegyzés	Kiegészítő információk

18. Táblázat: KPI kezdeti értékek és célállapotok
(Forrás: Saját szerkesztés)

KPI neve	Leírása	Mérés gyakorisága	Helyzetfelmérés állapota	Cél állapot
Felkészültség 1	az egy év alatt észlelt és megoldott biztonsági incidensek aránya	Évente	$= \frac{22}{28} = 79\ \%$	$= \frac{27}{28} = 96\ \%$
Email 1	felhasználói levelező fiókig 1 hónap alatt eljutott kártékony email-ek arány	Havonta	$= \frac{5}{30000}$ $= 1{,}66\ \%$	$= \frac{0}{30000}$ $= 0\ \%$
Észlelés 1	támadás észlelése és az arra adott válasz között eltelt időt adja meg, átlagban	Havonta	48 perc	kevesebb mint 15 perc
Adatvesztés 1	Adatvesztés során helyreállíthatatlanul megsemmisült fájlok száma	Havonta	4 db	0 db
Rendelkezésre-állás-1	Irodai infrastruktúra, belső hálózat működése	Havonta	$=\frac{10060\ perc}{10080\ perc} =$ $99{,}8\%$	$\frac{10080\ perc}{10080\ perc}$ $= 100\%$

A 18. táblázat pedig néhány létrehozott KPI-t tartalmaz a kezdeti értékekkel, valamint az IBIR bevezetése utáni cél állapottal.

A szervezetet valamennyi munkavállalójával, továbbá szükség esetén külsős érintett felekkel is tudatosítani kell, hogy a rendkívül gyorsan változó információtechnológiai környezetben az információbiztonsági **oktatások és képzések** mennyire fontosak. Mivel irodai tevékenységünk szinte minden pillanatban elektronikus úton kapcsolódik informatikai hálózatokhoz, az internethez, ezért az eszközök és szoftverek szakszerű használatán túl az oktatásunkat kiterjesztettem a kifejezetten internet felől várható fenyegetések felismerésére, a rosszindulatú, károkozás, vagy nyereségszerzés céljából elkövetett internetes csalásokra. Jelenleg a hackerek tevékenységének direkt vállalatokat célzó támadásai mind számosságában, mind a károkozás mértékében elképesztő módon, exponenciális mértékben növekednek, ezzel lépést tartani mind anyagi oldalról, mind oktatásmódszertani oldalról nagyon nehéz. A kulcsszó, a **biztonságtudatosság**, az állandó figyelés, az oktatott anyag naprakész szintű elsajátításán túl azok pontos betartása.

Ennek alapján elrendeltem, hogy új munkatárs csak és kizárólag akkor kap hozzáférési jogosultságot az informatikai erőforrások használatához, ha a munkajogviszonyhoz, vagy egyéb szerződéses jogviszonyhoz kapcsolódó dokumentumok aláírásra kerültek, továbbá a rendszergazda, az adatvédelmi tisztviselő, illetve a technikai munkatárs az új dolgozó informatikai alapképzettségéről meggyőződött, valamint őt alapszintű oktatásban részesítették. Ennek az oktatásnak a keretében a belépő munkavállaó megkapja az adatvédelemmel kapcsolatos képzést is a GDPR előírásainak tudatosításához. Az adatvédelmi oktatás egyik legfontosabb célja, hogy a dolgozó megfelelő tájékoztatást kapjon a Társaság által kezelt, illetve az általa adatfeldolgozói, esetlegesen adatkezelői minőségben feldolgozott adatokról, azok Adatatvédelmi Törvénynek megfelelő kezelési módjairól, valamint személyes felelősségéről az érintett folyamtokban.

Az oktatási anyag elkészítéséért az adatvédelmi tisztviselő és a rendszergazda felel. A szervezet az informatikai fejlődés folyamatos implementálása érdekében továbbá évente legalább egy alkalommal valamennyi munkatárs részére, - a biztonsági stratégia és informatikai szabályzat oktatásán túl, - képzési tervben előírt oktatást tart. A képzés, kifejezetten az egyes munkakörökhöz kapcsolódó új informatikai és biztonságtechnikai fejlesztésekre, valamint a megjelenő új technológiákra, alkalmazásokra terjed ki.

Az oktatási anyag cégünk szerverén az oktatási portál felületén valamennyi munkatárs részére hozzáférhető. Az oktatási terv egy példánya a *10.6. számú mellékletben* megtalálható, a nevek adatvédelmi okok miatt törlésre kerültek:

4.1.9. Biztonsági események és incidensek kezelése

A legalaposabban megtervezett IT rendszerekben is előfordulnak olyan események, amelyek az információvédelmi rendszer adminisztratív, fizikai, vagy logikai védelmére olyan hatást gyakorolnak, melyek során a felépített védelmi intézkedések nem érik el kívánt hatásukat és sérül az információs rendszerben lévő adatok bizalmassága, sértetlensége, vagy rendelkezésre állása. Ennek a kérdéskörnek a kezelése az Incidensmenedzsment feladata. Tehát valamely adatot arra nem jogosult személy ismer meg, vagy a hitelessége sérül, vagy az adat az eredeti helyén nem fellelhető. Ebben az esetben, optimális körülmények között a szervezet az incidens bekövetkezése előtt a fenyegetést már észleli, az incidens bekövetkezését felismeri, arra előírt határidőn belül hatékonyan reagál Ez a **PreDeCo, a Preventive-Detective-Corrective elv.**

Az adatvagyonban felhalmozott koncentrált tudás és vagyoni érték egy információbiztonsági incidens során viharos gyorsasággal képes „elolvadni”, ezért az IBIR kialakítása során, - figyelemmel a GDPR rendeletének párhuzamos vagy rokon szabályozási követelményrendszerére, - külön szabályzatban, részletes eljárásrendben, gyakorlatilag **munkautasítás szintjén szabályoztam** a végrehajtandó cselekményeket, a kezelésért felelős személyek körét, a dokumentálást és a bizonyítékok összegyűjtését. A bevezetett szabályozásnak megfelelően Információbiztonsági incidensnek kell tekinteni minden olyan eseményt, emberi cselekedetet, gépi működést, ami az IBIR dokumentumokban meghatározott alapelvek, célok, szabályok érvényesülését megsérti, függetlenül az elkerülhetetlen, véletlen, vagy, szándékos jellegétől.

Az eljárás során:

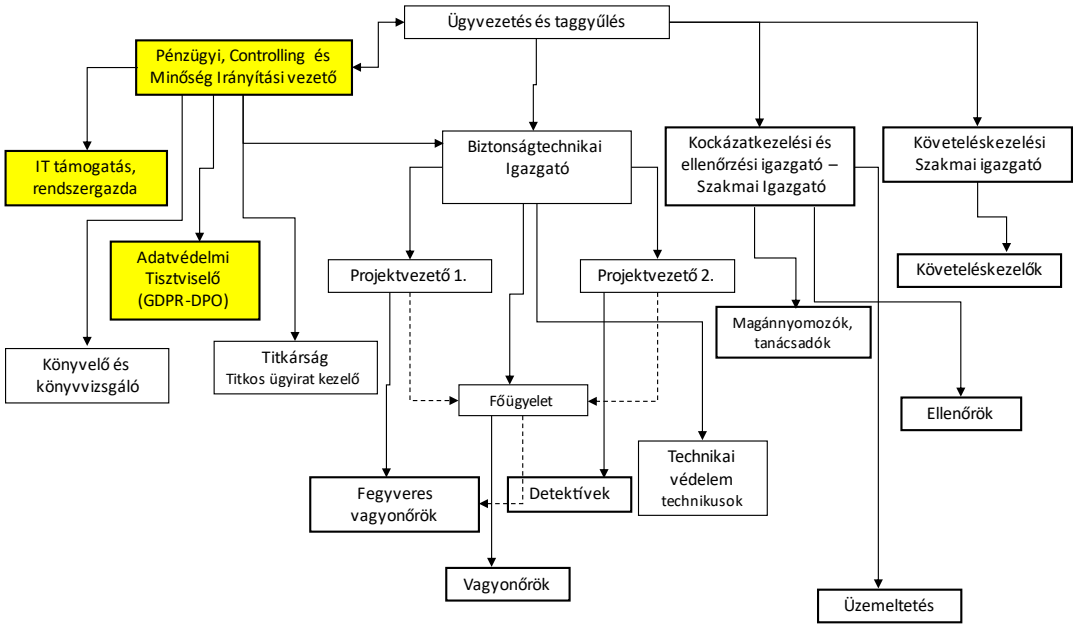
- Minden vélt vagy valós információbiztonsági incidenst a dolgozónak azonnal jelenteni kell a Rendszergazda és közvetlen vezetője felé.
- A jelentésben konkrétan meg kell határozni az esemény minden paraméterét.
- A bejelentő munkatársak kötelesek a rendszergazdától kapott utasításokat azonnal végrehajtani.

- A bejelentőnek az incidensről további személyeket tilos értesítenie.
- A rendszergazda azonnal gondoskodik az incidens elektronikus, vagy papír alapon feltalált bizonyítékainak összegyűjtéséről és megőrzéséről, egy esetleges későbbi jogi eljárásban történő felhasználásához.
- Azonnal megteszi a szükséges védelmi intézkedéseket az újabb információbiztonsági incidens elkerülése érdekében.
- Az IBIR vezető késlekedés nélkül lefolytatja a vizsgálatot, melynek során megállapításra kerül, hogy konkrétan milyen esemény történt, mekkora a károkozás mértéke, hogyan lehet a további károkat megelőzni, kit terhel a felelősség az adott ügyben.
- Objektív és gyors vizsgálatot követően a felelős személyt munkajogi eljárás alá kell vonni, jogosultságait ideiglenesen meg kell szüntetni.
- A feltárt sérülékenységet kockázatkezelési intézkedéssel haladéktalanul meg kell szüntetni.
- Bűncselekmény estén a rendszergazda fokozott gondossággal jár el a technikai jellegű bizonyítékok sértetlenmegőrzése érdekében.

4.1.10. Az IBIR szervezete

Az IBIR bevezetésével szervezetátalakítást is végrehajtottam, létrehoztam az **Adatvédelmi Tisztviselő** beosztást, továbbá kineveztünk egy dedikált **informatikus rendszergazdát** is, tevékenységük irányítását a Minőségbiztosítási Vezető, azaz én látom el. A módosított és egyszerűsített szervezeti struktúra az alábbi ábrán látható, eltérő színnel jelölve a létrehozott új pozíciókat:

15. Ábra: Az IBIR szervezete
(Forrás: Saját szerkesztés)



Amint látható, a szervezet **funkcionális** és tevékenységünkből adódóan szigorúan **hierarchikus** felépítésű, az információbiztonság pedig a szervezeti átalakítással hangsúlyos szerepet kap, közvetlenül az ügyvezetés és taggyűlésnek tartozik beszámolással, utasításadási és irányítási joga pedig a teljes szervezeti személyi állományra kiterjed. Ezzel biztosítottam, hogy a vezetés valamennyi tagja kellő elkötelezettséggel, támogatással, bizonyos értelmezésben közös felelősséggel viseltessenek az információbiztonság iránt. Az IBIR hangsúlyosabb szerepéből adódóan képviselteti magát a vállalati stratégia szintjén, jelentősen hozzájárul a szervezeti teljesítmény javulásához. A szervezetnél az alábbi beosztásokat és információbiztonsági felelősségi köröket hoztunk létre, illetve módosítottunk a szervezti felépítésben:

- Pénzügyi, Controlling és Minőségirányítási Vezető, mint IBIR vezető,
- IBIR megbízott,
- Rendszergazda, villamosmérnök és biztonságtechnikai mérnök munkatársak,
- Projektvezetők,
- Adatgazda, az adott információs körben.

IBIR vezető, főbb feladatai:

- Az Információbiztonsági Irányítási Rendszer működtetése és folyamatos fejlesztése,
- Az információbiztonsági szabályzatokban meghatározott feladatok ellátása,
- A szervezet képviselete a hatóságok és ügyfelek felé az információbiztonságot érintő megkeresésekben és kérdésekben,
- a szervezeti információbiztonsági tudatosság folyamatos fejlesztése,
- A biztonsági eseményekre, adatvédelmi és információbiztonsági incidensekre történő reagálás és a kivizsgálás irányítása,
- Az ügyvezetőtől és egyes estekben a taggyűléstől közvetlenül kapott IT-t érintő feladatok végrehajtása.

IBIR megbízott, főbb feladatai:

- Feladatai megegyeznek a IBIR vezető feladatkörrel. Munkáját az IBIR vezető irányítása alatt végzi,
- Az informatikai rendszerek technikai fejlesztésének és működtetésének irányítása az információbiztonsági követelményeknek megfelelően,
- Az információbiztonsági szabályzatokban meghatározott feladatok ellátása.

Rendszergazda, villamosmérnök és biztonságtechnikai mérnök, főbb feladatai:

- Az informatikai, villamos és biztonságtechnikai rendszerek üzemeltetése során az információbiztonsági követelmények betartása és az üzemelő rendszereken a követelményeknek megfelelő technikai működés megvalósítása.

Adatgazda, főbb feladatai:

- Az adatgazda felelős szervezési oldalról a felügyelete alá tartozó információk rendelkezésre állásának, sértetlenségének, bizalmasságának és hitelességének a megőrzéséért az információ teljes életciklusa során. Ezen belül:
- a felügyelete alatt álló dokumentumok, adatbázisok és azokat kezelő alkalmazások információbiztonsági besorolása, címkézése,
- a felügyelete alatt álló dokumentumokhoz adatbázisokhoz és azokat kezelő alkalmazásokhoz a hozzáférés felügyelete, az ezekre érvényes jogosultságok kiadásának az engedélyezése és visszavonatása,
- a felügyelete alá tartozó információk 3. félnek történő átadásának az engedélyezése,
- a felügyelete alá tartozó információk archiválásának és megsemmisítésének a felügyelete,
- Az adatgazdai szerepkört mindig az adatot tartalmazó vagy kezelő rendszer egy megszemélyesített felhasználójának kell betöltenie,
- Dokumentumok esetén a dokumentum tulajdonosa látja el az adatgazda szerepkörét,
- Adatbázisok esetén az adatgazdai szerepkört az adatbázis tulajdonosa látja el. Ha ez külön nem azonosított, akkor az adatbázist használó alkalmazás adatgazdája,
- Alkalmazások esetén az adatgazdai szerepkört az alkalmazásgazda, ennek hiányában a kulcsfelhasználó látja el.

4.2. Az IBIR bevezetési projekt folyamata

4.2.1. Projekt menedzsment tevékenység

Az IBIR bevezetéséről szóló menedzsment és tulajdonosi döntést követően megkezdtük a felkészülést a bevezetési projekt végrehajtására. Nagyvonalakban meghatároztuk a projekt lefutásának célként tartható időtartamát, költségkeretét, és a legfontosabb projekteredményt, ami a sikeres tanúsító autdit lefolytatását és a tanúsítvány megszerzését jelentette, ezzel **behatároltuk a porjekteredményt**. Kijelöltük a projekt vezetőjét, a szervezeten belül azokat a további tagokat, akik a projektben résztvesznek, meghatároztuk a projekt kompetencia szükségletét, ehhez elkészítettem **az emberi erőforrások szakmai leltárát**, ami az alábbit az alábbi táblázat szemléltet:

19. Táblázat: Kompetencia szükséglet
(Forrás: Saját szerkesztés)

Munkatár-sak	Kompetenciák						
	Pénzügy-számvitel és Controlling	**Rendszer-informati-kus**	**Vezető és belső auditor**	**Biztonság-techniai mérnök**	**Villamos-mérnök**	**Ügyvitel titkos ügyirat-kezelő**	**Vagyon-védelmi szakember**
Szabó József IBIR vezető	X	X	X				
[redacted]				X			
[redacted]					X		
[redacted]	X					X	
[redacted]				X			X
[redacted]		X					
[redacted]			X				

A projektciklus koncepció, tervezés-szervezés, végrehajtás és befejezés szakaszainak időbecslése alapján, előzetes ajánlatkérés után, megköttük a szerződést a felkészítő és a tanúsító cégekkel. A tervezés során kialakítottam az egyes projekttevékenységeket, meghatároztam a **tevékenységek logikai sorrendjét**, azokhoz erőforrásokat allokáltam, valamint egy közelítő pontosságú költségtervet is elkészítettem. Az időtervezést az alábbi lépések mentén végeztem el [Daróczi 2011]:

1. meghatároztam az egyes résztevékenységeket, amit **tevékenységjegyzékbe** foglaltam,
2. ezek közötti **logikai-függőségi kapcsolatok** alapján meg tudtam állapítani, hogy melyik tevékenységeket tudjuk párhuzamosan végezni és melyik tevékenység vár egy másik befejezésére,
3. meghatároztam az egyes tevékenységek időtartamait,
4. a teljesítési folyamat időtervét **Gantt diagramon** ábrázoltam,
5. a projekt kezdési és várható befejezési időpontját kijelöltem,
6. az egyes tevékenységek legkorábbi és legkésőbbi kezdési és befejezési időpontjait megállapítottam,
7. a **kritikus tevékenységeket** megjelöltem,
8. a tartalékidőket meghatároztam.

[1] adatvédelmi okból a résztvevő személyek nevét kitakartam.

Az egyes tevékenységek legkorábbi kezdési (ES- Earliest Start), legkorábbi befejezési (EF -Earliest Finish), a legkésőbbi kezdési (LS-Latest Start) a legkésőbbi befejezési (LF - Latest Finish) időpontjai alapján kiszámoltam az egyes tevékenységek időtartalékát (TS-Slack). Amint a táblázatból látható, a TS értékeknél két tevékenységen kívül sehol nincs tartalékidő, vagyis a **tevékenységek nagy része kritikus**, ezek bármelyikének megcsúszása esetén az egész projekt átfutási ideje megnövekszik.

20. Táblázat: Tevékenységjegyzék és időtartamok
(Forrás: Saját szerkesztés)

		Tevékenység jele	Időtartam	ES	EF	LS	LF	TS
1.	Menedzsment elhatározása és projektvezető megbízása	0-1	3	0	3	0	3	0
2.	Szakértői team-ek összeállítása, vezetői szerepek, hatáskörök kialakítása	1-2	3	3	6	3	6	0
3.	Információs Biztonsági Politika és Információs Biztonsági Stratégia megfogalmazása	1-5	4	3	7	3	7	0
4.	Szabványkövetelmények értelmezése	1-4	3	3	6	4	7	1
5.	A jelenlegi rendszer felmérése, folyamatok feltérképezése, rendszerhatárok és alkalmazási terület kijelölése	3-9	3	7	10	9	12	2
6.	Kiindulási és célállapot rögzítése	3-7	2	7	9	7	9	0
7.	Erőforrásigény meghatározása	6-8	2	9	11	9	11	0
8.	Bevezetési ütemterv elkészítése	7-9	1	11	12	11	12	0
9.	Folyamatok kialakítása és a szabványkövetelményekkel történő összhangba hozása *	8-13	6	12	18	12	18	0
10.	Szabályzatok hierarchikus szintjeinek kialakítása	8-11	2	12	14	12	14	0
11.	Rendszerdokumentáció elkészítése, illesztése a már működő irányítási rendszerekhez*	10-12	2	14	16	14	16	0
12.	Oktatás, képzés lebonyolítása	11-13	2	16	18	16	18	0
13.	Új szabályozás szerinti működés megkezdése, utána folyamatos figyelemmel kísérés, működésfelügyelet.	12-14	2	18	20	18	20	0
14.	Teljes körű belső audit végrehajtása	13-15	1	20	21	20	21	0
15.	Helyesbítések, utóellenőrzések megtétele	14-16	1	21	22	21	22	0
16.	Vezetőségi átvizsgálás	14-17	1	21	22	21	22	0
17.	Tanúsító szervvel szerződéskötés	16-18	1	22	23	22	23	0
18.	Tanúsítás megkezdése, dokumentumok átvizsgálása, helyszíni audit	17-19	2	23	25	23	25	0
19.	Szükséges helyesbítő intézkedések elvégzése	18-20	3	25	28	25	28	0
20.	Tanúsítvány kiadása	19-20	1	28	29	28	29	0
21.	Szabvány szerinti működés megkezdése, rendszerfelügyelet	19-21	1	28	**29**	28	**29**	0

A CPM háló felrajzolása nélkül is nyilvánvaló, hogy **a háló kifeszített**, ami ugyan projektmenedzsment szakirodalma szerint nem ajánlott, mindazonáltal az egyes projekttevékenységek alapidőtartamába, amik a tervben hetekben vannak megadva,

belekalkuláltam akkora tartalékot, ami a kifeszített háló okozta kockázatot jelentősen csökkentette.

A teljes projekt átfutási ideje 29 hét lett, ami figyelembe véve a szervezetünk nagyságát, a kialakítandó szabályozási kör adminisztratív feladatait, a kapcsolódó eszközbeszerzéseket, oktatásokat, valamint a teljes informatikai rendszer átkonfigurálását, a bevezetési időtervet reálisnak értékeltem. A projekt Gantt diagramja a következő oldalon található 21. táblázatban látható.

21. Táblázat: A teljes projekt Gantt diagrammja
(Forrás: Saját szerkesztés)

TEVÉKENYSÉGJEGYZÉK ÉS IDŐTERVEZÉS					Július					Augusztus					Szeptember				Október				November					December				Január			
	KONCEPCIÓ	Emberi erőforrás-szükséglet	Tevé-keny-ség	Időtar-tam hét			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.	29.
1.	Menedzsment elhatározása és projektvezető megbízása	4	0-1	3																														
2.	Szakértői team-ek összeállítása, vezetői szerepek, hatáskörök kialakítása	3	1-2	3																														
3.	Információs Biztonsági Politika és Információs Biztonsági Stratégia megfogalmazása	2	1-5	4																														
4.	Szabványkövetelmények értelmezése	2	1-4	3																														
	TERVEZÉS, SZERVEZÉS																																	
5.	A jelenlegi rendszer felmérése, folyamatok feltérképezése, rendszerhatárok és alkalmazási terület kijelölése	2	3-9	3																														
6.	Kiindulási és célállapot rögzítése	3	3-7	2																														
7.	Erőforrásigény meghatározása	2	6-8	2																														
8.	Bevezetési ütemterv elkészítése	2	7-9	1																														
	MEGVALÓSÍTÁS																																	
9.	Folyamatok kialakítása és a szabványkövetelményekkel történő összhangba hozása *	5	8-13	6																														
10.	Szabályzatok hierarchikus szintjeinek kialakítása	2	8-11	2																														
11.	Rendszerdokumentáció elkészítése, illesztése a már működő irányítási rendszerekhez*	4	10-12	2																														
12.	Oktatás, képzés lebonyolítása	3	11-13	2																														
13.	Új szabályozás szerinti működés megkezdése, utána folyamatos figyelemmel kísérés, működésfelügyelet.	5	12-14	2																														
14.	Teljes körű belső audit végrehajtása	3	13-15	1																														
15.	Helyesbítések, utóellenőrzések megtétele	2	14-16	1																														
16.	Vezetőségi átvizsgálás	3	14-17	1																														
17.	Tanúsító szerv kiválasztása, szerződéskötés	2	16-18	1																														
18.	Tanúsítás megkezdése, dokumentumok átvizsgálása, helyszíni audit	5	17-19	2																														
	BEFEJEZÉS																																	
19.	Szükséges helyesbítő intézkedések elvégzése	2	18-20	3																														
20.	Tanúsítvány kiadása	0	19-20	1																														
21.	Szabvány szerinti működés megkezdése, rendszerfelügyelet	8	19-21	1																														

A projekt zárásaként, a szabályozási környezet kialakítását, a szabályozott folyamatok kialakítását, a szervezetátalakítási lépések megtételét, a kockázatkezelés elvégzését, valamint oktatás és képzések lebonyolítását követően **belső auditra és vezetőségi átvizsgálásra** került sor, amit a felkészítő céggel közösen elvégeztünk, ez mintegy **előauditként** igazolta, hogy cégünk alkalmas a tanúsítási folyamat megkezdésére. A veztőségi átvizsgálás kérdéslistáját és egy terület belső audit jegyzőkönyvét láthatjuk az alábbiakban:

A **vezetőségi átvizsgálás** során szabályozott területenként az alábbi **kérdésjegyzéket** állítottam össze (csak kivonat, a hosszú terjedelem miatt):

1. A vezetőség felelősségi köre
    a. Egyértelműen meghatározták-e ai IBIR céljait?
    b. Vannak-e tervek és folyamatok az IBIR folyamatos fejlesztésére?
    c. Támogatja-e a szervezti felépítés az IBIR céljainak megvalósítását?
    d. Elkészültek-e a módosult munkaköri leírások, melyekben meghatározták a felelősséget, hatáskört?
    e. Biztosítja-e a cég vezetése a személyi, tárgyi, pénzügyi erőforrásokat az IBIR céljainak megvalósulásához?
2. Gazdálkodás az erőforrásokkal
    a. Részesülnek-e információbiztonsági oktatásban az új belépők?
    b. Megfeleően azonosítottak-e a HR folyamtok?
    c. Tervszerűen történik-e az elamortizálódott eszközök pótlása?
3. Folyamatok ellenőrzése, mérés, és fejlesztés
    a. Van-e kidolgozott teljesítményménrése az IBIR folyamatoknak és megkezdték-e annak használatát?
    b. Van-e elfogadott listája az IT szoftver és hardver beszállítóknak és szolgáltatóknak?
    c. Van-e fejlesztési terv az IBIR egyes részeire vonatkozóan? (képzés, folyamatfejlesztés, teljesítmény)?

A következő két oldalon pedig a belső audit jegyzőkönyvét olvashatjuk.

16. Ábra: Belső audit jegyzőkönyve
(Forrás: Saját szerkesztés)

sas Safety Sector	Belső audit jegyzőkönyv BAT - 2022-1	Kiadás: 1 Módosítás: 0 Lapszám: 1 Lapok száma: 2

Készítette (név): Szabó József IBIR vezető	Jóváhagyta (név): Orbán Péter ügyvezető
Budapest, 2022.07.15.	Budapest, 2022.07.31.
Aláírás:	Aláírás

Belső audit típusa: rendszer ☐ folyamat ☒ termék ☐

Belső audit célja: Videokamerás megfigyelő rendszerekben tárolt személyes adatok kezelésének információbiztonsági és adatvédelmi célú vizsgálata

Belső audit területe: az IBIR teljes érvényességi területre, összes rendszerelem és szervezeti egység

Belső audit kritériumait tartalmazó dokumentumok: Vonatkozó jogszabályok, megbízási szerződések, végrehajtási dokumentumok, elektronikus adathordozók, Informatikai Szabályzat, Oktatási jegyzőkönyvek

1. Vezető auditor	Szabó József	Kezdési időpont:	2022.07.25.
2. Auditor	[redacted]	Befejezési időpont:	2022.07.27.

Belső audit ütemterve:

1. Vonatkozó szerződések, adatvédelmi szabályzat átvizsgálása, jogszabályok áttekintése
Helye: iroda
Ideje: 2022.07.25.
Résztvevők: auditorok

2. Munkadokumentumok készítése
Helye: iroda
Ideje: 2022.07.25.
Résztvevők: auditorok

3. Nyitó megbeszélés
Helye: iroda
Ideje: 2022.07.25.
Résztvevők: auditorok, ügyvezető, vagyonvédelmi vezető, irodavezető,

4. Helyszíni audit végrehajtása, rögzített felvételek szúrópróbaszerű (mintavételes) ellenőrzése
Helye: Titkárság, szerverszoba, tárgyaló
Ideje: 2022.07.25.-26.
Résztvevők: auditorok,

5. Értékelés elkészítése
Helye: Iroda
Ideje: 2022.07.27.
Résztvevők: auditorok,

6. Záró megbeszélés
Helye: iroda
Ideje: 2022.07.27.
Résztvevők: auditorok, ügyvezető, vagyonvédelmi vezető, irodavezető

7. Auditjelentés elkészítése
Helye: iroda
Ideje: 2022.07.27.
Résztvevők: auditorok,

8. Az intézkedések végrehajtása és ellenőrzése
Helye: Auditjelentés szerint.
Ideje: intézkedési tervek szerint
Résztvevők: auditorok, ügyvezető, vagyonvédelmi vezető, irodavezető

Ez a program helyszíni auditra vonatkozik.
Vonatkozó szabvány / Támogató dokumentáció: ISO 27001:2014, MSZ EN ISO 9001:2015

Név/ Szerep	Vezető Auditor, Auditor	Név/ Szerep	Vezető Auditor, Auditor
Dátum	2022.07.25.	Dátum	2022.07.25.
Időpont	Helyszín/Szervezeti egység/Beosztás	Időpont	Helyszín/Szervezeti egység/Beosztás
09:00	Nyitó értekezlet		
09:30	**Videokamerás megfigyelő rendszerekben tárolt személyes adatok kezelésének információbiztonsági és adatvédelmi célú vizsgálata** Az IT szervezet és környezetének megértése; Az érdekelt felek igényeinek és elvárásainak megértése; Az IBIR alkalmazási területének meghatározása; Az IBIR és folyamatai	13:00	**A kockázatelemzés során az intézkedéseket igénylő elemek azonosítása, az ellenintézkedések megtörténtének utólagos kontrollja:** Erőforrások, Felkészültség (kompetencia), Tudatosság, Kommunikáció, Dokumentált információ
10:30	**A kockázatelemzés során az intézkedéseket igénylő elemek azonosítása, az ellenintézkedések megtörténtének utólagos kontrollja:**	14:00	**8: Működés – interjú az üzletágvezetőkkel és a szakmai vezetővel** **Információbiztonsági incidensek kezelése, észlelt események**
11:00		15:00	**9: Teljesítményértékelés - interjú az ügyvezetőkkel, üzletágvezetőkkel** Figyelemmel kísérés, mérés, elemzés és értékelés; **10: Fejlesztés - interjú az ügyvezetőkkel, üzletágvezetőkkel** Általános követelmények; Nem-megfelelőség és helyesbítő tevékenység; Folyamatos fejlesztés
12:30	Szünet	16:00	
		16:30	Napi Záró értekezlet
Kitöltötte:	Szabó József	**Az időbeosztás és a tartalom változhat.**	

Az audit céljai;

- Megerősítse, hogy az irányítási rendszert létrehozták, bevezették és fenntartják az audit szabvány követelményeinek megfelelően.
- Kiértékelje az irányítási rendszer képességét, amely biztosítja, hogy ügyfél szervezete megfelel az alkalmazható törvényi, jogszabályi, és szerződésben foglalt követelményeknek. Megjegyzés: Egy irányítási rendszer tanúsító auditja nem egy jogi megfelelőségi audit.
- Kiértékelje az irányítási rendszer hatékonyságát, amely biztosítja, hogy folyamatosan eleget tegyen a konkrét célkitűzéseknek
- Beazonosítsa az irányítási rendszer területeire vonatkozó lehetséges fejlesztéseket

Az audit alkalmazási területe leírja az audit mértékét és határait, mint pl. a fizikai helyszínek, szervezeti egységek, tevékenységek és folyamatok auditálása. Ahol a kezdeti vagy a megújító folyamat több mint egy auditból áll (pl.: különböző helyeken), a különálló audit alkalmazási területe nem terjedhet ki az egész tanúsítás alkalmazási területére, de az audit egészének összhangban kell állnia az alkalmazási területtel, ami a tanúsítói dokumentumban szerepel.

4.2.2. Az IBIR bevezetési projektjének pénzügyi tervezése és elszámolása

Cégünk, felmérve annak a jelentőségét, hogy egy IBIR bevezetésének és fenntartásának, valamint a szabványkövetelményeknek megfelelő működési többletköltségnek a nagysága nagyságrendekkel kisebb, mint egy információbiztonsági incidens által előídett kár lehetséges mértéke, valamint a közbeszerzéseink jelentős részén a kiíró szervezet műszaki követelményként határozza meg az IBIR tanúsításának igazolását, ezért az anyagi forrásaokat a cég messzemenőleg biztosította a beveeztési projekt végrehajtásához, majd a további működéshez.

A projekt költségtervezése során a **tanácsadó, felkészítő szervezet díjazása** mellett, egy belső kalkulációs metódus szerint a saját munkatársaink projket munkavégzésre fordított munakidejéből származó **személyi jellegű ráfordítások**, továbbá a szabvány szerinti működés megkezdésének elengedhetetlenül szükséges **tárgyi eszközök beszerzési költségével** is kalkuláltam. A projekt pénzügyi adatait E Ft-ban megadva az alábbi táblázatban láthatjuk:

22. Táblázat: Projekt költségvetése
(Forrás: Saját szerkesztés)

Időszakok	Közvetlen bérköltség és bérjárulékok	Általános költségek	Technikai eszközök beszerzési költségei	Felkészítő és auditor cég költségei
Előkészítő szak	2.900.000	200.000	0	100.000
Tervezés, szervezés	1.500.000	150.000	0	250.000
Megvalósítás	7.320.000	350.000	3.500.000	2.800.000
Zárás, befejezés	600.000	150.000		
Működés megkezdése	800.000	0		30.000
Összesen:	**13.120.000**	**850.000**	**3.500.000**	**3.180.000**
MINDÖSSZESEN:	**20.650.000**			

A projekt előrehaladtával a költségeket figyelve megállapítottam, hogy sem a cash-flow tervben, sem az eredményszemléletű kimutatásokban nem mutatkozott jelentős eltérés a tervezéshez képest, tehát a költségek becsült nagysága közelítette a valóságot.

Mindazonáltal, mivel egy közel nettó 21 MFt-os költség a cég tárgyévi adózott eredményére már jelentős hatással van, ezért **élve a Számviteli Törvény adta lehetőséggel**, melynek során a minőségbiztosítás bevezetésének, mint **Immateriáliks javak/alapítás-átszervezési költségeknek** az eszközként való aktiválásával a költségek egy 3 éves amortizációs ciklussal szétteríthetőek, ezért a főkönyvi nyilvántartásokban az alábbi módon került a projekt gazdasági eseményeinek rögzítése és elszámolása a megfelelő főkönyvi számlaszámokon: (összehasonlításképpen bemutatom, az „B" normál verziót, tehát, ha nem aktiváljuk a költségeket, ebből látható, hogy mennyivel kisebb negatív eredmény hatást gyakorol a második, „A" változat:

23. Táblázat: Bevezetési projekt költségeinek számviteli elszámolása
(Forrás: Saját szerkesztés)

B verzió						
Ssz	**Gazdasági esemény**	**Számlaszám**		**Összeg**		**Eredményhatás**
		Tartozik	**Követel**	**Tartozik**	**Követel**	
1/1	Személyi jellegű ráf.	54-56	46-47	13 120 000	13 120 000	-13 120 000
2/1	Általános költségek	51-52	454	850 000	850 000	-850 000
2/2	Áfa	466	454	229 500	229 500	0
3/1	Technikai eszköz beszerzése	161	454	3 500 000	3 500 000	0
3/2	Áfa	466	454	945 000	945 000	0
3/3	Aktiválás-irodai berendezés	143	161	3 500 000	3 500 000	0
4/1	Tanácsadási díj	52	454	3 180 000	3 180 000	-3 180 000
4/2	Áfa	466	454	858 600	858 600	0
5	Irodai berendezés ÉCS-(0,5/5 év)	571	149	350 000	350 000	-350 000
EREDMÉNYHATÁS						**-17 500 000**

A verzió						
Ssz	**Gazdasági esemény**	**Számlaszám**		**Összeg**		**Eredményhatás**
		Tartozik	**Követel**	**Tartozik**	**Követel**	
1/1	Személyi jellegű ráf.	54-56	46-47	13 120 000	13 120 000	-13 120 000
1/2	Alapítás átszervezés, költségek aktiválása	111	582	13 120 000	13 120 000	13 120 000
2/1	Általános költségek	111	454	850 000	850 000	0
2/2	Áfa	466	454	229 500	229 500	0
3/1	Technikai eszköz beszerzése	161	454	3 500 000	3 500 000	0
3/2	Áfa	466	454	945 000	945 000	0
3/3	Aktiválás-irodai berendezés	143	161	3 500 000	3 500 000	0
4/1	Tanácsadási díj	111	454	3 180 000	3 180 000	0
4/2	Áfa	466	454	858 600	858 600	0
5	Immateriális javak ÉCS (0,5/3 év)	571	1 191	2 858 333	2 858 333	-2 858 333
6	Irodai berendezés ÉCS-(0,5/5 év)	571	149	350 000	350 000	-350 000
EREDMÉNYHATÁS						**-3 208 333**

Az IBIR bevezetés folyamata eredményesen zárult, szervezetünk csupán néhány **enyhe nemmegfelelőséget** kapott a tanúsító audit során, és több mint fél éves felkészülés után sikeres auditot zárt le, aminek az eredménye az akkreditált szervezet részéről kiállított auditigazolás és tanúsítvány lett.

17. Ábra: A sikeres tanúsító audit igazolása
(Forrás: EMT Zrt. 2020)

EMT Zrt.

TANÚSÍTVÁNY

Tanúsítjuk, hogy a

Safety Sector Biztonsági Tanácsadó és Szolgáltató Kft.

1062 Budapest, Andrássy út 125.

információ biztonsági irányítási rendszere megfelel az

MSZ ISO/IEC 27001:2014

(Információ biztonsági irányítási rendszerek követelményei)

szabvány követelményeinek, a következő alkalmazási területeken:

Üzleti információszerzés, magánnyomozás, személy- és vagyonvédelem, biztonságtechnikai rendszer tervezése és telepítése, haditechnikai termékekkel kapcsolatos szolgáltatások nyújtása, ingatlan üzemeltetés, takarítás, épülettakarítás

Összhangban a Safety Sector Kft. Alkalmazhatósági Nyilatkozatával, verziószám 3,

A tanúsítvány száma: 100-0893
Dátum:
Újra kiadás:
Érvényes: 2020.09.01.
EA kód: 28/32/34/35

Budaörs,

Bujtás Gyula
vezérigazgató

5. IBIR és GDPR kapcsolata

A „GDPR”az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)-e, valamint az Információbiztonsági Irányítási Rendszer nemzetközi szabványának az ISO/IEC 27001:2023 szabvány, Információbiztonság, kiberbiztonság és a magánélet védelme - Információbiztonság-irányítási rendszerek idei változásának iránya is jelzi, hogy a **két szabályozó környezet bizonyos értelemben vett közeledése figyelhető meg**, legalábbis ami a személyes adatok védelmére vonatkozó kritériumokat tartalmazza. Olyannyira igaz ez, hogy az ISO, 2019-ben hatályba léptette **a saját, személyes adatok védeleméről szóló szabványát**, az **ISO/IEC-27701:2019-et (Privacy Information Management Systems (PIMS)** Fontos különbség, hogy míg a GDPR egy kötelező EU-s rendelet, ami valamennyi Uniós, vagy az Unió területén szolgáltatást nyújtó jogalanyra nézve kötelező, ráadásul be nem tartása nagyon komoly büntető szankciókat vonhat maga után, addig az ISO, mint szabvány szabadon választható.

Mégis, megvizsgálva a két előírásrendszer tartalmi elemeit, az előírások rendelkező céljait, egymás értelmező rendelkezéseit és szakszótárát, egyértelmű, hogy a 27.000-es ISO nagymértékben segítheti a cégeknek a GDPR megfelelőségek szervezeti szintű garanciális feltételeinek biztosítását. Kicsit leegyszerűsítve, ha a neki akarunk kezdeni a két rendszer összehasonlításának azt mondhatjuk, hogy **minden adatvédelmi incidens egyben információbiztonsági incidens is, de nem minden információbiztonsági incidens válik adatvédelmi incidenssé**. Ebből kiindulva láthatjuk a rész-egész halmaz egymáshoz való viszonyát, vagyis azt, hogy a két szabályozó eljárás az adathalmaz mely körét veszi célpontba és védelme alá. Rengeteg párhuzam figyelhető meg az IBIR információbiztonsági kontrolljai és a GDPR adatvédelmi kontrolljai között, mégis a párhuzamosságok és az eltérő célrendszer miatt, sajnálatos módon a cégek kénytelenek két párhuzamos védelmi rendszert működtetni, már ami az adminisztratív oldalt és néhány folyamatot illet. A GDPR-ban olyan kötelező folyamatokkal, szereplőkkel, előírásokkal találkozunk, melyeket egy az egyben megfeleltetni az IBIR-ben nem lehet. IT vezetőként akarhatnék én ugyan olyan biztonsági mentési stratégiát kialakítani, hogy a hosszú évek alatt felhalmozott adatok teljes köre a birtokunkban maradjon, abból adatbázist, igazi vállalati adatvagyont hozzunk létre, ha az

Adatvédelmi Törvény ezt egyszerűen nem teszi lehetővé. Egy gyakorlati példa a vagyon elleni bűncselekményeket elkövető személyekről készült kép, video és hangfelvételek köre, szerethetném én ugyan tudni 10 év múlva is, hogy az adott áruházba éppen belépő személy már lopott a kereskedelemi egységből, de mind az Infó törvény, mind a Vagyonvédelmi Törvény tiltja a személyes adatok ilyen célból, korlátlan ideig történő megőrzését, videós adatbázist pedig egyáltalán nem hozhatunk létre az elkövetőkről. Csak néhány példa a GDPR fogalmi rendszeréből:

- Hazai hatósága és jogszabálya: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Info Tv) és a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH),
- adtakezelés, adatfeldolgozás, célhoz kötöttség, profilalkotás,
- az adatkezelés alá vont érintetti jogok, hozzáférés, helyesbítés, törléshez való jog, a tiltakozáshoz való jog, jogorvoslati jogok,
- adatvédelmi tisztviselő, adatbiztonsági incidens,
- adatvédelmi nyilvántartás, adatkezelési nyilvántartás,
- adatvédelmi bírság.

Jellemző a GDPR rendelet által előírt követelmények adminisztrációs terheire, hogy csak az Adatvédelmi Szabályzatunk 50 oldal!, valamint az egymásnak ellentmondó jogi értelmezéseknek, hogy bevezetése után mind a cégek, mind a magánszemélyek -gondoljunk a netes böngészés során folyamatosan felbukkanó és rettenetesen idegesítő adatkezelési hozzájárulási nyilatkozatokra-, nagy része felesleges nyűgnek érzi az egész adatvédelmi kérdés ilyetén módon történő kezelését. Véleményem szerint az Unió jogalkotói ebben a kérdésben, bár a szándékuk nemes volt, gyakorlatilag lábon lőtték magukat. Nekünk, átlag felhasználóknak csak feleslegesen megkeseríti az életünket, az IT mamutok pedig (Google, Apple, Microsoft, Amazon, Facebook) továbbra is újabb és újabb technikai megoldássokkal lopják el digitális profilunkat, hogy aztán hirdetéskiszolgálókon keresztül nagyon pontos és személyre szabott ajánlatokkal találjon el bennünket például az ecipo.hu, miután rákerestünk egy jó minőségű téli bakancsra.

6. Következtetések, javaslatok

Cégünk tevékenységének alapelve a lehető legmagasabb szintű kiszolgálása üzleti és hatósági ügyfeleinknek, amely szolgáltatást folyamatosan, a nap 24 órájában végezzük. Az alapvető tevékenységi körünk, valamint kiegészítő szolgáltatásaink meghatározzák azt, hogy szervezetünknél az adatok és információk érzékeny, szenzitív köre, valamint személyes és különleges személyes adatok kezelése történik, ez pedig a legfontosabb vagyonelemeink egyike. Üzleti tevékenységünket az IBIR bevezetését követően immár magas szintű, támogató információs menedzsment eljárásokkal valósítjuk meg, amely eljárások összessége az értékteremtés folyamatát szervezési és technikai eszközökkel oldja meg.

Az IBIR bevezetését követően maradéktalanul képesek vagyunk a társaság informatikai környezetének zavartalan és folyamatos működésének biztosítására, az adatvédelem és adatbiztonság szabályozására, továbbá az adatok hitelességének, integritásának, sértetlenségének és rendelkezésre állásának szavatolására. A folyamatos oktatási és képzési követelmények teljesítésével munkatársaink kellő információbiztonsági tudatossággal, megfelelő felhasználói készségekkel rendelkeznek az informatikai és ügyviteli eszközök szakszerű kezeléséhez. Az IT eszközök beszerzése a korábbi ac-hoc jelleg után tervszerűen, a fenyegetési és sebezhetőségi faktorok folyamatos nyomonkövetésével történik, a rendelkezésre álló anyagi eszközöket pedig képesek vagyunk a legoptimálisabb módon felhasználni. Társaságunk kiemelkedően nagy jogi, pénzügyi és technikai kockázatot képes kezelni a bevezetett információbiztonsági és adatvédelmi incidenskezelési eljárásaival, az IBIR pedig nagymértékben hozzájárul ezeknek a folyamtoknak a jogi megfelelőségének a biztosításához. Természetesen az IBIR bevezetést követően nem ért véget az információbiztonsági tevékenységünk fejlesztése, a PDCA logika és az évenkénti felülvizsgálati auditok adminisztratív követelményeinek teljesítése, de leginkább az újabb fenyegetési módszerek, eljárások megjelenése folyamatos fejlesztést kíván tőlünk.

Ennek jelei máris megjelentek az információbiztonság területén, a rendszerek helyett a munkavállalókat célzó megszemélyesítési elven működő hacker tevékenység megerősödése, egyes telepített technikai eszközökben, hardverekben megbúvó és a nemzetközi közösség által felfedezett, egyelőre technikailag nem orvosolható támadási módszerek adott esetben az eszközök azonnali cseréjét teszik szükségessé.

Javaslom tehát az oktatási terv módosítását, valamint néhány informatikai eszköz cseréjét, továbbá azoknak a mutatóknak a naprakész figyelését, amelyek a rendellenes hálózati tevékenységet, adatszivárgást, jeleznek. Szükségesnek tartom tovább a biztonsági mentési stratégia felülvizsgálatát, ugyanis a zsaroló vírusok fenyegetési szintje olyan mértékben megnőtt, ami azonnali intézkedést kíván.

Állandó cica-macska harc ez, sajnos a számítástechnikai bűnözők mindig előttünk járnak, de határozott véleményem, hogy az IBIR bevezetését követően a működési kockázatokat az információbiztonság területén sikerült olyan mértékben csökkentenünk, ami egy adott, felelős menedzsmenttel rendelkező szervezettől elvárható.

7. Összefoglalás

Dolgozatom elkészítése során egy IBIR rendszer bevezetési projektfolyamatát mutattam be jelenlegi a munkahelyemen, kiemelve azt, hogy a vállalati adatvagyon hatékony menedzselését és védelmét nem tartom megvalósíthatónak megfelelő minőségbiztosítási, információbiztonsági és vállalatirányítási rendszer működtetése nélkül. Célkitűzéseimnek megfelelően dolgozatom elméleti, hazai és nemzetközi szakirodalmat feldolgozó részében összekötöttem ezeket a fogalmakat, bemutattam a minőségügyi rendszerek fejlődéstörténetét, napjaink minőségmenedzsmentjében alkalmazott minőségtechnikákat, módszertanokat, valamint mintegy tisztelegve előttük, a kifejlesztő szakembereket, gurukat. A komplex vállalatirányítási rendszerek után, harmadik elemként az információbiztonsági szabványcsalád, ajánlások, nemzetközi sztenderdek ismertetését végeztem el, megmutatva azt, hogy ezek a módszertanok milyen módon kapcsolódnak egymáshoz, miben különböznek egymástól, illetve, hogy a szerveztek, figyelembe véve saját igényeiket, szabadon választhatnak ezek közül.

Az IBIR bevezetési projektfolyamat végrehajtása során:

- elvégeztem a vállalkozás információbiztonsági helyzetének komplex felmérését,
- elkészítettem a vagyonleltárt, a védendő eszközök, információk, folyamatok körét tartalmazó nyilvántartást,
- elemeztem a szervezetet kockázati elemeit, azok által okozott sérülékenységeket, valamint fenyegetéseket, ezek alapján megterveztem a lehetséges ellenintézkedéseket, melyeket kockázatkezelési tervbe foglaltam,
- kialakítottam és módosítottam a szervezeti struktúrát, ami megfelelő hatáskörrel ruházza fel az információbiztonság szervezetét,
- elkészítettem az adminisztratív védelem dokumentumait
- a fizikai védelem részét képező biztonságtechnikai fejlesztéseket hajtottam végre,
- szabályozó folyamatokat hoztam létre a humánerőforráshoz kapcsolódó kockázatok kezeléséhez, az oktatáshoz és képzésekhez,
- létrehoztam az IBIR rendszer teljesítményméréséhez és fejlesztéséhez szükséges mutatószámok rendszerét,
- meghatároztam a bevezetési projekt elemi tevékenységeinek logikai sorrendjét, majd Gantt diagram segítségével időtervezést végeztem, továbbá pénzügyi tervezést is végrehajtottam a szükséges erőforrások meghatározása érdekében.

- néhány gondolatban vázoltam az IBIR és a GDPR lehetséges kapcsolódási pontjait, a követelményrendszereiket.

Mind a dolgozatom által megfogalmazott célkitűzéseim megvalósulását, mind konkrétan a bevezetési folyamatot sikeresnek tartom, szervezetünk az információvédelem követelményeinek szempontjából biztonságosabban és hatékonyabban működik.

8. Summary

During the preparation of my thesis, I presented an introduction to an IBIR (Information, Quality, and Risk Management) system implementation project process currently being undertaken at my workplace. I emphasized that the efficient management and protection of corporate data assets are not achievable without the operation of adequate quality assurance, information security, and corporate governance systems. In accordance with my objectives, in the theoretical section of my thesis, I connected these concepts, explored the history of quality management systems, and showcased the quality techniques and methodologies applied in today's quality management. Additionally, I paid tribute to the pioneering experts and gurus in this field. Following the discussion of complex corporate governance systems, as a third element, I provided an overview of the information security standard family, recommendations, and international standards, demonstrating how these methodologies are interconnected, what sets them apart from one another, and how organizations, considering their specific needs, can freely choose among them. During the execution of the IBIR implementation project process:

- I completed a complex assessment of the company's information security situation,
- I prepared an inventory, maintaining a record of the assets to be protected, including information, processes, and resources.
- I analyzed the organization's risk factors, vulnerabilities caused by them, and threats they pose. Based on this, I designed possible countermeasures, which were documented in a risk management plan.
- I created and modified the organizational structure, which empowered the information security organization.
- I generated the administrative protection documents.
- I implemented security enhancements encompassing physical protection measures.
- I created regulatory processes for the management of risks related to human resources, education and training.
- I created a system of performance metrics for the IBIR system and its continuous improvement.
- I determined the logical sequence of elementary activities for the implementation project, performed time scheduling using Gantt charts, and executed financial planning to identify the required resources.

- In a few words, I outlined possible points of connection between IBIR and GDPR, including their respective requirements.

I consider both the achievement of the objectives formulated in my thesis and the implementation process itself to be successful. Our organization operates more securely and efficiently in terms of information protection requirements.

9. Irodalomjegyzék

[1] Alan C., Steve W. (2019): *It Governance: An International Guide to Data Security and ISO 27001/ISO 27002*. USA, Kogan Page

[2] Bartos I, Elek E (2010): *Minőségirányítás*. Budapest: Óbudai Egyetem

[3] Capterra (2023): https://www.capterra.com/enterprise-resource-planning-software/), Arlington, Letöltés ideje: 2023. 11. 03.

[4] Claude E. S., Warren W. (1986): *A kommunikáció matematikai elmélete, Az információelmélet születése és távlatai*. Budapest: Országos Műszaki Információs Központ és Könyvtár

[5] Committee of Sponsoring Organizations: *COSO ERM 2017- Enterprise Risk Management:* USA: COSO

[6] Daróczi M. (2011): *Projektmenedzsment, Oktatási segédlet*, Gödöllő: Szent István Egyetem

[7] Decipher Zone Technologies Pvt. Ltd. (2023): *Top 10 Frameworks for Web Application Development, https://www.decipherzone.com/blog-detail/top-web-frameworks :* India. Letöltés ideje: 2023.10.31.

[8] Dévai Z., Fésüs N., Kosztolányi J., Kővári R., Nika T. (2020): *Lean szolgáltatásfejlesztés 1-2.*, Budapest: Kaizen Pro Kft.

[9] Drégelyi-K., Farkas G., Galla J., Tóth G., (2013): *Minőségbiztosítás*. Budapest: Óbudai Egyetem

[10] ElevatiIQ (2023): *Top 10 ERP Vendors For 2023*. https://www.elevatiq.com/post/top-10-erp-vendors/ USA, Letöltés ideje: 2023.10.31.

[11] Enyedi M. (1997): *Bevezetés a döntéselméletbe*. Budapest: Ligatura kiadó

[12] Fehér N. (2018): *A Lean six sigma folyamatfejlesztés kézikönyve*, Zalaegerszeg: Cash Flow Navigátor Tanácsadó Kft.

[13] Fehér O. (2023): http://feherotto.hu/modszerek.html Budapest, Letöltés ideje: 2023.09.28.

[14] Georg W.F.H. (1957): *A Logika Tudománya*. Budapest: Akadémiai Kiadó

[15] Horváth Zs, Horváth I. (2023): A megújult ISO/IEC 27001 információbiztonsági szabványra való átállás követelményei. *Magyar Minőség.* 2023. február, pp. 4-15.

[16] Husti I. (2020): *Műszaki termelésmenedzsment*, Gödöllő, Szent István Egyetem

[17] Index Portál (2023): Wolkswagen-csoport üzemeinek leállása, Budapest, Letöltés ideje: 2023.09.28.

[18] Kaoru I. (1991): *What Is Total Quality Control? The Japanese Way*. Japan: PublisherPrentice Hall Direct

[19] Koczor Z. (2010): *Minőségirányítási rendszerek fejlesztése*. Budapest: TÜV Reinland Akadémia

[20] Komenczi B. (2011): *Információelmélet*. Eger: Eszterházy Károly Főiskola

[21] Kovács I. (2011): *Integrált vállalatirányítási rendszerek*. Gödöllő: Szent István Egyetem

[22] Kövesi J., Topár J. (2006): *A minőségmenedzsment alapjai*. Budapest: Typotex Kiadó

[23] Leanforum (2015) : 7 lépéses problémamegoldás: https://www.leanforum.hu/index.php/szocikkek/148-7-lepeses-problemamegoldas , Budapest, Letöltés ideje: 2023.10.31.

[23] Magyar Szabványügyi Testület (2015): *Minőségirányítási rendszerek*. *Követelmények (ISO 9001:2015).* Budapest*,* Magyar Szabványügyi Testület

[24] Medina V. (2019): *Minőségmenedzsment oktatási segédlet*, Gödöllő, Szent István Egyetem

[25] Mesics Z. (2019): Biztonsági irányítási rendszerek fejlesztése, biztonsági teljesítmény mérés. *Védelem Tudomány – IV. évfolyam, Iparbiztonság különszám, 2019. 2. hó, pp.* 174-190.

[26] Michelberger P. (2017): *Gazdasági Informatika*. Budapest: Óbudai Egyetem

[27] Muha L., Krasznay Cs. (2014): *Az elektronikus információs rendszerek biztonságának* menedzselése. Budapest: Nemzeti Közszolgálati Egyetem

[28] Nemzetközi Szabványügyi Testület (2023): *Standards catalogue:* https://www.iso.org/standards-catalogue/browse-by-ics.html , Svájc. Letöltés ideje: 2023.10.31.

[29] Szádeczky T. (2014): *Információbiztonsági szabványok*. Budapest: Nemzeti Közszolgálati Egyetem

[30] Székely T. (2022): *Agilis, waterfall, vagy hibrid megoldást válassz céged szoftverfejlesztési projektjéhez*? https://www.allwin.hu/post/a-vallalati-digitalizacio-dilemmai-agilis-waterfall-vagy-hibrid-szoftverfejlesztes. Budapest, Letöltés ideje: 2023.10.31.

[31] The Center for Internet Security, Inc. (CIS®) (2023): *CIS Controls.* USA*:* Center for Internet Security, Inc.®)

[32] Turban, E., McLean, E. Wetherbe, J. (2002*): Information Technology for Management* 3rd edition. Usa, John Wiley & Sons

[33] Turcsányi K. (2014): *Minőségelmélet és módszertan*. Budapest: Nemzeti Közszolgálati Egyetem

[34] Visure Solutions (2023): *CMMI vs SPICE*: https://visuresolutions.com/hu/cmmi-guide/cmmi-vs-spice/ San Francisco. Letöltés ideje: 2023.10.31.

[35] XAPT Hungary Kft (2023): *A Magyarországon elérhető legnépszerűbb ERP rendszerek listája: https://www.minuszos.hu/wp-content/uploads/doc/a-25-legnepszerubb-erp-rendszer.pdf* Budapest, Letöltés ideje: 2023.10.31.

10. Táblázatok és ábrák jegyzéke

11. Mellékletek

11.1. Japán eredetű minőségmenedzsment technikák

Minőségmenedzsment technika megnevezése	A technika rövid leírása
JIDOKA	lényege, a gépek és berendezések felszerelése olyan automatizmussal, ami megakadályozza a selejtgyártást, hiba észlelése esetén a gépsor azonnal megáll
3MU-5MU	a Muda, Muri, Mura szavak pazarlás, túlterhelés és egyenetlenség megfelelői, a veszélyek és problémaforrások feltárására használatos, kiegészítve a Mushi és a Muchi szavakkal, a tudatlansággal és a szakképzetlenséggel, az 5MU módszert kapjuk.
HEIJUNKA	célja az egyenletes termelés biztosítása, a termelés programozásához használatos módszertan
KANBAN	a jel és a kártya japán szavakból képzett mozaikszó, lényege, hogy az áruk áramlása és feltöltése, a készletek figyelése Kanban kártyákkal, nagyon egyszerű módszerrel megoldható
SMED	A Single Minute Exchange of Die angol szóból képezték, a termelés gépeinek szerszámcseréjéhez szükséges időzítéseket és ütemezéseket lehet a termelés hatékonyságának növelése érdekében szabályozni
KAIKAKU	ez a villámgyors Kaizen megfelelője, koncentrált, rövid idejű beavatkozást ír elő, gyors eredményekkel párosítva
20 KULCS	Iwao Kobayashi könyve alapján lett ismert, ami a munkahely fejlesztésének húsz pontjaira épülve segíti a munkahelyi kultúra javítását
7 MUDA	a hét veszteségforrást veszi célpontba a túltermelés, várakozás, szállítás, gyártás, készletezés, felesleges mozdulatok selejt szabályozásával

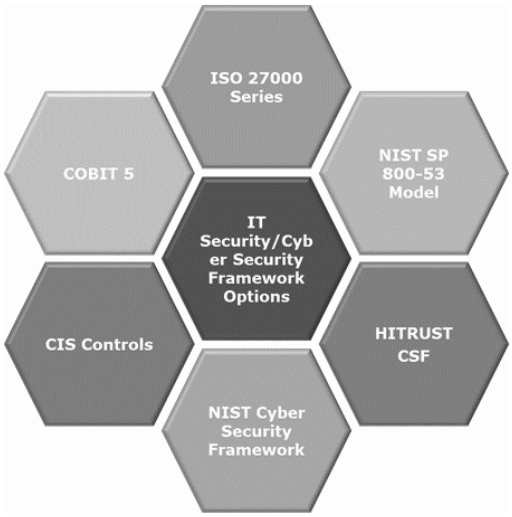
11.2. ERP-t használó hazai cégek 2022-es iparági megoszlásának táblázata

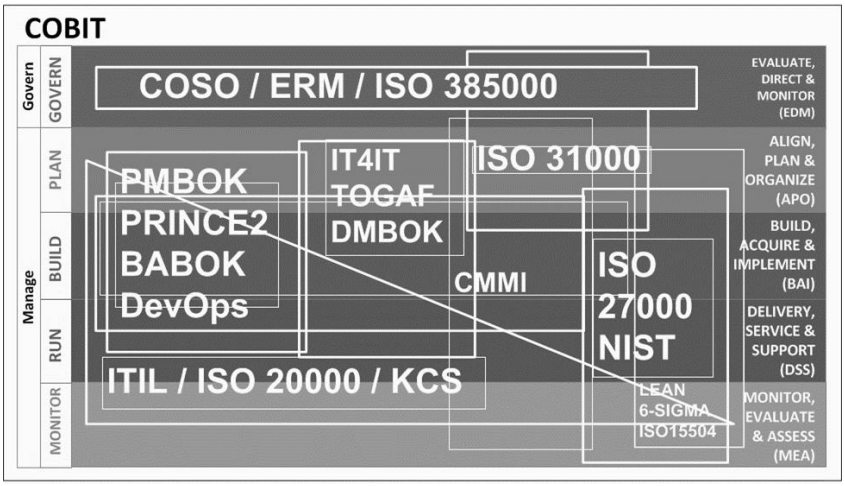
(Forrás: XAPT Hungary Kft)

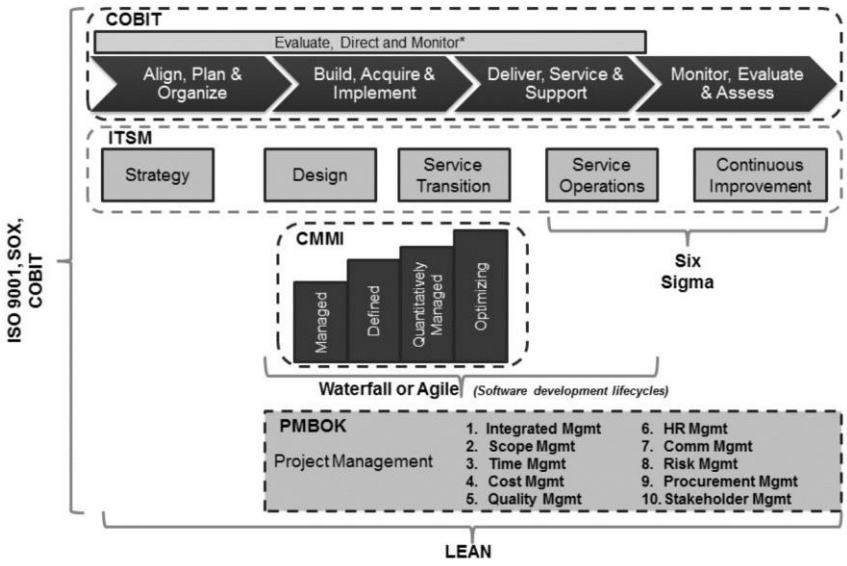
ERP rendszer	Tipikus iparágak	
abas	Ipari berendezések gyártása Gyümölcs és zöldség nagykereskedelem Gépgyártás	Gyógyászati eszközök kereskedelme Fémmegmunkálás és feldolgozás
Cobra	Bútorgyártás Építőipar Kiadványterjesztés	Közigazgatás Munkagép kereskedelem Szépségipar
Coda (Unit4)	Logisztika Üzleti szolgáltatások Disztribúció és nagykereskedelem	Pénzügyi szolgáltatások Gyártás Média- és kiadóvállalatok Kiskereskedelem
exPanda	Gumiabroncs kereskedelem Vegyipar Irodatechnika	Autóipar Nagy- és kiskereskedelem Közigazgatás
Infosys	Járműipar Kohászat Bányászat	Építőipar Média Telekommunikáció
Epicor	Gyártástervezés Disztribúció Kiskereskedelem és vendéglátás	Szolgáltatások
GriffSoft Forrás	Közigazgatás Mezőgazdaság	
proALPHA	Fémmegmunkálás és -feldolgozás Szolgáltatások Elektrotechnika	Orvostechnika Műszaki nagykereskedelem Műanyagfeldolgozás

11.3. példa a szabványok, keretrendszerek és ajánlások egymásba épülésére a nemzetközi szakirodalom alapján

(Forrás: https://cyberrisk-countermeasures.info/cyber-security-control-frameworks/)







11.4. Az információbiztonsági mutatószámok rendszere, csoportosítva

Felkészültségi szintet jelző mutatók	az egy év alatt észlelt és megoldott biztonsági incidensek száma, vagy a proaktív biztonsági intézkedések, a végpontvédelem, a behatolásészlelő rendszerek miatt megakadályozott incidensek százalékos aránya, esetleg az alkalmazottak biztonsági tudatosságának szintje és a kiberbiztonsági tudatosságot növelő képzési programok gyakorisága
Rendszerbe érkezett kártékony email-ek aránya	Az összes beérkezett email és a felhasználói postafiókokba beérkezett levelek aránya
Szolgáltatás rendelkezésre állási mutatók	internet, belső hálózat rendeltetés szerinti működési óráinak és az összes órák hányadosa
Azonosítatlan eszközök száma	a belső hálózaton: IoT eszközök és a munkavállalók saját eszközeinek használatára vonatkozó szabályok megsértésének aránya, vagy a hálózatra csatlakozott eszközök és az érzékeny adatot hordozó eszközök aránya
Behatolási kísérletek és biztonsági incidensek száma	behatolási kísérlet észlelése és a reagálás között eltelt idő aránya, vagy hány jogosulatlan hozzáférési kísérletet észlelt a tűzfal, esetleg mekkora a biztonsági incidenshez kapcsolódó átlagos költség, beleértve az incidensek kezelésének, a helyreállításnak és a hírnév károsodásának költségeit és milyen típusú incidensek okozták a kárt
Átlagos észlelési idő	a fenyegetésreagálási időre vonatkozóan ad statisztikai adatot, több körülményt is figyelembe kell venni előállítása során, például mi a biztonsági fenyegetések és incidensek észlelésének és reagálásának folyamata, és hogyan tesztelik és érvényesítik ezt a folyamatot
Átlagos megoldási idő	Mi a folyamata a rendszerek és adatok visszaállítására egy biztonsági incidenst követően, és hogyan érvényesül ennek a folyamatnak a hatékonysága? Mennyi a rendszer átlagos újraindulási ideje
Beszállítók biztonsági kockázatelemzése alapján a magas kockázatúak aránya	magas kockázatú beszállítók és az összes beszállító aránya
Kiadott szoftverfrissítések átlagos telepítési ideje	az Update-k kiadásának és valamennyi eszközre történő feltelepítésének időkülönbségének átlaga egy év alatt

11.5. Az információs vagyonelemek azonosítása a helyzetfelmérés során

Vagyonelem	Tulajdonos	Fenyegetések	Sérülékenységek	Hatások	Helyzetfelmérés során feltárt ellenintézkedések
Bizalmas információk	Létrehozó, dokumentum/irat felelős	Bizalmas információk kiadása indokolatlan, túlzott jogosultságok, bentragadt jogosultságok jogosulatlan hozzáférés információkhoz, bizalmas információk kompromittálása	titoktartási megállapodás hiánya, nem megfelelő felek/szintek kötött megállapodás, hiányos megállapodás a jogosultságkezelési rendszer ellenőrzésének hiánya hibásan, hiányosan szabályozott és kezelt megosztott erőforrások	adatok kiszivárgása, károkozás ügyfélnek bizalmasság elvesztése, adatok elvesztése, adatok kiszivárgása, rosszindulatú támadások, szabotázs adatok kiszivárgása, visszaélés személyes adatokkal,	Titoktartási megállapodások, beszállítói szerződések, klauzulák, dokumentumkezelés Felhasználói hozzáférési jogosultságok átvizsgálása Információ hozzáférés korlátozása
Desktop alkalmazások	Alkalmazás felhasználója	adatvédelmi szabályok megsértése, hátrányos jogi következmények Nem optimális szoftver és hardver konfigurációk Nem optimális szoftver és hardver konfigurációk, BIOS UEFI beállítások módosítása	személyes adatok szabálytalan vagy hanyag kezelése adathalászat, vírusfertőzés, ransomeware vírusok hardver meghibásodása, vírusfertőzés	hátrányos jogi következmények vírusok behatolása, adatvesztés, szolgáltatások leállása vírusok behatolása, adatvesztés, szolgáltatások leállása	Adatvédelem és a személyes adatok titkossága Informatikai, installációs feladatok, Informatikai, installációs feladatok,
Elektronikus dokumentumok, adatok	Létrehozó	Bizalmas információk nem megfelelő kezelése adatok kiszivárgása, bizalmasság sérülése	a dokumentumok, dokumentum tárak bizalmasságának hiányos vagy téves megjelölése információk hibás-, hanyag kezelése, szabálytalan levelezés, faxolás, file küldés, nyomtatás	adatok kiszivárgása, károkozás ügyfélnek, hátrányos jogi következmények adatvesztés, adatok kiszivárgása	Az Információk jelölése és kezelése Információkezelési eljárások (IT szabályzat)
Elektronikus levelezési rendszer	Létrehozó	e-mail rendszer szabálytalan használata elavult szoftver, tárhelykezelési problémák, vírusfertőzés lehetősége	az email használat szabályozására és annak ismeretének, ellenőrzésének hiánya rendszerleállás, szolgáltatások leállása	adatok kiszivárgása, vírusok behatolása, rendszer túlterhelése, levéltitok megsértése, hátrányos jogi következmények adatok kiszivárgása, vírusok behatolása, rendszer túlterhelése, rendszerleállás	Elektronikus üzenetek kezelésének szabályozása, titkosítás Új szoftver telepítése, ideiglenesen szerver és kliens oldali feladatok (töredezettség mentesítés, archiválás)

Energia ellátás	Ingatlan üzemeltetés	Rossz, elavult nagyfeszültségű hálózat érintésvédelmi problémák	BCP, szolgáltatások leállása, vagyonbiztonsági kérdések	BCP, szolgáltatások leállása, vagyonbiztonsági kérdések	Épületgépészet, érintésvédelmi szabályzat, kábelek, elosztók, villamossági elemek cseréje, szünetmentes tápegységek alkalmazása
Épületek	Ingatlan üzemeltetés	Épületgépészeti problémák, felújítási munkálatok elvégzése	Munkavédelmi, munkajogi kérdések, esztétika	Baleset, sérülés, vagyonkárosodás	Szabályok, utasítások (parkolás rendje)
Fizikai védelmi rendszerek	Őrzésvédelmi szolgálat, ingatlan üzemeltetés	Vagyonbiztonsági fenyegetettség	Lopás, rongálás, üzleti titoksérelem	Vagyonban ért károsodás, rendszerleállás, szolgáltatások leállása, iratok-adatok-eszközök eltulajdonítása	Élőerős őrzésvédelem biztosítása, vagyonbiztonsági-technikai eszközök, rendszerek telepítése, újra konfigurálása
Hálózati aktív elemek, Szerver számítógépek	Rendszergazda	adatok elvesztése, vagy a működés megszakadása, túlterhelés	elégtelen, vagy hibás mentések, mentési állományok keveredése, azonosíthatatlansága, mentési ütemezés hiánya, mentés megőrzési idők hibás beállítása, szerver oldali leállás,	adatvesztés, rendszerek üzemképtelensége, BCP/DRP tevékenységek lehetetlenné válása	Szerver oldali programok és néhány hardver eszköz cseréje, újra konfigurálása
IT szolgáltatás folyamatok (produktív)	Rendszergazda	támogató folyamatok leállása, üzletfolytonosság, adatbiztonság, adatvédelem	külső adatbázisokban lévő adatok biztonsági mentésének hiánya	adatvesztés, rendszerek üzemképtelensége, BCP/DRP tevékenységek lehetetlenné válása	külső szolgáltatókkal történő szorosabb együttműködés
LAN, WAN, Desktop számítógépek	Rendszergazda, felhasználó	szabálytalan hálózati szolgáltatások és internet használat, adatlopás	szabályok, tudatosság, védelmi megoldások hiánya vagy elégtelensége	munkaidő kiesés, információ kiszivárgás, hátrányos jogi következmények	Hálózati szolgáltatások használatára vonatkozó szabályzat, rendszer újra konfigurálása
Mentési adathordozók	Adatgazda, rendszergazda, létrehozó tulajdonos	Adatok kiszivárgása Bizalmas információk kikerülése, adatvédelem, üzleti titkok	adatmentesítés elmaradása titkosítatlan és nem nyilvántartott adathordozók használata, felhőtárhely szolgáltatások igénybevétele	adatok kiszivárgása, jogi következmények jogi és üzleti következmények, publicitás, sajtó	Berendezések biztonságos selejtezése, illetve újra felhasználása Titkosítás, rezsim intézkedések, IT Szabályzat

Minden vagyonelem	Szervezet valamennyi tagja, érdekeltje	az információbiztonság gyenge hatékonysága visszaélések információ feldolgozó eszközökkel, eszközök ellenőrizetlen használata, eszközök hibás, vagy hanyag használata, adatvesztés, adatok kiszivárgása, szolgáltatások megszakadása 3. fél részéről történő az információbiztonságot veszélyeztető tevékenység vagyonelemek felelőtlen kezelése Bizalmas információk nem megfelelő kezelése	vezetés támogatásának hiánya, az erőforrások hiánya ellenőrizetlen jogosultságok rosszindulatú vagy téves, hanyag tevékenységek, munkavégzés, takarítás, karbantartás, építés során vagyontárgyakért való felelősség tisztázatlansága az osztályozási elvek hiánya, következetlensége, vagy hiányos ismerete	károkozás ügyfélnek, üzletmenet megszakadása adatok kiszivárgása, adatok elvesztése, hátrányos jogi következmények, károkozás ügyfélnek szolgáltatások megszakadása, adatok kiszivárgása adatok elvesztése, adatok kiszivárgása, károkozás ügyfélnek adatok kiszivárgása, károkozás ügyfélnek, hátrányos jogi következmények	A vezetés elkötelezettsége az információbiztonság ügye iránt Jogosultsági engedélyezési folyamat az információ-feldolgozó eszközökre, illetve az egyes információkhoz való hozzáférésre vonatkozóan Vagyontárgyak tulajdonjoga Osztályozási elvek
Mobil adathordozók (pendrive, cd, dvd, ...)	Adatgazda, rendszergazda, létrehozó tulajdonos	Adatok kiszivárgása, adatok elvesztése	adathordozók engedélyezetlen kivitele, adathordozók gondatlan kezelése, adathordozók elvesztése, adathordozók elhasználódása	adatok kiszivárgása, adatvesztés, adatok konzisztenciájának elvesztése	Vagyontárgyak eltávolítása, az eltávolítható adathordozók kezelése
Mobil számítógépek és mobiltelefonok	Felhasználó	mobil eszközök sérülése, elvesztése, ellopása	a mobileszközök védelmének hiányos vagy hibás szabályozása, tudatosság hiánya	adatok elvesztése, adatok kiszivárgása	Berendezések biztonsága a telephelyen kívül
Munkakörnyezet	Ingatlan üzemeltetés	vihar és villámlás okozta elektromos túlfeszültségek, tüzek, vízbetörés, gázömlés, földrengés, robbanás áramellátás megszakadása	hibás vagy elégtelen épületvédelmi rendszerek, szünetmentes áramellátás nem megfelelősége nem megfelelő szünetmentes áramellátás	üzletmenet megszakadása	Külső és környezeti veszélyekkel szembeni védelem Közműszolgáltatások (UPS)
Munkatársak	Szervezet valamennyi tagja, érdekeltje	Visszaélések az üzemeltetésben Visszaélések az üzemeltetésben Hibás vagy rosszindulatú tevékenységek Hibás vagy rosszindulatú tevékenységek illetéktelen hozzáférések, rosszindulatú tevékenységek	az üzemeltetési jogkörök és felelősségek nem megfelelő szétválasztása szakmailag nem megfelelő, információbiztonsági szempontból nem megbízható munkatársak felvétele felelősségek, követelmények, szabályozások hiányos vagy hibás ismerete, szakmai alkalmatlanság	adatok kiszivárgása, károkozás ügyfélnek adatok kiszivárgása, károkozás ügyfélnek, hátrányos jogi következmények adatok kiszivárgása, károkozás ügyfélnek, hátrányos jogi következmények szolgáltatások megszakadása, üzletmenet megszakadása, hátrányos jogi következmények	Feladat- és felelősségi körök (munkaköri leírások) Átvilágítás Alkalmazási kikötések és feltételek A vállalatvezetés felelőssége Felelősségek az alkalmazás megszűnésekor ("kilépő papír")

			információbiztonsági szabályok hiányos bevezetése, elfogadásának, következetes használatának hiánya, szabályok megsértésének eltűrése, kilépett, elbocsátott munkatársak jogosultságainak nem történik meg a megszüntetése	illetéktelen hozzáférés, adatok kiszivárgása, károkozás ügyfélnek	
Nyomtatók	Felhasználók	illetéktelen hozzáférések, rosszindulatú tevékenységek, pazarlás	nyomtatások felügyelete, adminisztrációja nem megoldott	illetéktelen hozzáférés, adatok kiszivárgása, károkozás cégnek, ügyfélnek	Csak a szükséges nyomtatások elvégzése, papír alapú iratkezelés szabályozása
Papíralapú dokumentumok	Létrehozó, dokumentum/irat felelős	illetéktelen hozzáférések, rosszindulatú tevékenységek, pazarlás, iratok nyomon követhetőségének hiánya, üzletit titoksértés, adatvédelem,	szabályozatlan ügyviteli folyamtok	illetéktelen hozzáférés, adatok kiszivárgása, károkozás cégnek, ügyfélnek, iratok elvesztése	ügyviteli és iratkezelési szabályzat kialakítása
Szerver számítógépek	Rendszergazda	Lassan elavuló hardver, szerver oldali programok elavultak, jelszavak hiánya, gyengesége, optimális szerver oldali szolgáltatások akadozása, adatbiztonság, adatvédelem, üzletfolytonosság,	desktop oldalon jelszókezelési szabályok hiányos meghatározása és érvényesítése	jogosulatlan hozzáférések, adatvesztés, adatok kiszivárgása, szabotázs, rosszindulatú támadás, üzletmenet teljes leállása, óriási információs vagyonvesztés	Szerver oldali szoftverek és hardver eszközök cseréje, jelszópolitika és csoportházirendek alkalmazása, hálózati eszközök aktívabb felügyelete
Szerver alkalmazások	Rendszergazda	illetéktelen hozzáférések, visszaélések adatokkal, jelszavak kompromittálódása, jelszavak feltörése, Visszaélések jogosultságokkal	a felhasználó azonosításának hiánya, hibás vagy nem biztonságos bejelentkezési eljárások, látható, visszakereshető jelszavak, korlátozott felhasználói tevékenységek csoportos felhasználók, tévesen azonosított felhasználók	jogosulatlan hozzáférések, adatok kiszivárgása, adatok kiszivárgása, információbiztonsági események kivizsgálásának ellehetetlenülése adatvesztés, adatok kiszivárgása szabotázs, incidensek kivizsgálásának ellehetetlenülése,	Felhasználó azonosítása és hitelesítése, biztonságos bejelentkezési eljárások, csoportházirendek elkészítése Felhasználók regisztrálása
Üzemeltetési dokumentáció	Rendszergazda	Nem érhetőek el egységes felületen keresztül, szétszórt dokumentáció	üzletmenet folytonossági fennakadásokat okoz	hiba, módosítás esetén nehezen előkereshető információk	Üzemeltetési dokumentáció iratkezelési szabályzatba történő felvitele, egységes tárolás kialakítása

11.6. Oktatási terv

SAFETY SECTOR Kft.	OKTATÁSI TERV			LAPSZÁM: 2022/1	
Sor-szám	Oktatás, képzés tárgya, témája	Oktatási intézmény, illetve oktató	Tervezett időpont	Megvalósult időpont	Megjegyzés	Aláírás
1.	Vezetőségi oktatás Informatikai szabályzat, IBIR rendszer, adatvédelem, IT kockázatok a mindennapokban, zsaroló vírusok, elektromos gépjárművel intelligens vezérlő rendszerei	Szabó József	2022.01.15.	2022.01.22.	1/2022	
2.	Mobil eszközök biztonsága, telefonokkal történő kommunikáció	[redacted] Kft.	2022.02.11	2022.02.11.	2/2022	
3.	A távmunkavégzés módja, internetes kapcsolat, mobil videokamerák használata, biztonsági kérdések, dokumentumok szállítása és használata	Szabó József	2022.03.26.	2022.03.26.	3/2022	
4.	Haditechnikai eszközök használata, konfigurálása	Szabó József, [redacted]	2022.04.30.	2022.04.30.	4/2022	
5.	Webbank használata és kockázatai, kétfaktoros azonosítás, ellenőrző kódok, Token használata, jelszavak	Szabó József	2022.05.19	2022.05.21.	5/2022	
6.	Irodai számítógéphasználat, érintésvédelem, biztonságos jelszavak.	Szabó József, [redacted]	2022.07.31.	2022.....[2].	6/2022	

[2] Adatvédelmi okból a résztvevők nevét kitakartam.

HALLGATÓI NYILATKOZAT

diplomadolgozat nyilvános hozzáféréséről és eredetiségéről

A hallgató neve:	Szabó József
A Hallgató Neptun kódja:	CQJVYQ
A dolgozat címe:	INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR) BEVEZETÉSE ÉS FENNTARTÁSA SZENZITÍV ADATOKAT KEZELŐ VÁLLALKOZÁSNÁL
A megjelenés éve:	2023
A konzulens intézetének neve:	Műszaki Intézet
A konzulens tanszékének a neve:	Műszaki Menedzsment Tanszék

Kijelentem, hogy az általam benyújtott diplomadolgozat egyéni, eredeti jellegű, saját szellemi alkotásom. Azon részeket, melyeket más szerzők munkájából vettem át, egyértelműen megjelöltem, és az irodalomjegyzékben szerepeltettem.

Ha a fenti nyilatkozattal valótlant állítottam, tudomásul veszem, hogy a záróvizsga-bizottság a záróvizsgából kizár és a záróvizsgát csak új dolgozat készítése után tehetek.

A leadott dolgozat, mely PDF dokumentum, szerkesztését nem, megtekintését és nyomtatását engedélyezem.

Tudomásul veszem, hogy az általam készített dolgozatra, mint szellemi alkotás felhasználására, hasznosítására a Magyar Agrár- és Élettudományi Egyetem mindenkori szellemitulajdon-kezelési szabályzatában megfogalmazottak érvényesek.

Tudomásul veszem, hogy dolgozatom elektronikus változata feltöltésre kerül a Magyar Agrár- és Élettudományi Egyetem könyvtári repozitori rendszerébe. Tudomásul veszem, hogy a megvédett és

- nem titkosított dolgozat a védést követően
- titkosításra engedélyezett dolgozat a benyújtásától számított 5 év eltelte után

nyilvánosan elérhető és kereshető lesz az Egyetem könyvári repozitori rendszerében.

Kelt: Gödöllő év 2023 hó november 6. nap

Szabó József

Hallgató aláírása

KONZULENSI NYILATKOZAT

Szabó József (hallgató Neptun azonosítója: CQJVYQ) konzulenseként nyilatkozom arról, hogy a diplomadolgozatot áttekintettem, a hallgatót az irodalmi források korrekt kezelésének követelményeiről, jogi és etikai szabályairól tájékoztattam.

A diplomadolgozatot a záróvizsgán történő védésre **javaslom** / nem javaslom[1].

A dolgozat állam- vagy szolgálati titkot tartalmaz: igen nem*[2]

Kelt: Gödöllő, 2023. év november hó 6. nap

Dr. Kovács Imre
belső konzulens

[1] A megfelelő aláhúzandó.
[2] A megfelelő aláhúzandó.