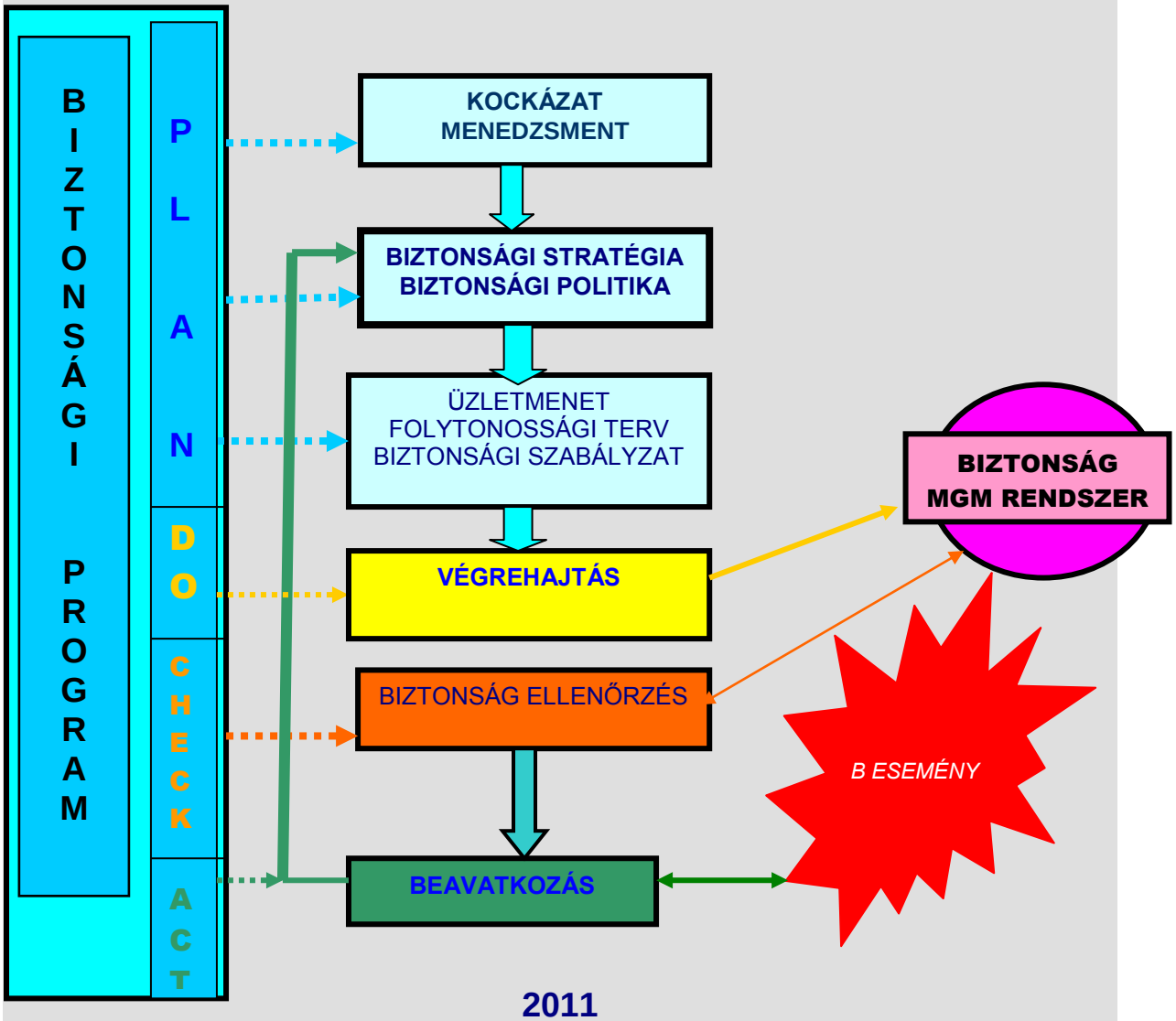
VASVÁRI GYÖRGY CISM

BIZTONSÁGSZERVEZÉSI MÓDSZERTAN

INFORMATION SECURITY MANAGEMENT SYSTEM ORGANISATION METHODOLOGY

ISMS I. kötet



2011

Szakmai lektor:

Erdősi Péter Máté CISA, elektronikus aláírás szolgáltatás szakértő

" A biztonságban egy dolog 100%-os, mégpedig az, hogy semmi nem 100%-os."

(Egy hacker feljegyzéseiből)

ISMS I. kötet.

BIZTONSÁGSZERVEZÉSI MÓDSZERTAN

INFORMATION SECURITY MANAGEMENT SYSTEM METHODOLOGY

2011

Tartalom

1. BEVEZETÉS

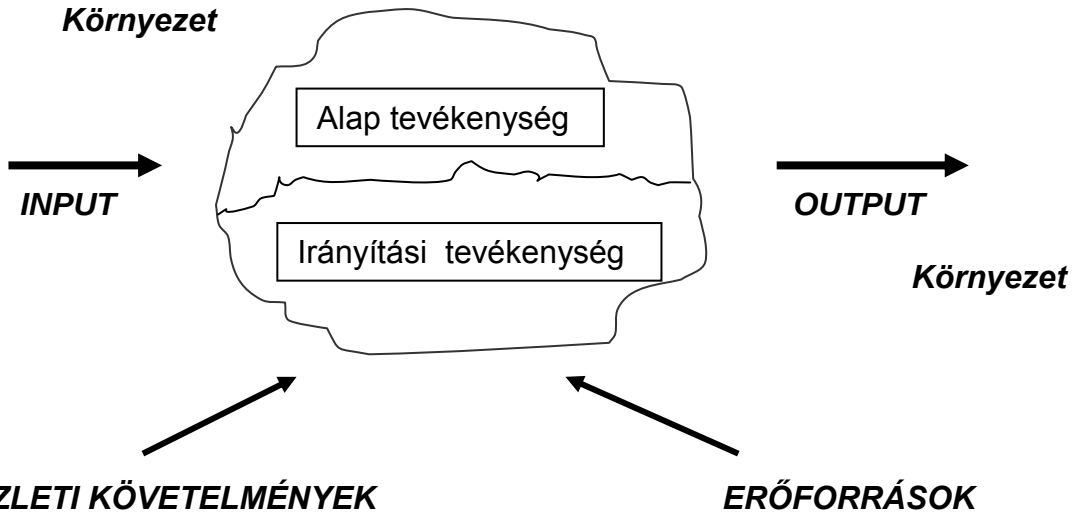
Az ISMS célja, hogy a biztonságszervezéssel foglalkozók számára értelmezze a szervezési feladatokat, a megvalósítás módszereit, és az eszközeit.

*A **biztonságszervezés** egyrészt **auditálási** (Kockázat menedzsment), másrészt **tanácsadási** (Biztonsági Stratégia, és Politika, Katasztrófaterv, Biztonsági Szabályzat, és Biztonság ellenőrzési módszertan készítése) feladat. Az ISMS ezért e két szakmai tevékenység elveit, és tapasztalatait is felhasználja.*

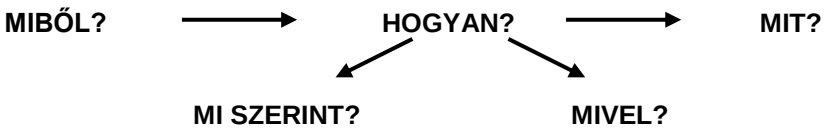
1.1. ALAPKÉRDÉSEK

1.1.1. A biztonság helye a gazdasági szervezetben

A gazdasági szervezet funkcionális modellje:



A gazdasági szervezet funkcionális modellje a következő kérdésekre ad választ



A miből, a hogyan, és a mit az adott vállat alaptevékenységétől függ, amely lehet

- ⇒ *Termelési*
- ⇒ *Logisztikai*
- ⇒ *Szellemi*

Az erőforrásokra a későbbiekben visszatérünk, míg az üzleti követelmények a következők:

- ⇒ *Minőségi*
- ⇒ *Megbízhatósági*
- ⇒ *Biztonsági*

A minőségi követelmények *a termék és/vagy szolgáltatás minőségére, a költség hatékony működésre, és a szállítókészségre vonatkoznak.*
A megbízhatósági követelmények *a rendeltetésszerű működésre, a hatályos jogszabályok és a belső szabályzatok betartására, valamint a kiszámítható üzleti magatartásra vonatkoznak.*
A biztonsági követelmények, *pedig a bizalmasság, a sértetlenség, és a rendelkezésre állás.*

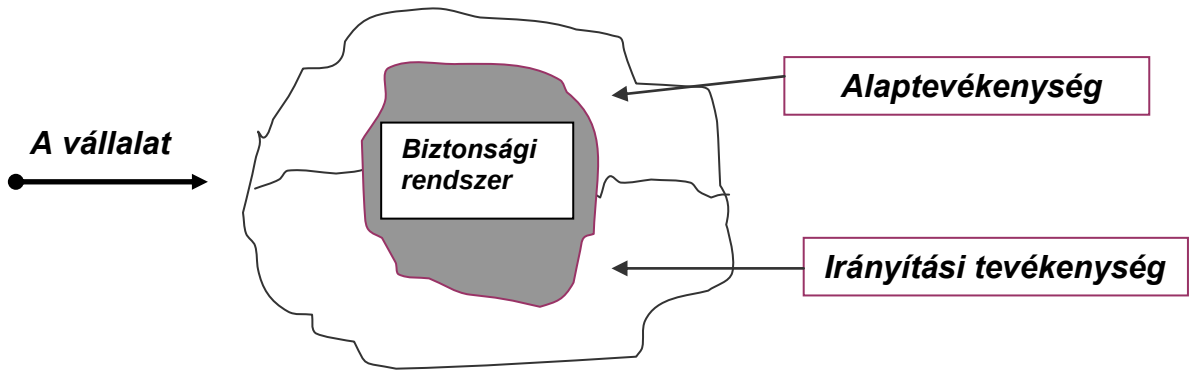
Kiindulási pontunk tehát az, hogy

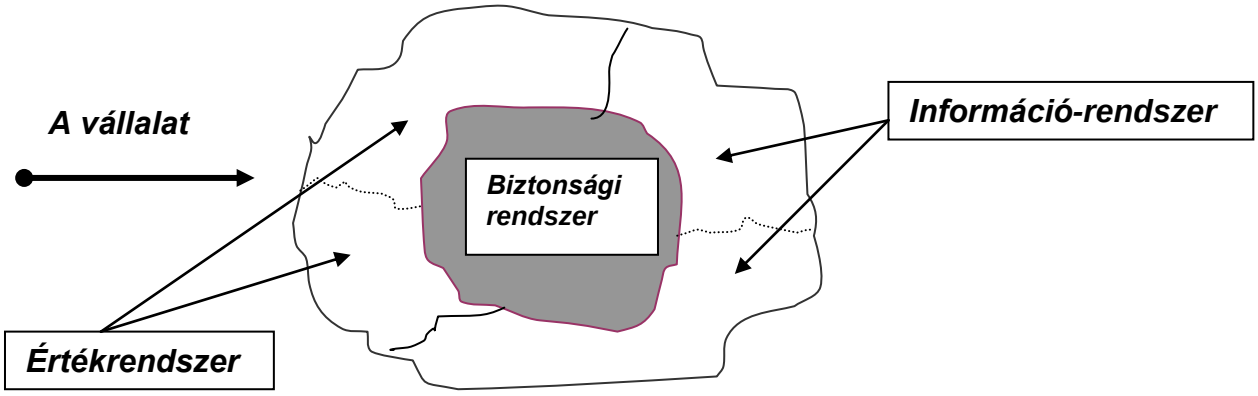
\+ ***A BIZTONSÁG ÜZLETI KÖVETELMÉNY.***

A biztonság egy gazdasági szervezeten belül a biztonsági rendszerben valósulhat meg, mégpedig a biztonságszervezés útján.

Esetünkben biztonság alatt a vagyon, és az IT biztonságot értjük, tehát nem foglalkozunk a termelő vállalatoknál kiemelten jelentős üzembiztonsággal, valamint a vállalat gazdasági biztonságával.

A biztonsági rendszer a vállalat, mint mikró gazdasági rendszerben az egyik rendszer, amely kiterjed az alaptevékenységre, és az irányítási tevékenységre, illetve az érték-, és az információ-rendszerekre egyaránt (lásd alábbi ábrák).





*Az értékrendszerben zajlanak **az üzleti,** és ha az alaptevékenység termelés, vagy szolgáltatás **a termelési** (és/vagy szolgáltatási) **folyamatok zajlanak,** amelyeket kiszolgál az információs rendszer, **az informatikai alkalmazások.***

***Az üzleti folyamatok:** lényegében a vállalat alaptevékenységet valósítják meg.*
***A támogató folyamatok:** a vállalatirányítás, menedzsment, fejlesztés, marketing, pénzügy, számvitel, kontrolling, humán erőforrás menedzsment, jogi, minőségbiztosítási, ellenőrzési folyamatok, amelyek támogatásával tudnak az üzleti folyamatok végbe menni.*

A gazdasági szervezet tevékenysége felbontható
⇒ *Az **értékrendszerre** (ÉR), amely áll*
- *Az üzleti rendszerből (ÜR), azaz az üzleti, és támogató folyamatokból, ahol definiáljuk a vagyonbiztonsági alrendszert, és ha van*
- *A termelési (szolgáltatási) rendszerből (TR) azaz a termelési folyamatokból, ahol definiáljuk az üzembiztonsági alrendszert, valamint*

⇒ *Az **információs rendszerre** (IR) azaz az informatikai alkalmazásokra, ahol definiáljuk az informatikai biztonsági alrendszert.*

Az üzleti rendszerben valósul meg a papír alapú iroda, míg az információs rendszerben, rendszerrel az elektronikus iroda.
*A rendszereket átfogja a **biztonsági rendszer,** melynek célja az egyenszilárdságú biztonság feltételeinek megteremtése a gazdasági szervezet minden pontján (egyenszilárdság elve).*

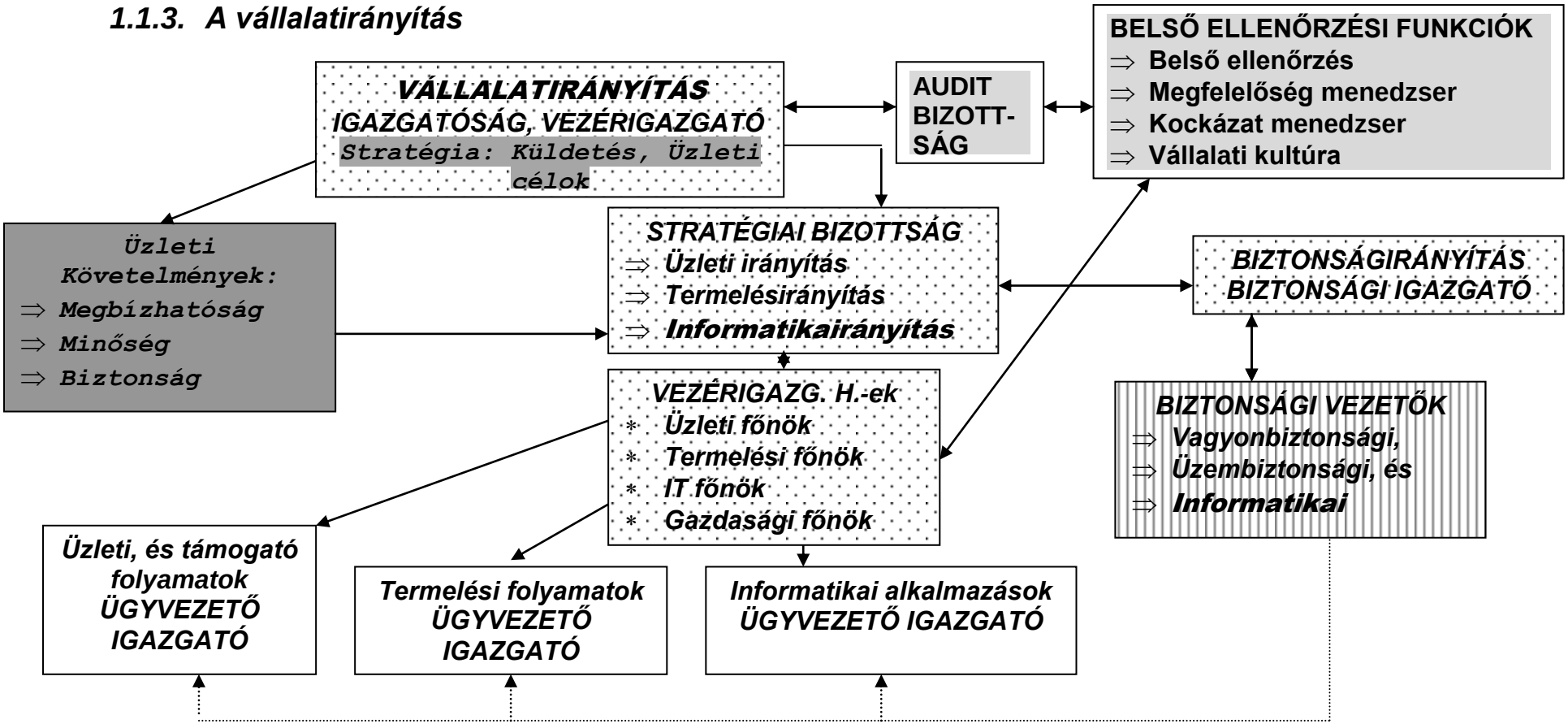
1.1.2. A biztonság összetevői

A biztonság összetevői mind az ÉR, mind IR-ben
⇒ *A szervezési (ezen belül a humán) biztonság*
⇒ *A fizikai (természeti) biztonság, és*
⇒ *A logikai biztonság.*

A biztonság elemei pedig
⇒ *A bizalmasság,*
⇒ *Sértetlenség, és a*
⇒ *Rendelkezésre állás.*

Itt tehát azt rögzítjük, hogy az IT biztonsághoz képest sem a biztonság összetevői, sem a biztonság elemei vonatkozásában nincs a három rendszer vonatkozásában eltérés.

1.1.3. A vállalatirányítás



A vállalatirányítás definíciója a COBIT 4.1 alapján:

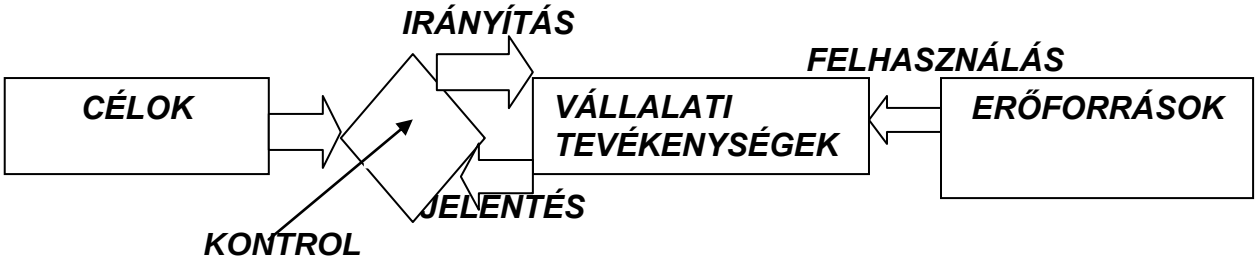
+ A vállalatot irányító, és ellenőrző összefüggések, és folyamatok struktúrája, annak érdekében, hogy a vállalatok érték hozzáadással elérhessék céljaikat, mérlegelve a kockázatot az ÉR (ÜR, TR), és IR, és folyamataik használ szemben.

A felső vezetés (IGAZGATÓSÁG, Vezérigazgató) feladata a vállalatirányítással kapcsolatban:

⇒ *Meghatározza a vállalati stratégiát,*
⇒ *Felméri a költségeket, kockázatokat, lehetőségeket.*
⇒ *Felméri, hogy a célok teljesülhetnek-e, hozhatnak-e eredményt a magvalósítás folyamatai.*
⇒ *Létrehoz a három irányítási területre Stratégiai Bizottságokat, az előbbiek megvalósítására.*

A Stratégiai Bizottságok (VEZ. IG .H.-ek, +Bizt. Vez.) tevékenységei:
⇒ *Közreműködés az üzleti célok, a stratégia érvényesítésében.*
⇒ *Gondoskodás a stratégiai céloknak megfelelő erőforrások rendelkezésre állásáról.*
⇒ *A költségek optimalizálása.*
⇒ *A külső erőforrások szerepének meghatározása, ellenőrzése.*
⇒ *A kockázatok feltárásában, és csökkentésében közreműködés.*

A vállalatirányítás *(Enterprise Governance)* ***funkcionális modellje*** *(COBIT3 alapján):*



Amint az ábrából látható:

* *A vállalatirányítás az igazgatóság feladata, amelynek gyakorlati bonyolítását a Vezérigazgató, és a Stratégiai Bizottság végzi.*
* *Az egyes szakterületek irányítása (üzlet, termelés, informatikairányítás) a szakterületek vezetőinek feladata.*
* *A Biztonságirányítás a vezetőjén keresztül részt vesz a vállalati-stratégia irányításában, míg a szakterületeknek a biztonságirányításáért (vagyon, termelési, informatikai biztonságirányítás) a szakterületek biztonságáért felelős vezetők (vagyon, üzem, informatikai biztonság) viselik a felelősséget.*

1.1.4. Mit kell védeni?

A biztonság e fenti elemek maximális biztosításával teremthető meg, azaz a védelem tárgya az erőforrások bizalmassága, sértetlensége, és rendelkezésre állása fenyegetettségének a minimálisra csökkentése, és ezzel a vállalat (szervezet) üzleti céljának, a küldetése teljesülésének védelme.

AZ ERŐFORRÁSOK:

Az üzleti rendszerben (ÜR):

⇒ *Az **adatok, információk, a pénz, az értékek, az áruk***
⇒ *Az **üzleti infrastruktúra***
- *A technológia, (az ügyviteltechnika, informatika),*
- *Támogatások, létesítmények (mint épületek és helyiségek), rendszerek (mint áramellátás, légkondicionálás, egyéb kisegítő berendezések),*

⇒ *Az automatikus, és manuális **üzleti folyamatok***
⇒ *Az **ember.***

A termelési (TR), szállítási rendszerben

⇒ *A **nyersanyagok, anyagok, félkész áruk, és az adatok**, **információk***
⇒ *A **termelési infrastruktúra***
- *A technológia, (termelési, termelésirányítási),*
- *Támogatások, létesítmények (mint épületek és helyiségek), rendszerek (mint áramellátás, légkondicionálás, egyéb kisegítő berendezések),*

⇒ *Az automatikus, és manuális szállítási és/vagy **termelési, és termelésirányítási folyamatok,** eljárások, és*
⇒ *Az **ember.***

Az informatikai rendszerben (IR):

⇒ *Az **adatok, információk***
⇒ *Az **IT infrastruktúra***
- *A technológia, (a hw, rendszer sw, nw),*
- *Támogatások, létesítmények (mint épületek és helyiségek), rendszerek (mint áramellátás, légkondicionálás, egyéb kisegítő berendezések),*

⇒ *Az automatikus, és manuális **alkalmazási folyamatok**,*
⇒ *Az **ember.***

*Az üzleti rendszerben **VAGYON BIZTONSÁGRÓL***
*A termelési rendszerben **ÜZEMBIZTONSÁGRÓL**, míg*
*az információs rendszerben **INFORMATIKAI BIZTONSÁGRÓL** beszélünk.*

A három rendszer biztonsága, pontosabban a biztonság megteremtése érdekében teendő védelmi intézkedések részben átfedik egymást. Ezzel a következőkben foglalkozunk.

A vállalatszervezés a következő szervezési tevékenységekből áll

⇒ *Munka, és üzemszervezés*
⇒ *Informatikai rendszerszervezés*
⇒ *Biztonsági rendszerszervezés*

⇒ *Minőségbiztosítás*

A munka, és üzemszervezés az alap (termelési, anyagi, logisztikai, szellemi), és az irányítási folyamatok szervezése. (Idetartozik például a szervezet, és működésszabályozás).

Informatikai rendszerszervezés az alap, és irányítási folyamatok információs folyamatai számítástechnikai eszközökkel történő támogatásának szervezése.

Biztonsági rendszerszervezés a gazdasági szervezet (az alap, és az irányítási tevékenység) folyamatos, és rendeltetésszerű működése biztonsági feltételeinek biztosítása. A biztonsági rendszer, mint a fenti ábrákból is következik, nem független attól a környezettől, amelyben működését ki kell fejtenie. A gazdasági szervezet, a vállalat szervezettsége, tehát magába foglalja a biztonságszervezést is.

A minőségbiztosítás a vállalat termékeinek, és saját működésének minőségbiztosítására irányuló tevékenység (ISO 9000, és ISO 14000 szabványok alkalmazása).

1.1.5. A biztonságszervezés

*A **szervezés**alkotó szellemi tevékenység, amely meghatározott cél érdekében, az adott kor ismeretanyagának, tudományos eredményeinek felhasználásával a különböző szervezetekben a küldetésüknek megfelelő folyamatok, és a szervezet erőforrásai felhasználásának működési rendjét meghatározó tevékenység (lásd [52]-ben).*

*A **biztonságszervezés** a biztonság optimális biztosítása, a kockázatok (az erőforrások fenyegetettségét) minimálisra csökkentése érdekében végzett szervezési tevékenység, amely a biztonsági rendszer biztonságos létrehozására, üzemeltetésre, és fejlesztésére irányul.*

A biztonságszervezési tevékenység egy folyamat, amelynek táblázatos bemutatása az 1.1.6.-ban található. A biztonság követelményeit meghatározó Common Criteria (USA, Kanada, és Nyugat Európa szabványosítási intézeteinek közös munkája) felhasználásával, ma már az ISO/IEC 17799 nemzetközi szabvány, illetve a Commmon Evaluation Methodology, ma már ISO/IEC 15408, amelyeknek van magyar változata. Az alábbi táblázatban, pedig bemutatjuk, hogy miből kiindulva, milyen feladatot kell megoldani a biztonságszervezőnek, pontosabban a biztonságszervezési folyamatnak melyek a szintjei
TARGOWSKI, és T.RIENZO írja (9)-ben, hogy
„ A rendszer elemek cél orientált készlete, valamint azok tudatosan orientált, strukturált kapcsolatai, amelyek mérhető eredményeket állítanak elő a rendszeren kívül,…”továbbá„….a rendszer több mint a részeinek összessége”.
A BS 7799-2:2002, angol szabvány (a 12.2. pontban) a rendszerszemléletet a következőképpen határozza meg:
„Egy szervezet folyamatai rendszerének alkalmazását, ezeknek a folyamatoknak az azonosításával,, kölcsönhatásaival, és a menedzsmentjükkel együtt, nevezhetjük rendszer szemléletű megközelítésnek.”

Ebből következik, hogy a védelmi rendszer kiépítése a gazdasági szervezet, mint rendszer megközelítését, azaz rendszerszemléletet kíván meg. Azaz védeni az egész rendszert kell, és miután a rendszer elemei kölcsönhatásban vannak, a védelemnek ezt figyelembe kell venni. Ez nem kevesebbet jelent, mint azt, hogy a védelmi rendszert az egész vállalatra tekintve, az elemek kapcsolatait figyelembe véve, egységesen kell kiépíteni. Nem lehetséges a biztonsági kockázatokat megfelelően csökkenteni, ha egyes kiragadott problémákat oldunk meg, pl. a logikai belépés ellenőrzés önmagában nem nyújt megfelelő védelmet, csak további védelmi intézkedésekkel együtt. Az informatikai védelem vagyonvédelem nélkül nem hozhatja a kívánt eredményt.

A támadó a támadás előkészítésére általában sok idővel rendelkezik, ezért ki keresheti a védelmi rendszer gyenge pontját, és ott támad majd. Vigyázat! Gyenge pont a megkerülhetőség kockázatát képezi, és olyan hatással, hogy az egyik alrendszeren belüli gyengeség a másik alrendszer (-ek) megkerülhetőségét eredményezheti. Az Internetről letölthetők szabadon olyan scanner programok, amelyek egy tűzfalnál akár 200 gyengeséget tudnak találni, amelyek erős behatolási lehetőséget jelentenek a támadó számára, azaz a megkerülhetőséget. Továbbá, például K.D. Mitnick, a most megjelent könyvében azt írja: A social engineering a befolyásolás és rábeszélés eszközeivel megtéveszti az embereket, manipulálja, vagy meggyőzi őket arról, hogy a támadó, tényleg az, akinek mondja magát. Ennek eredményeként az ezzel élő támadó képes az alkalmazottakat információ szerzés érdekében kihasználni. Ez ellen csak erős behatolás, illetve hozzáférés védelmi rendszer biztosításával lehet védekezni.

Az egyenszilárdság elve kimondja, hogy a hatékony védelem előfeltétele a gazdasági szervezet minden pontján minimum azonos erősségű, és ellenálló képességű védelmi intézkedések alkalmazása, amely egyúttal meghatározza a maximális maradék kockázatot, és ezzel figyelembe veszi a vállalat kockázat tűrő képességét. (lásd még: 10.6)

A COBIT Security Baseline 2nd edition. 2007. a biztonság céljának meghatározásakor egyértelműen rámutat arra, hogy a biztonságot az egész rendszerre, teljes körűen (holistic) kell szervezni, mégpedig a vállalat mint rendzseren belül folyamat orientáltan. Ugyanis az üzleti folyamatokat az informatikai folyamatok, ha van a termelési folyamatok kiszolgálják. Azaz például az információs rendszer jelen van papír alapon, és elektronikusan egyaránt. Ebből következik, hogy az **információ védelme, az egész vállalaton belüli védelmet igényli. Az említett COBIT anyagban P. Dorey az információ biztonság célját a következőképpen fogalmazza meg:**

Az információ biztonság gondoskodik a menedzsment folyamatokról, technológiákról, és szavatolja, hogy az üzlet menedzsment lehetővé tegye, hogy az üzleti tranzakciókban meg lehessen bízni, az IT szolgáltatás használható, és megfelelően ellenálló legyen, állítsa vissza a hibák, támadások vagy katasztrófák miatti meghibásodásokat, gondoskodjon a kritikus, bizalmas információk visszatartásáról, azok elől, akiknek nem lehet hozzáférésük.

Tehát az információ biztonság, amely nem azonos az informatikai biztonsággal, az információk, a vállalaton belüli rendszerek, alrendszerek, folyamatok, és kommunikációk teljes körű védelmét jelenti, hogy azok a rendelkezésre állás, bizalmasság, és sértetlenség sérülésétől mentes információkat szolgáltassanak.

A BIZTONSÁGSZERVEZÉS SZINTJEI

AZ ALAP		***A feladat***		***AZ EREDMÉNY***
		❶SZINT		
JOGSZABÁLYOK, ŰZLETI STRATÉGIA BELSŐ SZABÁLYOK ERŐFORRÁSOK MŰKÖDŐ VÉDELEM	⇨	***Mit kíván az üzleti érdek?***	⇨	***BIZTONSÁGI KÖRNYEZET*** AZONOSÍTÁSA
		❷SZINT		
BIZT.-I KÖRNYEZET FENYEGETÉSEK	⇨	***Mi a gyakorlat?***	⇨	***KOCKÁZATOK***
		❸SZINT		
KOCKÁZATOK	⇨	***Mit kell elérni ?***	⇨	***BIZTONSÁGI*** KÖVETELMÉNYEK
		❹SZINT		
BIZTONSÁGI KÖVETELMÉNYEK	⇨	***Mit, hogyan kell védeni?***	⇨	***VÉDELMI INTÉZK. SPECIFIKÁCIÓJA***
		❺SZINT		
VÉDELMI INTÉZKEDÉSEK IMPLEMENTÁLÁSA	⇨	***Hogyan kell megvalósítani?***	⇨	***BIZT. RENDSZER***

1.1.6. A biztonságszervezés folyamata

A biztonságszervezés folyamatát, a tevékenységeket, a témákat, és a végtermékeket a következő ábrán mutatjuk be. Felhívjuk a figyelmet arra a biztonságszervezési folyamat egyes lépéseinek sorrendje nem változtatható meg, illetve nem lehet egy lépést a korábbiak megtétele nélkül megtenni., mert ez az egyenszilárdság elvének a megsértéséhez vezet.
A Kockázat menedzsment alapján a kockázatok csökkentésére, kerül kidolgozásra a Biztonsági Stratégia, amely hosszútávon határozza meg a biztonságirányítás céljait, követelményeit, míg rövid távon taktikai megvalósítást a védelmi intézkedéseket a Biztonsági Politika, és az Üzletmenet folytonossági Terv határozza meg.

TEVÉKENYSÉG → ***TEVÉKENYSÁG TÁRGYA ↓***	***HELYZET FELTÁRÁS***	***VESZÉLY FORRÁS FELTÁRÁS KOCKÁZAT MGM***	***VÉDELMI KÖVETE TELMÉ NYEK***	***VÉDELMI INTÉZKEDÉSEK SPECIFIKÁCIÓJA RÉSZLE GES***	***ÁTFOGÓ***	***SZABÁ LYOZÁS***	***IMPLEMEN TÁCIÓ***	***ÜZEMELTE TÉS***	*ElIEN ŐRZÉS*	***REND SZER KÖVET ÉS***
BIZTONSÁGI KÖRNYEZET Szervezési környezet Erőforrások Védelmi intézkedések Fenyegetettség	***x*** ***x*** ***x*** ***x***	***X***								
KOCKÁZAT Szervezési veszélyforrások, Technikai veszélyforrások Kockázatai		***X*** ***X***			***x*** ***x***					
BIZTONSÁGI CÉL Bizalmasság Sértetlenség Rendelkezésre állás Számon kérhetőség Garanciák			***x*** ***x*** ***x*** ***x*** ***x***		***x*** ***x*** ***x***					
BIZTONSÁGI KÖVETELMÉNYEK Szervezési Technikai			***x*** ***x***							***x*** ***x***
VÉDELMI INTÉZKEDÉSEK ***Szervezési*** ***Technikai*** ***Fizikai*** ***Logikai***				***X*** ***X*** ***X***	***X*** ***X*** ***X***	***X*** ***X*** ***X***	***X*** ***X*** ***X***		***X*** ***X*** ***X***	***X*** ***X*** ***X***
IT BIZTONSÁGI PROGRAM										
VÉGTERMÉK	***Kockázat menedzsmenti jelentés***		***B.-i Straté gia***	***B.-i Politika***	***ÜFT***	***Bizt.-i Szabály-zat***	***Működő B.-i Rendszer***	***Üzemelő B.-i rendszer***	***Ellenőr-zés***	***Intézkedések***

1.2. A SZEMÉLY, ÉS A VAGYONVÉDELEM

A személy, és a vagyon védelem szükséges mind a három biztonsági alrendszerben, ezért 2005. évi CXXXIII. Törvényben meghatározott követelmények itt kerülnek ismertetésre.

A törvény célja, hogy - a közrend, a közbiztonság javítása, s ezek részeként a személy- és vagyonvédelem, a bűnmegelőzés hatékonyságának fokozása érdekében - erősítse a vállalkozás keretében végzett személy- és vagyonvédelmi, szolgáltatás törvényességét, és további garanciát nyújtson a társadalom számára az e szolgáltatásokat igénybe vevők, illetve az e szolgáltatások gyakorlása során érintettek személyhez fűződő jogai, vagyoni érdekei sérthetetlenségére irányuló igényeinek érvényesítéséhez.

A törvény jogi kertekbe foglalja a követelményeket:

- az e tevékenységet ellátó személyekre, illetve vállalkozásokra (az élőerős védelemnél, és outsourcing esetén, veendő figyelembe),
- A tevékenység közben ismertté vált személyes adatok védelmére (humán, és fizikai biztonságnál veendő figyelembe),
- A belépés, és mozgás ellenőrzés során rögzített személyes adatok kezelésére (fizikai biztonságnál veendő figyelembe)
- A tevékenységet gyakorlók jogosultságaira (a humán biztonságnál veendő figyelembe),
- a védelemhez felhasznált technikai védelmi eszközök felhasználásának feltételeire, korlátaira, illetve a felhasználás során keletkezett, és rögzített adatok kezelésére (a fizikai biztonságnál veendő figyelembe).

1.3. A BIZTONSÁG SZERVEZÉSE AZ ÉRTÉKRENDSZERBEN

1.3.1. A biztonság szervezése az Üzleti Rendszerben

1.3.1.1. A Kockázat menedzsment

A nehézséget az képezi, hogy az üzleti, és támogató folyamatok egyes esetekben igen nagy számot képezhetnek, és részben átfedhetik egymást. Ennek következtében a Kockázat felmérésnél az erőforrások tisztázását nagy gonddal kell elkészíteni.
További probléma, hogy az Üzleti rendszer több ponton kétirányú kapcsolatban lehet a termelési (szolgáltatási), és/vagy az informatikai rendszerrel, amelynek a helyzetfelmérése, és a veszélyforrások tisztázása kiemelten fontos, az egyenszilárdság elve szempontjából különösen.

1.3.1.2. A Biztonsági Politika készítése

A vagyonbiztonsági védelmi intézkedések egy része vonatkozni fog a másik két rendszerre is, ezért ezt a készítésnél figyelembe kell venni.

Felhívjuk a figyelmet arra, hogy az Üzleti Rendszerben logikai védelmi intézkedések is lehetnek, hiszen pl. az épület (intelligens épület) irányítás, vagy a vagyonbiztonsági alrendszer irányítása történhet informatikai eszközökkel.

1.3.1.3. A Katasztrófaterv készítése

A katasztrófaterv készítésénél az egyes üzleti folyamatokat egyenként kell megvizsgálni, és a Felhasználói Katasztrófatervezésnél alkalmazott módszereket kell használni, esetleg üzleti folyamatonként, ebben az esetben háttér eljárásokról kell gondoskodni. Ez nem zárja ki egy hagyományos Katasztrófaterv készítésének szükségességét, ahol például az épületek, munkahelyek esetében háttérről kell gondoskodni, valamint kezelni kell az olyan vészhelyzeteket, mint bombariadó (kiürítési terv). Végül, ahol az üzleti rendszerben informatikát alkalmaznak az Informatikai Katasztrófa tervezés módszertanát kell alkalmazni. Az üzleti folyamatok katasztrófaterve folyamat orientált, míg az üzleti rendszer, és az informatikai katasztrófaterv rendszer orientált.

1.3.1.4. A Biztonsági Szabályzat készítése

A Biztonsági Szabályzat készítésénél figyelembe kell venni a három rendszer közötti átfedéseket, és azokat egyszer kell szerepeltetni, a másik két esetben hivatkozni kell rájuk.

1.3.2. A biztonság szervezése a Termelési (szolgáltatási) Rendszerben

1.3.2.1. A Kockázat menedzsment

Az üzembiztonság szervezése egy teljes mértékben az adott üzemtől függő, különleges hozzáértést igénylő szakma, ezért a megfelelő szakember végezheti a kockázatfelmérést, és a veszélyforrás elemzést is.

1.3.2.2. A Biztonsági Politika készítése

A Biztonsági Politikában figyelemmel kell lenni a másik két rendszerrel való kétirányú kapcsolatokra. Külön célszerű foglalkozni magával a termelési (szolgáltatási) technológiával, és a termelést irányító informatikával. A Biztonsági Politika készítésénél figyelembe kell venni, hogy a Szervezési védelmi intézkedéseknél átfedés lehet a vagyonbiztonságnál alkalmazott védelmi intézkedésekkel, mint Humánvédelem, Szervezeti Szabályzat, Iratkezelési Utasítás, Titokvédelmi Szabályzat. Az elveket például egyszer, de általános érvénnyel kell meghatározni, és az egyes rendszereknél a sajátosságokra kell kitérni. A Fizikai hozzáférés védelmi intézkedések megegyeznek a vagyonbiztonsági védelmi intézkedésekkel, a fizikai rendelkezésre állásnál, pedig pl. a tűzvédelem, polgári védelem egyezik meg a vagyonbiztonsági védelmi intézkedésekkel.

1.3.2.3. Az ÜFT (Katasztrófaterv) készítése

Katasztrófatervet (Üzletmenet Folytonossági Tervet) külön kell készíteni a termelési rendszerekre, és a termelés irányító informatikára.

1.3.2.4. A Biztonsági Szabályzat készítése

A Biztonsági Szabályzat készítésénél figyelembe kell venni a három rendszer közötti átfedéseket, és azokat egyértelműen (egyszer kell szerepeltetni, a másik két esetben hivatkozni kell rá.

1.4. A BIZTONSÁG SZERVEZÉSE AZ INFORMÁCIÓS RENDSZERBEN

Az információs rendszerben a biztonságszervezését az ISMS részletesen leírja. Arra kell vigyázni, hogy itt is átfedések lehetnek a vagyonbiztonsági rendszerben tett védelmi intézkedésekkel.

1.5. A VÉDELMI INTÉZKEDÉSEK ÁTFEDÉSÉNEK ÖSSZEFOGLALÁSA

Az előbbiek szerint tehát a szervezési és a technikai védelmi intézkedések egyaránt előfordulhatnak bármelyik biztonsági alrendszerben, és egy vállalatnál nem lehet pl. több egymástól független biztonsági politika (Szabályzat).

Továbbá pl. az Iratkezelési Utasítás ma már egyaránt vonatkozik a papíralapú és az elektronikus iratokra. A Titokvédelmi Utasítás pedig foglalkozik nemcsak a személyes adatok és egyéb adatok, hanem minden további biztonság érzékeny erőforrás titokvédelmi osztályozásával. Pl. titkos papíralapú iratok tárolásával (helyiségek osztályozása) vagy titkos osztályozású papíralapú iratok elektronikus továbbításával, vagy a kinyomtatott titkos minősítésű informatikai outputok védelmével. A termelési rendszerben vagyonvédelmi (pl. a technológiát védő), a termelésirányító rendszerben informatikai védelmi intézkedések, a vagyonvédelmi alrendszerben az informatikai védelmi intézkedések is szükségesek.

Mind ebből következik, hogy a három alrendszerben a fentiekben megadott biztonsági összetevők egyaránt előfordulhatnak, így ma már indokolt és az egyik biztonsági alapkövetelmény a rendszer szemléleten alapuló integrált, vállalati szintű védelmi rendszer kialakítása.

A védelmi intézkedések a három biztonsági alrendszerben, és példák az átfedésre:

Alrendszerek⇒ / Védelmi intézkedések⇓	1Vagyon biztonsági alrendszer	2.Üzembiztonsági alrendszer		3.Informatikai biztonsági alrendszer
		Termelési rendszer	Termelés irányító r.	
SZERVEZÉSI Humán Véd. Int.	Humán politikai védelmi intézkedések			
Biztonsági szervezet és működés	Integrált biztonsági szervezet, és működés			
Adat és titok Kezelés	Adatvédelmi, Adatbiztonsági Szabályzatok Titokvédelmi Utasítás			
Iratkezelés	Iratkezelési Utasítás (papír és elektronikus)			
Biztonság a Szerződésekben	Szolgáltatási, karbantartási, szállítási, biztosítási szerződésekben a biztonsági követelmények			
TECHNIKAI Fizikai hozzá-Férés védelem	Fizikai hozzáférés védelem (belépés és mozgás ellenőrzés, behatolás védelem)			
Fizikai rendelkezésre állás biztosítása biztonsága	Erőforrás és rendszer fizikai háttér biztosítás, tűzvédelem, kisugárzás védelem, energiaellátás folyamatossága	← Az előző + a termelő rendszer specifikus rendelkezésre állás biztosítása		Erőforrás és rendszer háttér biztosítás, tűzvédelem, kisugárzás védelem, energiaellátás biztosítása
Logikai hozzá-Férés védelem	Logikai belépés és behatolás védelem	← Az előző + a termelő rendszer specifikus hfv.		Logikai belépés, és behatolás védelem
Logikai Rend. állás biztosítása	Erőforrás és rendszer logikai háttér biztosítás, ki- és besugárzás védelem	← Az előző + termelő rendszer specifikus logikai rendelkezésre állás biztosítása		Erőforrás és rendszer logikai háttér biztosítás, ki- és besugárzás védelem
Az életciklus Védelem	A teljes életciklus alatt a biztonsági követelmények biztosítása			
Hálózatok védelme	A hálózat és a továbbított adatok védelme	A termelési rendszeren továbbított félkész és kész termékek védelme		A hálózat és a továbbított adatok védelme

1.6. A BIZTONSÁGI RENDSZER ÜZEMELTETŐI

SZERVEZÉSI BIZTONSÁG

- ***Szervezet és működés szabályozása*** — ***Titkárság***
- ***Biztonságszervezési dokumentumok*** — ***Biztonsági vezető***
- ***Titok (adat) védelem szabályozása*** — ***Titkárság***
- ***Iratkezelés szabályozása*** — ***Titkárság***
- ***Humán politika*** — ***Humán erőforrások vezető***
- ***Szerződések (Kockázat áthárítás)*** — ***Gazdasági vezető***

TECHNIKAI BIZTONSÁG

⇒ ***Fizikai biztonság***

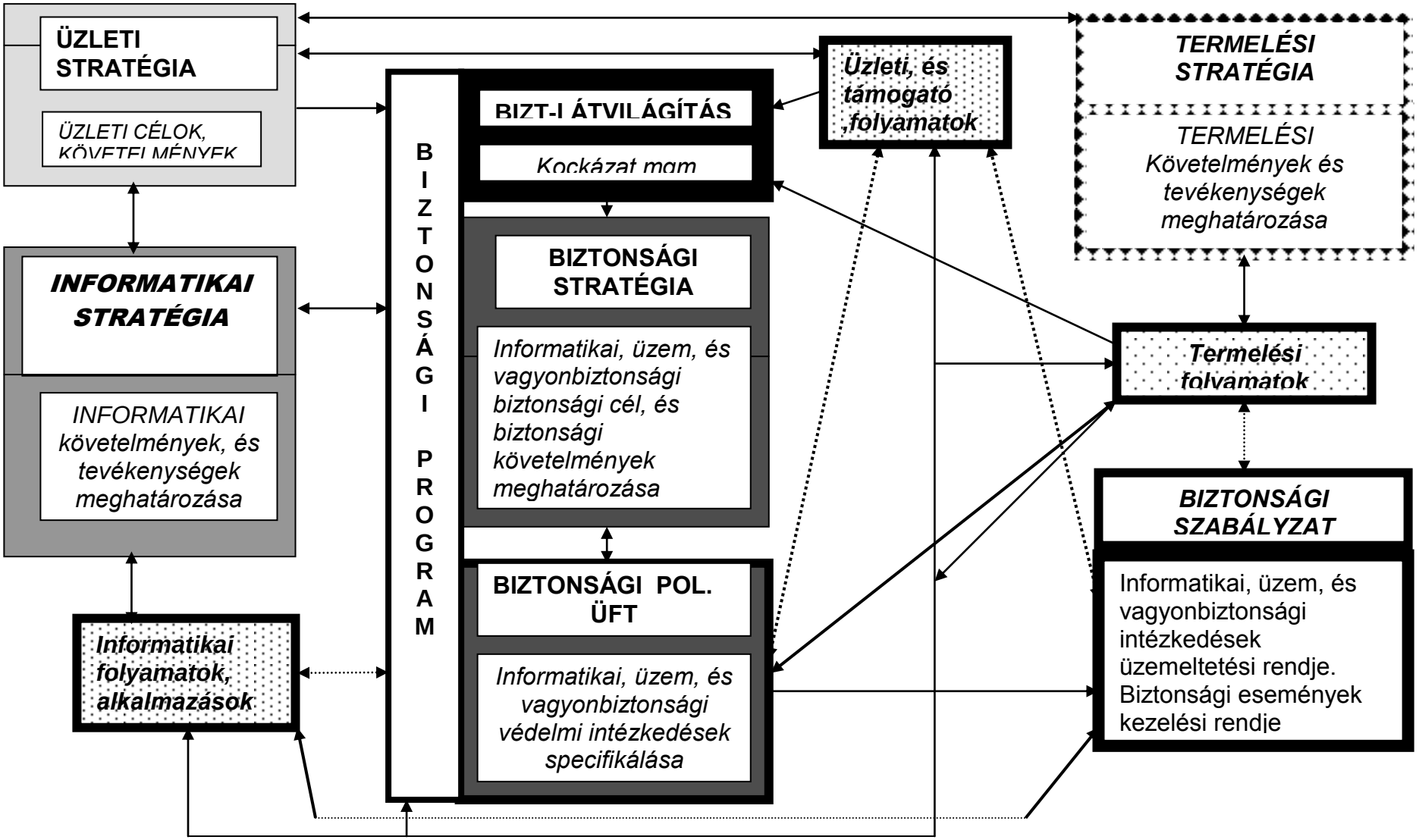
- ***Hozzáférés védelem*** — ***Vagyonbiztonsági vezető***
- ***Rendelkezésre állás*** — ***Vagyon bizt. vezető***

⇒ ***LOGIKAI BIZTONSÁG***

- ***Hozzáférés védelem*** — ***inf.-i biztonsági vez.***
- ***Rendelkezésre állás*** — ***„***
- ***Hálózati védelem*** — ***„***
- ***Védelem az életciklus során*** — ***„***

ÜZEMBIZTONSÁG — ***üzembiztonsági vez.***

AZ ÜZLETI, TERMELÉSI, AZ INFORMÁCIÓ, ÉS A BIZTONSÁGI RENDSZER ÖSSZEFÜGGÉSEI



1.7. A MÓDSZERTAN FOGALMA

*A **módszertan** bizonyos eredményhez elvezető eljárás, a szervezet tevékenységeinek, és azok egymástól való függősége (tartalmi, és végrehajtási feltételei) rendjének meghatározása.*

*A **biztonságszervezési módszertan** a szervezet tevékenységei, erőforrásai bizalmassága, sértetlensége, és rendelkezésre állása optimális biztosítására irányuló eljárás (irányítás, és ellenőrzés) rendje.*

*Az **ISMS** a biztonság szervező tevékenységének módszertana, amelynek sikeres felhasználásához a biztonságtechnika alapismeretei is szükségesek.*

1.8. AZ ISMS, ÉS AZ MSZ-ISO/IEC 1779

Az ISMS az MSZ-ISO/IEC 17799-ben szereplő védelmi intézkedéseket a 10.sz Tájékoztatóban megadott táblázat szerinti pontokban tartalmazza.. Figyelembe kell azonban venni, hogy az ISMS jóval szélesebb körben, a teljes vállalati biztonsággal foglalkozik, valamint a struktúrája más hatékonyabb filozófiára épül. Ezért az ISMS szerint végzett biztonságszervezés megfelel az MSZ-ISO/IEC 17799-nek, de nem azonos tartalmú, és felépítésű. Amennyiben egy Megrendelő ragaszkodik az MSZ ISO/IEC 177999- szerinti felépítéshez, akkor szemben az ISMS-mel

- *A Kockázat menedzsmentet célszerű, szűkebb körben, mint az ISMS elkészíteni.*
- *Biztonsági Szabályzatot kell készíteni (az ISO/IEC 17799 magyar fordítása a Security Policyt Biztonsági Szabályzatnak fordítja).*
- *Ez a gyakorlatban annyit jelent, hogy egy szabályzatba kell foglalni az ISMS szerinti Biztonsági Stratégiát, Biztonsági Politikát, és Biztonsági Szabályzatot.*
- *Ebből az következik, hogy egy védelmi intézkedés egyszer kell szerepeljen, amikor is mind a B. Politikában, mind a B. Szabályzatban megadott ismérvek a védelmi intézkedésről együtt szerepelnek.*

Az MSZ-ISO/IEC 17799 szerinti BIZTONSÁGI SZABÁLYZAT tartalmi vázlatának fő pontjai:

- A biztonsági cél, a vállalat vezetésének elkötelezettsége,
- A biztonsági követelmények,
- A védelmi intézkedések specifikálása, és üzemeltetésük szabályai,
- Az Informatikai Biztonság irányítása,
- Az Informatikai Biztonság struktúrája,
- A biztonsági tudatosság erősítése, az oktatás,
- A biztonsági események kezelésének rendje,
- A BSZ karbantartásnak rendje,
- A BSZ belső, és külső auditálása.

1.9. AZ ITIL, AZ MSZ-ISO/IEC 17799, ÉS A COBIT 4.1

A szerző figyelembe vette, hogy hazánkban több gazdasági szervezetnél alkalmazzák az ITIL, BS 7799 (BS=British Standard), vagy az MSZ-ISO/IEC 17799, és a COBIT 4.1 ajánlásokat, szabványokat. Ezek célja, illetve tárgya a következőképen írható le:

ITIL: Az Information Technology Infrastructure Library, meghatározza, az IT *szervezeti struktúrát, egy IT szervezet gyakorlati követelményeit, és a tevékenység menedzsment szabványokat, amelyek lehetővé teszik a szervezet számára az IT szolgáltatások, és a kapcsolódó IT infrastruktúra menedzselését. (AZ ITIL, az ITIL Foundation meghatározása szerint)*
A Gartner GROUP (2002) szerint: az ITIL egy nyilvános, gyártó független keretrendszer, az IT szolgáltatások irányítására.
Az ITIL megjelent angol szabványként a BS 15000, és magyar elő szabványként MSZE 15100), mint az IT szolgáltatás menedzsment szabványa, amely meghatározza az IT menedzsment folyamatokat az ITIL keretrendszer alapján. Végeredményben az ITIL az IT szolgáltatások minőségjavítására is szolgál.
Feltétlenül figyelnünk kell arra, hogy a BS 15000 szabvány maga azt mondja, hogy az ITIL-nek megfelelő BS 15000 szabvány nem biztosít BS 7799 megfelelősséget, ezzel szemben a BS 7799 biztosít BS 15000 megfelelősséget.

Az ITIL háromfokozatú minősítést ad az azt ismerő, alkalmazó szakemberek számára. Az ISACA pedig CISA (információs rendszer auditor), és CISM (informatikai biztonsági szakértő) minősítéseket ad, amelyet több ezer auditor szerzett meg, és használ a világon. Hazánkban ma már CISA minősítése van több, mint 150 auditornak, és egyre nő CISM minősítések száma. A jelentősebb hazai cégek csak CISA, CISM minősítettek által aláírt auditálási anyagokat fogadnak el, már hazánkban is. Megszerezhető ezen kívül CRISC (kockázat és Információs Rendszer ellenőrzés) és CEGIT (vállalatirányítás) minősítés is.

Angol IT biztonsági szabványok:
Az alábbi szintén Angliában kidolgozott, az informatikai biztonság menedzsment eljárások, szabványok:

- *BS7799:1995. Code of practice for Information Security Management.*
- *BS7799-1,2000. Information technology — Code of practice for information security management (MSZ ISO/IEC 27001).*
- *BS7799.-2, 2002. Information security management systems — Specification with guidance for use.*
- *BS17799-2002. Code of practice for Information Security Management, amelyből lett az ISO, majd a hazai szabvány*

.Az MSZ ISO/IEC 17799: 2006 *Információtechnika. Az informatikai biztonság menedzselésének az eljárás rendje, a BS 17799, ISO szabvány változatának, magyar megfelelője.*

A COBIT 4.1 *a CONTROL OBJECTIVES for INFORMATION and RELATED TECHNOLOGY, az Information System Audit and Control Association, az ISACA, az Információs rendszer Ellenőrök Nemzetközi Szövetsége kiadványa, amely folyamatosan fejlesztés alatt ál, négy szakterületen, 34 folyamatban, több mint*

háromszáz magas szintű auditálási szempontot tartalmaz az információs rendszer auditorok számára. A COBIT a informatika irányítás, és ellenőrzés a legjobb gyakorlat szerinti meghatározása. .

Ezeket összehasonlítva:

***Az ITIL** tehát az IT biztonság menedzsment keret rendszere, és alkalmazása az IT szolgáltatások minőségjavítására.*

***Az MSZ-ISO/IEC 17799** az informatikai biztonság menedzsment szabványa, amelynek betartásával lehet az IT biztonsági rendszert megteremteni.*

***A COBIT 4.1** az IT technológia ellenőrzésének, auditálásának magas szintű ellenőrzési céljait (és ezzel a megvalósítandó követelményeket is) adja meg, ahol alpontonként szerepelnek a biztonsági ellenőrzési célok is. Alkalmazása alapját képezheti az IT biztonság irányításának, és auditálásának, de egyben az IT biztonsági követelmények is megállapíthatók az egyes ellenőrzési célokból.*

A BIZTONSÁG szempontjából tehát, az MSZ-ISO/IEC megfelelősség, és a COBIT 4.1 (amely az ITIL-t is alkalmazza) megfelelősség az IT biztonság vonatkozásában meghatározó.

*Mindehhez hozzájárul, hogy a biztonságtechnikában is néhány éve követelmény lett a best practice (legjobb gyakorlat) alkalmazása, amely ma a konkrét informatikai biztonsági feladatok tekintetében az MSZ-ISO/IEC 27001, és az MSZ-ISO/IEC 17799, és a COBIT 4.1 megfelelősséget jelenti, ezért ezt hazánkban is egyre inkább megkövetelik Egyes vállalatok tévesen egy korábbi BS szabvány megfelelősséget, írnak elő (a BS 7799-et). Megjegyezzük, hogy az ITIL megfelel az IT szolgáltatások legjobb gyakorlat alapján történő biztosítása követelményének, például az ISO 9000 minőségbiztosítási tanúsításnál. **A szerző a az ISMS-ben biztosítja az MSZ-ISO/IEC 17799, és COBIT 4 megfelelősséget,** amely, elfogadva a BS 15000 meghatározását, azt jelenti, hogy így megfelel az ITIL-nek is.*

1.10. INFORMATIKAI BIZTONSÁG MENEDZSMENT RENDSZER, ÉS AZ ISMS

Az Information Security Management System (ISMS) az ISO/IEC 27001:2005 szabványban került specifikálásra. Az alábbiakban röviden összefoglaljuk a szabvány lényegét, és a módszertan megfelelősségét a szabványnak.

AZ ISMS célja

Az ISMS célja egy modell kialakítása, a biztonsági rendszer megalapozására, megvalósításra, működtetésére, megfigyelésére, jelentésére, karbantartásra, és fejlesztésére. Ez a modell a biztonságszervezés (és így az ISMS módszertan) keretrendszere. A szabvány szerint az ISO/IEC 17799: 2005. szabvány nélkülözhetetlen az ISMS alkalmazásához, és az MSZ-ISO/IEC 17799-es szabványnak az ISMS megfelel. A szabvány Mellékletében megadott ellenőrzési célok, az ellenőrzendő biztonsági intézkedések, az ISMS módszertan alapú biztonságszervezés tárgyai. Az ISMS a PDCA modellt alkalmazza, amely a következő:

PLAN (tervezés)
Az ISMS politika, célok, folyamatok, és eljárások megalapozása (a Biztonsági Stratégia végrehajtására), a kockázat menedzsment alapján, az informatikai biztonság fejlesztési eredmények elérésére.

DO (megvalósítás)
Az ISMS politikák, célok, folyamatok, és eljárások megvalósítása, és működtetése.

CHECK (ellenőrzés)
A folyamatok teljesítményének, értékelése, ahol lehet mérése az ISMS politika, célok, és a gyakorlati tapasztalatok alapján, és a menedzsment tájékoztatása.

ACT (intézkedés)
Javító, és megelőző akciók az ISMS belső ellenőrzése, és a menedzsmentnek adott jelentés, illetve más relevans információk, az ISMS folyamatos fejlesztése érdekében.

A PDCA modellnek az ISMS-ben, az IT biztonsági programban foglaltak felelnek meg, éspedig

PLAN ➔*Kockázatfelmérés, Veszélyforrás elemzés, Védelmi intézkedések specifikálás (kockázat mgm), Szervezet, és Működésszabályozás, Biztonsági Program,*
DO ➔*Fejlesztés/beszerzés, Implementálás,. Üzemeltetés, Karbantartás (életciklus intézkedések),*
CHECK ➔ *Ellenőrzés (életciklus intézkedés),*
ACT ➔ *Intézkedés az ellenőrzés és/vagy biztonsági esemény alapján.*

1.11. AZ ISMS FELÉPÍTÉSE

Az ISMS, a fentieknek megfelelően, az IT biztonsági programon belül, a következő biztonsági dokumentumokkal elkészítésével, karbantartásával foglalkozik:

- ⇒ *Kockázatfelmérés (amely része a Kockázat menedzsmentnek),*
- ⇒ *Veszélyforrás elemzés (amely része a Kockázat menedzsmentnek),*
- ⇒ *Kockázat értékelés*
- ⇒ *Biztonsági Politika (Biztonsági Stratégia),*
- ⇒ *Katasztrófaterv,*
- ⇒ *Biztonsági Szabályzat, és*
- ⇒ *Biztonság belső ellenőrzése*

***A kockázat menedzsment** a Kockázat menedzsmentből (kockázatok meghatározása), és a Biztonságpolitikai koncepcióból áll (kockázatok csökkentésére teendő védelmi intézkedések).*
Az ISMS külön fejezetben tárgyalja az egyes végtermékek készítésének szempontjait, és a végtermékek tartalmi felépítését.
Az ISMS a Mellékletben meghatározza a biztonságtechnikai alapfogalmakat (és azok angol nyelvű megfelelőjét), és megad egy széles körű irodalomjegyzéket, valamint ismertetést ad a nemzetközi biztonságértékelési szabványról (Common Criteria).
Amennyiben a megbízás csak az információ-rendszerre vonatkozik a végtermékek tartalmi ismertetéseiben csak az informatikára vonatkozó részeket kell felhasználni..

Az ISMS értelemszerűen az üzembiztonsággal nem foglalkozik, mint iránymutatás azonban az üzembiztonság szervezésénél is használható.

Az alkalmazott rövidítések: ÉR=értékrendszer, ÜR=üzleti rendszer, TR=termelési rendszer, IR=információ-rendszer, hfv=hozzáférés -védelem, rsw=rendszerszoftver, asw=alkalmazói szoftver.

A felsorolásoknál alkalmazott jelölés hierarchia:

- *1.szint*
  - ⇒ *2.szint*
    - ➢ *3..szint*

1.12. A BIZTONSÁGSZERVEZÉS ETIKAI KÖVETELMÉNYEI

A biztonságszervező egy vállalat titkait ismeri meg, és tevékenységének célja e titkok védelmének biztosítása. Mindez igen szigorú etikai követelményeket támaszt a biztonságszervezővel szemben. Az alábbiakban ezeket az etikai követelményeket adjuk meg, az információrendszer ellenőrök (ISACA) etikai követelményeinek felhasználásával.

A BIZTONSÁGI RENDSZERSZERVEZŐ ETIKAI KÖVETELMÉNYEI:

- ***Meg kell őriznie függetlenségét.***
- ***Korrekt, és tárgyilagos módon kell végeznie tevékenységét, kerülnie kell az olyan helyzeteket, amelyek fenyegetik a függetlenségét.***
- ***Nem vehet részt illegális vagy nem korrekt tevékenységben.***
- ***Védenie kell a feltárt információk bizalmasságát.***
- ***Magas követelményeket kell, magatartását, és jellemét illetően maga elé állítania mind a szakmai, mind a magán életében.***
- ***Szakmai kompetenciája alapján kell megközelítenie a kapcsolódó szakterületeket.***
- ***Elegendő ténnyel kell a következtetéseit, és a javaslatait alátámasztania.***

2. A VÁLLALATI KOCKÁZAT MENEDZSMENT

A vállalati kockázat menedzsment (ERM) egy vállalatirányítási folyamat, a vállalati stratégia kidolgozáshoz, és a vállalatot átfogóan a szervezetre hatást gyakorló potenciális események azonosítására, és a kockázatok menedzselésére a szervezet kockázati étvágyán belül, a szervezet céljai elérésének ésszerű biztosítására.(COSO [62]).

A vállalati kockázatok táblázata a következő oldalon található.

A menedzsmentnek fel kell ismernie, hogy bizonytalanságok léteznek, amelyekből nem tudhatja bizonyosan mikor fognak események bekövetkezni. Az események azonosításának részeként külső, és belső tényezőket (veszélyforrásokat, fenyegetésforrásokat) vesz figyelembe, amelyek hatása eseményt idézhet elő.
A vállalati szintű kockázatok (külső, és belső) között a belső működési kockázatok része a biztonsági kockázat.

A bizonytalanság *a jövő eseményei valószínűsége, és hatása előre ismeretének képtelensége (inability) [62].*

A kockázat menedzsment tehát módszeres megközelítés, a legjobb gyakorlatnak megfelelő tevékenység meghatározásra, a kockázatoknak az azonosítására, megértésére, az intézkedésre, és a kommunikálására [64].

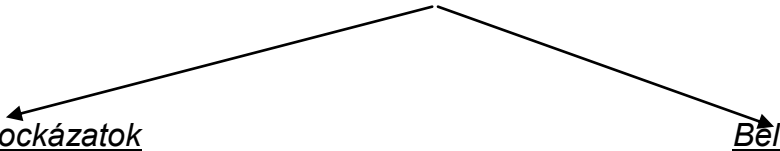
A biztonsági kockázatok (a vállalati kockázatokon belül) menedzsmentje az alábbiak szerint hajtandó végre, a biztonságszervezési folyamatban (lásd 1. 1.5.), a Kockázat menedzsment keretében:

- ⇒ Kockázatfelmérés
- ⇒ Kockázat azonosítás, veszélyforrás elemzés
- ⇒ Kockázat értékelés
  - ➢ Bekövetkezési valószínűség meghatározása
  - ➢ Sebezhetőség, kárkövetkezmény, üzleti hatás meghatározása
  - ➢ Kockázat meghatározása, a kockázati étvágy, és tűrőképesség figyelembevételével,
- ⇒ Védelmi intézkedésekre javaslat
  - ➢ Költséghatékonyság elemzés
  - ➢ Maradék kockázat meghatározása
- ⇒ A menedzsment döntése
- ⇒ Dokumentálás

A biztonsági kockázat menedzsment folyamatos tevékenység, amelyet végrehajtása után az esetleg bekövetkező biztonsági eseményeket követően, az érintett kockázatokra újra végre kell hajtani, illetve a teljes rendszerre, vállalatra pedig, legalább kétévenként meg kell ismételni.

KOCKÁZATI TÁBLÁZAT

VÁLLALATI SZINTŰ KOCKÁZATOK



Külső kockázatok

- *Gazdasági (pénzügyi [hitel, likviditás], tőke)*
- *Üzleti,*
- *Természeti, környezeti,*
- *Szociális,*
- *Politikai, és*
- *Humán kockázatok*

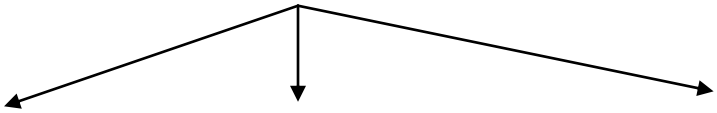
Belső kockázatok

- *Folyamat,*
- *Humán,*
- *Infrastruktúra,*
- *Technológiai*
- *Megfelelőségi kockázatok*

KOCKÁZATOK A RENDSZEREKBEN

ÜZLETI RENDSZER	TERMELÉSI RENDSZER	INFORMÁCIÓS RENDSZER
Üzleti kockázatok (bank)	Termelési kockázatok	Informatikai kockázatok
-pénzügyi (likvidítási)	-technológiai	-beruházási
-piaci (piaci)	-vállalati	-biztonsági
-hírnév (hírnév)	-fejlesztési	-projekt
-jogi (jogi)	-tulajdonjogi	-infrastrukturális
-működési (működési)	-szerződési	-megbízhatósági
-rendszeres (átutalási)	-működési	-működési
(kamat)		
(hitelezési)		
(megfelelőségi)		
(rendszeres)		

KOCKÁZATOK A BIZTONSÁGI ALRENDSZEREKBEN



Vagyon bizt. alrendszer — Üzembizt. alrendszer — Informatikai bizt. alrendszer

----Funkcionális: szervezési (admin, humán), technikai (fizikai, logikai, életciklus, hálózati),

----Garanciális: kikényszerítés, teljes körűség, életciklus, biztonsági esemény, és konfigurációkezelés, számon kérhetőség.

2.1. A KOCKÁZAT MENEDZSMENT FÁZISAI

A kockázat menedzsment három fázisa

- ⇒ *a kockázatfelmérés,*
- ⇒ *a kockázat azonosítás, veszélyforrás elemzés, és*
- ⇒ *kockázat értékelés.*

A kockázat menedzsment alapvető tevékenységei a következők:

- ⇒ *a biztonsági környezet, és a működő védelmi intézkedések feltárása,*
- ⇒ *a kockázatok azonosítása, a veszélyforrások elemzése*
  - ➢ *a védelmi intézkedések megfelelősségének értékelése,*
  - ➢ *a védelmi intézkedések végrehajtásának értékelése.*
- ⇒ *a kockázat értékelés*
  - ➢ *a veszélyforrások által képzett kockázatok szintjének megállapítása,*
  - ➢ *a rendszer biztonsági minősítése.*
- ⇒ *A biztonság színvonalának mérése, értékelése*

A kockázat menedzsment módszertana, az INFORMATION SYSTEM AUDIT AND CONTROLL ASSOTIATION (ISACA) által kidolgozott módszertani irányelvek, a COBIT 4.1 felhasználásával készült (lásd irodalomjegyzék).

Az információ-rendszerek átvilágítási szempontjait magas szinten, beleértve az informatikai kockázat menedzsment is, a COBIT4.1 tartalmazza. A kockázat menedzsment készítőinek célszerű világosan látni, hogy az informatikai kockázat menedzsment az információ-rendszer általános átvilágításának részét képezi. A 3. fejezet pedig a kockázat menedzsment részletes szempontjait (ellenőrzési lista) tartalmazza, amely a COBIT 4.1-ben megadott kockázat menedzsmenti szempontok felhasználásával készült.

Az ISACA kiadványa, a CISA REViEW MANUAL 98 alapján a biztonsági auditálásra (átvilágításra) is érvényes fogalmakat az alábbiakban ismertetjük:

Az audit

- ⇒ *Az* **auditálás** *(general audit) a kockázatok felismerésére, és mérséklésére a folyamatokba beépített* ***kontroll-****intézkedések, és megvalósulásuk feltárása, és értékelése .*
- ⇒ *Az auditornak elsősorban meg kell értenie az* auditálás tárgyát *képező szervezetet.*
- ⇒ Az auditálás történhet
  - ➢ *a megfelelősség vizsgálatával (compliance testing), és*
  - ➢ *a megvalósulás vizsgálatával (substantive testing).*
- ⇒ *Egy szervezet biztonsága szempontjából alapvető, ezért fel kell tárni a szervezet üzleti tevékenységéből következő kockázatot (business risk).*
- ⇒ *Az auditálás maga is kockázatokkal jár (overall audit risk).* Az auditálás kockázati kategoriái:
  - ➢ *Eredendő kockázat (inherent risk) független az audittól,*

- *Kontroll kockázat (control risk) a kontroll rendszerben nincs megelőzés vagy jelzés,*
- *Feltárási kockázat (detection risk) az auditor nem ismeri fel.*

⇒ Az auditálás folyamata*:*

- *az auditálás tárgyának (a területnek) a meghatározása,*
- *az auditálás céljának a megjelölése,*
- *az auditálás előkészítése,*
- *az auditálás végrehajtása,*
- *az auditálási jelentés készítése,*
- *a követés.*

⇒ Az auditálás lehet

- *pénzügyi (a pü.-i rekordok, és számadások korrektségének ellenőrzése),*
- *működési (a kontroll rendszer ellenőrzése),*
- *komprehenzív (az előbbi kettő együtt).*

A kontroll

⇒ *A* **kontroll** *az ésszerű garanciák biztosítására, és a nem kívánt események megelőzésére, jelentésére, valamint kijavítására tervezett politikák, folyamatok, gyakorlat, és szervezeti struktúra.*

⇒ A kontroll célja *egy kívánt eredmény vagy szándék megállapítása, amely az egyes IT folyamatokba implementált kontroll folyamtokkal érendő el.*

⇒ A kontroll célja lehet:

- *a belső elszámolás ellenőrzése (internal accounting control's),*
- *működési ellenőrzések (operational cont's), és*
- *adminisztratív ellenőrzések (administrative cont's),*

továbbá ezek a következőket foglalhatják magukba:

- *erőforrások védelme,*
- *a vállalati, és jogi követelményeknek való megfelelés,*
- *az input hitelesítés,*
- *a feldolgozási folyamatok pontossága, és teljessége,*
- *az outputok,*
- *a folyamatok megbízhatósága.*

⇒ Az információ-rendszer kontroll célja lehet*:*

- *az információk védelme a jogosulatlan hozzáféréstől, és a védelem naprakészsége,*
- *minden adat hitelesített-e, és csak egyszer kerül-e a rendszerbe,*
- *minden visszautasított tranzakció jelentésre kerül-e,*
- *a duplikált tranzakciók jelentésre kerülnek-e,*
- *a file-nak van-e megfelelő háttere a visszaállításhoz,*
- *minden sw csere jóváhagyásra, és tesztelésre kerül-e,*

⇒ A kontroll jellege szerint lehet

- *megelőző (preventív), pl. feladat szétválasztás, hozzáférés-védelem,*
- *feltáró (detective) pl. hash total, naplózás,*
- *javító (corrective) pl. katasztrófaterv, újrafuttatási folyamatok,*

továbbá mind a három lehet:

- *alap (basic) kontroll (programozási módszerek, back up and recovery procedures),*
- *fegyelmező (disciplinary) kontroll (feladat szétválasztás, tranzakciók hitelesítése).*

⇒ A kontrollokat megkülönböztethetjük a szerint is, hogy más kontrollokhoz mi a viszonyuk, *éspedig*

- *kompenzációs kontroll (compensating control), amikor egy kontroll gyengeségének kockázatát egy másik kontroll csökkenti, pl. audit trail, batch control total reconciliation, independent review,*
- *átfedő kontroll (overlapping control), amikor egy erős kontrollt, egy másik erős kontroll egészít ki, pl. kártyás belépés ellenőrzés plusz élőerő.*

A kockázat menedzsmentnél kontroll alatt védelmi intézkedéseket értünk. A kockázat menedzsment a megfelelősség, és megvalósulás vizsgálatát jelenti, és jellegét tekintve megelőző. A védelmi intézkedések, pedig lehetnek megelőző, feltáró, és javító jellegűek.

2.2. A KOCKÁZATFELMÉRÉS

A kockázatfelmérés célja a biztonsági környezet feltárása, és rögzítése. Ennek keretében fel kell tárni

- ⇒ *az erőforrásokat (az erőforrások meghatározását lásd 1.1.3.-ban),*
- ⇒ *a működő védelmi intézkedéseket, és*
- ⇒ *az időközben fellépett új veszélyforrásokat.*

2.3. A KOCKÁZATFELMÉRÉS VÉGREHAJTÁSA

2.3.1. A kockázatfelmérés módszere

A kockázatfelmérés folyamatábrája a következő oldalon található. A kockázatfelmérés a következő főbb tevékenységekből áll:

- ⇒ *az ellenőrzési listák adaptálása,*
- ⇒ *interjúk készítése,*
- ⇒ *dokumentumok tanulmányozása, és*
- ⇒ *szemlék.*

2.3.2. Ellenőrzési lista

A kockázatfelmérés megkezdése előtt rendelkezésre állnak az átvilágítás általános ellenőrzési szempontjai. Az általános ellenőrzési szempontokat az átvilágítás megkezdése előtt adaptálni kell. A védelmi intézkedéseknek az átvilágításához fel kell használni a 11.3.3. pontban megadott, védelmi intézkedések köre tárgyú táblázatot. Az általános ellenőrzési lista adaptálása az alábbi lépésekből áll.

- ⇒ *1. Lépés. Megközelítés*

A következő anyagokat kell a biztonsági rendszerszervezőnek megismernie:

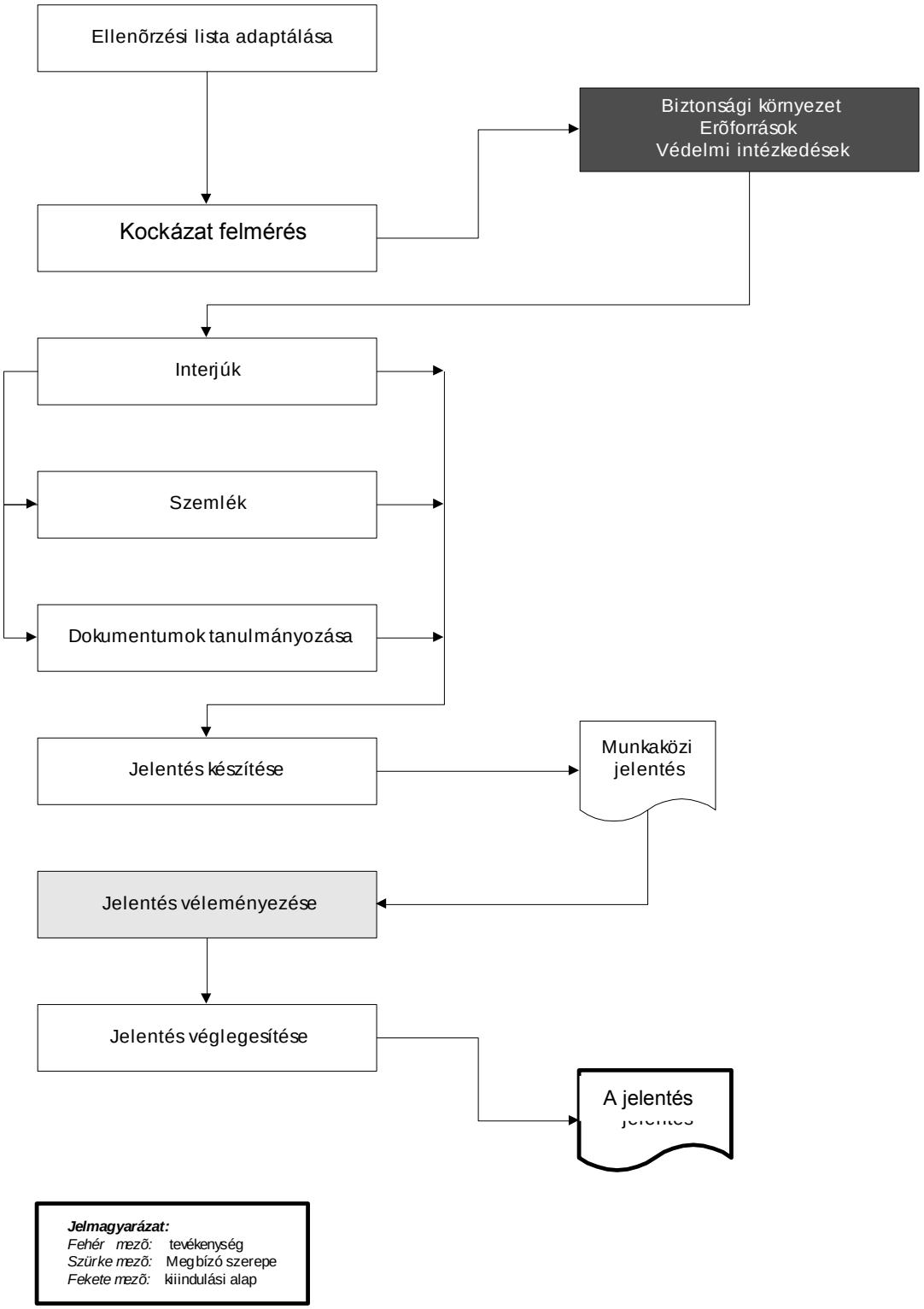
- ➢ *üzleti (igazgatási szervezetnél küldetésből adódó) követelmények,*
- ➢ *szervezet és működés,*
- ➢ *jogszabályok, szabályzatok,*
- ➢ *erőforrások,*
- ➢ *alkalmazott védelmi módszerek,*
- ➢ *biztonság menedzsment, és*
- ➢ *biztonsági dokumentumok (korábbi kockázat menedzsmenti jelentés, Biztonsági Politika, ÜFT, Biztonsági Szabályzat, és biztonsági események naplói)*

- ⇒ *2. Lépés. Alkalmazás*

A következőket kell végrehajtani:

- ➢ *az általános ellenőrzési lista alkalmazása a kijelölt átvilágítási területre (ÜR és /vagy IR),*

A KOCKÁZATFELMÉRÉS FOLYAMATÁBRÁJA



- *a tanulmányozandó dokumentumok meghatározása,*
- *a mintavétel elve alapján szervezeti egységek kijelölése, és*
- *az interjú alanyok kijelölése.*

⇒ *3. Lépés. Specifikálás*

A következőket kell az ellenőrzési listán átvezetni:

⇒ *szektor specifikus követelmények,*
⇒ *szabványok,*
⇒ *megvalósítás specifikus követelmények (pl. informatikánál: platformfüggő követelmények).*

2.3.3. Dokumentumok

A Megbízónak az átvilágítás megkezdésekor az alapvető dokumentumokat rendelkezésre kell bocsátani, valamint az átvilágítás során felmerülő további eseti dokumentum igényeket is biztosítania kell. Az induláskor rendelkezésre bocsátandó dokumentumok a következők (amelyeknek tartalma, és védelme vizsgálandó):

⇒ *Üzleti stratégia (igazgatási szervezetnél küldetés)*
⇒ *Informatikai stratégia*
⇒ *Szervezeti és működési szabályzat,*
⇒ *Iratkezelési utasítás,*
⇒ *Adatvédelmi Szabályzatok,*
⇒ *Titokvédelmi utasítás,*
⇒ *Tűzvédelmi szabályzat,*
⇒ *Polgári védelmi szabályzat,*
⇒ *biztonsági dokumentumok (korábbi átvilágítási jelentés, Biztonsági Politika, Katasztrófaterv, Biztonsági Szabályzat, Konfigurációkezelési Utasítás, Programváltozás kezelési eljárás rend, biztonsági események kezelési rendje, és naplói), és*
⇒ *Információ-rendszer dokumentációi (rsw, asw-ek, stb)*

A kockázatfelméréshez felhasznált dokumentumok jegyzékét az Átvilágítási jelentésben rögzíteni kell.

2.3.4. Interjúk

A kockázatfelmérés egyik fontos eszköze az interjúkészítés. Ennek alapja az ellenőrzési lista. A több egységgel rendelkező szervezetek esetében az átvilágítás a mintavétel elve alapján történik. A különböző szintű szervezeti egységekből legalább egynek a mintában szerepelni kell. Az interjú alanyok első megközelítésben a következők:

⇒ *a. top menedzsment vizsgált területért felelős tagja,*
⇒ *a humánpolitikai vezető,*
⇒ *a biztonsági vezető (vagyon és az IT biztonságért felelős),*
⇒ *a titokvédelemi felelős,*

⇒ *az iratkezelésért felelős vezető,*
⇒ *az informatikai vezető,*
⇒ *az informatika fejlesztésért felelős vezető,*
⇒ *az informatika üzemeltetéséért felelős vezető,*
⇒ *a beszéd és adattávközlésért felelős vezető,*
⇒ *az átvilágításba bevont egységek vezetői,*
⇒ *az ÜR-ben alkalmazott berendezések, eszközök üzemeltetésért felelős vezető.*

Az interjúk során tett megállapításokat az átvilágítónak saját részére rögzítenie kell, továbbá az Átvilágítási jelentésben szerepeltetni kell az interjút adó személyek nevét, és beosztását.

2.3.5. Szemlék

Az átvilágítás szerves részét képezi az erőforrások, és a védelmi intézkedések üzemeltetésének helyszíni tanulmányozása. A szemlék tárgya a technikai védelmi intézkedések üzemeltetési gyakorlatának feltárása. A szemlék tárgyát, és helyét a 2.4.2.ben ismertetettek szerint kell meghatározni. A szemléknél alkalmazható módszerek a következők:

⇒ *megfigyelés, amely történhet*
① *helyszínbejárással,*
② *az üzemeltető által működés közben bemutatott védelmi intézkedés megtekintésével,*

⇒ *tesztelés, amely történhet*
③ *a védelmi intézkedés megkerülési kísérletével,*
④ *védelmi intézkedés feltörési kísérlettel,*
⑤ *ellenőrző programmal (Computer Assisted Audit Techniques, pl. Internet, és bizalmas számítástechnikai bázis scannerek),*
⑥ *méréssel.*

Az egyes módszerek például a következő védelmi intézkedéseknél alkalmazhatók:

① *belépés, és mozgás ellenőrzés,*
behatolás védelem,
logika hfv. biztonsági környezete,
fizikai rendelkezésre állás (mentések, eredeti programok, forrásnyelvi változatok tárolása),
② *belépés, és mozgás ellenőrzés,*
logikai jelszavas hfv.,
tartalom hitelesítés,
rejtjelezés,
③ *belépés, és mozgás ellenőrzés,*
logikai jelszavas hfv.,
④ *belépés, és mozgás ellenőrzés,*
logikai jelszavas hfv.,
⑤ *logikai jelszavas hfv.,*

mentések,
- akusztikus kisugárzás,
elektromágneses kisugárzás.

2.4. A KOCKÁZAT FELMÉRÉSI JELENTÉS ELKÉSZÍTÉSE

2.4.1. A jelentés felépítése

A kockázat felmérési jelentés felépítése, tartalma az 5. fejezetben található. Az egyes pontok meghatározzák az átvilágítás során feltárandó témákat, területeket. A jelentés készítésének időszakára biztosítani kell a további interjúk, szemlék, illetve dokumentumok tanulmányozásának a lehetőségét.
A teljes vállalat kockázat felmérésének elkészítése esetén az erőforrások felmérését az üzleti rendszerre (ÜR), és az információ-rendszerre (IR) nézve is el kell végezni. Az üzleti rendszer erőforrásai az adott vállalattól nagymértékben függnek. Az üzleti rendszer erőforrásai felmérési szempontjainak a kidolgozására csak az adott vállalat alaptevékenységének ismeretében kerülhet sor. A bankoknál jelentős technológia (pl. pénzfeldolgozás) alkalmazása történhet az üzleti rendszerben. Kereskedelmi vállalatoknál pedig jelentős logisztikai erőforrások lehetnek. Felhívjuk a fegyelmet arra, hogy egy termelő vállalat esetében a termelési technológia az üzembiztonság keretébe tartozik, itt tehát nem foglalkozunk vele.
A kockázat felmérésnek az erőforrás feltárásból kell kiindulnia, ezért azt kell először elvégezni.

2.4.2. A Megbízó szerepe

A Megbízónak a Kockázat felmérési Jelentést (a megfelelősségét a tényeknek) jóvá kell hagynia, mivel az képezi a további munka alapját. Ebből következik, hogy a Jelentés módosítására időt kell biztosítani. A Megbízónak tehát a tények alapján teljes körű kifogásolási joga van, illetve az átvilágítónak elemi érdeke elnyerni a Megbízó egyetértését, amelyről a Megbízótól ELFOGADÁSI NYILATKOZATOT kell kérni, és azt a Kockázat felmérési Jelentéshez csatolni kell, amely a megállapított tényeket bizonyítékként támassza alá, az auditorok kötelezettsége szerint.

Az elfogadó nyilatkozat célszerű, ha a következőket tartalmazza (Minta):

ELFOGADÁSI NYILATKOZAT

A …… vállalat biztonságért is felelős, vezetőjeként kijelentem, hogy a Kockázat felmérési Jelentésben foglaltak,

- *a biztonságért felelős (lásd mellékletben) munkatársakkal készített interjúkon,*
- *a vállalat (a mellékletben megadott) szabályzatain, és*
- *a folyamatok szemléin alapulnak.*
- *A ……..-án tartott egyeztetésen, a vitás kérdések tisztázása, majd az anyagon történt átvezetése megtörtént.*
- *Nincs tudomásom olyan, a vizsgálat tárgyával kapcsolatos tényről / körülményről, szerződéses kötelezettségről, amelyet a vizsgálóval magam vagy kollégáim ne ismertettünk volna.*

Ezek alapján a Kockázat felmérési Jelentésben foglaltakat elfogadom.

2.4.3. A kritikus pontok

A felmérés során ügyelni kell a következőkre:

- ⇒ *a Kockázatfelmérés nem tartalmazhat minősítést csak a tényeket,*
- ⇒ *a mintavétel elve nem jelentheti azt, hogy tipikus jelenségek kimaradhatnak az átvilágításból. Ezért a mintavétel helyszíneit úgy kell megválasztani, hogy az a jellemző helyszíneket tartalmazza,*
- ⇒ *a feltárásnál az átvilágítónak abból kell kiindulnia, hogy a rögzített biztonsági környezetet figyelembe véve kell majd a veszélyforrásokat meghatároznia, majd azokhoz a védelemi intézkedéseket hozzárendelnie,*
- ⇒ *a Megbízónak egyértelműen felelősséget kell vállalnia a Kockázatfelmérés megfelelőségéért, ezért vitának csak olyan esetben van helye, ha az átvilágító tapasztalatai eltérnek a Megbízó által mondottaktól. Ilyen esetben a Jelentésben rögzíteni kell mind a két álláspontot.*

3. ELLENŐRZÉSI LISTA A VÁLLALATI SZINTŰ KOCKÁZATFELMÉRÉSI JELENTÉSHEZ

3.1. A VÁLLALATI SZINTŰ BIZTONSÁGI RENDSZER

⇒ *A vállalatirányítás, vállalati biztonságirányítási rendszer.*
⇒ *Van-e vállalati szintű integrált védelem?*
⇒ *A vállalati szintű kockázatokat feltárják-e, menedzselik-e (Enterprise Risk Management, ERM)?*
⇒ *A vállalati szintű biztonsági dokumentumok.*
⇒ *Az integrált vállalati szintű azonosítás menedzsment (Enterrprisewide Identity Management, EIM) van-e?.*
⇒ *A biztonsági események vállalati szintű kezelése.*
⇒ *A vagyonbiztonsági, és informatikai biztonsági alrendszerek (fizikai, logikai) határai.*
⇒ *A biztonsági kultúra helye, szerepe a szervezeti, vállalati kultúrában.*

4. ELLENŐRZÉSI LISTA AZ ÜZLETI RENDSZER KOCKÁZATFELMÉRÉSI JELENTÉSÉHEZ

4.1. AZ ÜZLETI FOLYAMATOK FELTÁRÁSA

⇒ *Az üzleti, és a támogató folyamatok meghatározása, megnevezése*
⇒ *A folyamat célja*
⇒ *A folyamat során végrehajtott tevékenységek*
⇒ *A folyamat által használt eljárás, technológia*
⇒ *A folyamat által használt IT szolgáltatások*
⇒ *A folyamat szabályozása*

4.2. SZERVEZÉSI KOCKÁZATFELMÉRÉS

Megegyezik az 5.1 pontban foglaltakkal

4.3. AZ ÜZLETI RENDSZER TECHNIKAI KOCKÁZAT FELMÉRÉSE

4.3.1. *A folyamatok által felhasznált erőforrások*

- *Adatok (értékek, anyagok, áruk)*
  - *Input (honnan)*
- *Technológia*
  - *Ügyvitel technikai eszközök*
  - *Szállító eszközök*
  - *Tároló (archiváló) eszközök*
- *Eljárások*
  - *Manuális*
  - *technikai*
- *Támogatások, létesítmények*
  - *Épületek, helyiségek*
  - *Légkondicionálás*
  - *Áramellátás (általában energia ellátás)*
  - *Egyéb berendezések*
- *Az emberi erőforrások*
  - *Tulajdonos(-ok)*
  - *Végrehajtók*
  - *Felhasználók*
- *A folyamatok végtermékei*
  - *Papíralapú*
  - *IT felé output*

4.3.2. Fizikai kockázatfelmérés

A fizikai kockázatfelmérés alapvetően megegyezik az informatikai kockázatfelmérésnél írtakkal. A vagyonbiztonság elsősorban fizikai biztonság, amely nagyrészt átfed az informatikai biztonsággal.

4.3.3. Logikai kockázatfelmérés

A logikai kockázatfelmérés csak akkor szerepel, ha az erőforrások között felsorolt technológiai eszközöknél értelmezhető, van elektronikus intelligenciával rendelkező technikai eszköz, rendszer (pl. számítástechnikával irányított raktározási rendszer, intelligens épület).

4.3.4. A hálózatok

Hálózatoknál a beszéd hálózat helyzet feltárása szerepel

4.3.5. Életciklus

Az üzleti folyamatoknál is értelmezhető az életciklus, mivel azok létrejönnek, üzemelnek, és megszüntetik őket. Ide tartozik a kapacitástervezés is.

5. ELLENŐRZÉSI LISTA AZ INFORMÁCIÓS RENDSZER KOCKÁZATFELMÉRÉSI JELENTÉSÉHEZ

5.1. SZERVEZÉSI KOCKÁZATFELMÉRÉS

5.1.1. A vállalati üzleti stratégia

⇒ *Az üzleti cél, és az üzleti követelmények*
⇒ *A biztonság az üzleti stratégiában (üzleti követelmények között)*
⇒ *A vezetés biztonság iránti elkötelezettsége ki van-e nyilvánítva (hol?)*

5.1.2. Szabályzások

5.1.2.1. Szervezet és működés szabályozása

⇒ *SZMSZ, szervezeti felépítés*
⇒ *Informatikai szervezet és működés*
⇒ *Munkaköri leírások tartalmi vázlata*
⇒ *Számítástechnikai munkakörök*
- *Számítástechnikai munkakörök*
- *A számítástechnikai munkatársak feladat körei (név szerint)*

5.1.2.2. Biztonsági infrastruktúra szabályozása

⇒ *A biztonsággal foglalkozó munkakörök a szervezetben*
- *az adatvédelemi felügyelő*
- *titokvédelmi felügyelő,*
- *az IT biztonsági infrastruktúra,*
  - ✓ *IT biztonsági szervezet*
  - ✓ *IT Biztonsági Forum*
  - ✓ *IT biztonsági feladatok a menedzsment szintjein, és*
- *a Vagyonbiztonsági infrastruktúra.*

⇒ *Együttműködés a külső szervezetekkel*
⇒ *Az IT biztonság hatékonysága (lásd részletesen a II. Kötet. 6.6 pontban)*

5.1.2.3. Tűzvédelmi szervezet, és működés szabályozása

⇒ *A tűzvédelem szervezettsége*
⇒ *A tűzvédelmi dokumentumok*
⇒ *A tűzvédelmi oktatás rendje*

5.1.2.4. Polgári védelmi szervezet, és működés szabályozása

⇒ *A polgári védelem szervezettsége*
⇒ *A polgári védelmi dokumentumok*

5.1.2.5. Biztonsági alapdokumentumok

⇒ *Kockázat menedzsment*
⇒ *Belső ellenőrzési, és Kockázat menedzsmenti jelentések*

⇒ *Biztonsági Stratégia*
⇒ *Biztonsági Politika (Biztonsági Szabályzat)*
⇒ *Katasztrófaterv*
⇒ *Biztonsági Szabályzat*
⇒ *Biztonság ellenőrzése*
⇒ *Biztonsági események kezelési rendje, és a statisztikája*

5.1.2.6. Adatvédelem szabályozása

5.1.2.6.1. Adatvédelmi szabályzat van-e

5.1.2.6.2. Adatbiztonsági szabályzat van-e

5.1.2.7. Titokvédelem szabályozása

5.1.2.7.1. Adatok, értékek

⇒ *Adatok védelmének szabályozása*
⇒ *Adatok, értékek védelmi osztályozási rendszere.*

5.1.2.7.2. Eszközök

⇒ *Eszközök védelmi osztályozási rendszere*

5.1.2.7.3. Eljárások

⇒ *Eljárások (alkalmazások, fontos rekordok) védelmi osztályozási rendszere*

5.1.2.7.4. Helyiségek

⇒ *Helységek védelmi osztályozásának rendszere*

5.1.2.7.5. Alkalmazások

⇒ *A fenti osztályozások kötelező alkalmazása a védelmi intézkedések meghatározásánál.*
⇒ *Az osztályozás feltüntetése mind a papír, mind az elektronikus adathordozón (címkézés).*
⇒ *Input, output adatok ellenőrzése*
⇒ *A feldolgozás ellenőrzése*

5.1.2.8. Iratkezelés szabályozása

⇒ *Az Iratkezelés szabályozottsága, egyáltalán van-e szabályozva*
- *Papíralapú iratok, és adathordozók (kezelés, archiválás, megsemmisítés)*
- *Elektronikus iratok, és adathordozók (kezelés, archiválás, megsemmisítés)*
- *A papír, és az elektronikus iroda közötti kétirányú kapcsolat szabályozva van-e*
- *Hard copyk kezelésének, elosztásának rendje szabályozva van-e*

5.1.3. Humánpolitikai intézkedések

- ⇒ *Milyen követelményeket érvényesítenek a felvételnél, és hogyan (állandó. szerződéses, és időszaki munkatársak, pl. végeznek háttér ellenőrzést)*
- ⇒ *Titoktartási nyilatkozat*
- ⇒ *Feladatok meghatározása és biztonság kritikus feladatok szétválasztása*
- ⇒ *A bizalmasság védelme a munkaviszony alatt*
  - ➢ *a megbízhatóság fenntartásának módszere, és gyakorlata,*
  - ➢ *szabadság, illetve szabadnap kiadási politika,*
  - ➢ *munkakör csere*
  - ➢ *karrier menedzsment*
- ⇒ *A munkaviszony megszüntetés gyakorlata*
- ⇒ *A biztonsági kultúra, és a biztonsági tudatosság hiányosságai*
  - ➢ *Van-e gazdája a biztonsági kultúra, tudatosság biztosításának, a biztonsági kultúra kialakításának, fenntartásának (Program)*
  - ➢ *Volt-e a biztonsági tudatossággal kapcsolatos biztonsági esemény*
  - ➢ *A felső vezetés, a menedzserek, a munkatársak (a vállalat munkatársai, és nem csak az IT munkatársak) biztonsági kultúrájának, és tudatosságának szintjei*
- ⇒ *A biztonsági oktatás, a biztonsági kultúra, tudatosság biztosítása*
- ⇒ *Van-e csalás elleni politika (fraud detection)*
- ⇒ *Van-e ipari kémkedés elleni politika (megtévesztés elleni védelem, megfelelő adat-, és titokvédelmi szabályozás, és ennek alapján kialakított humán, fizikai, logikai védelme) (Lásd 9.sz.tájékoztató)*
- ⇒ *Az élőerős védelemalkalmazói, és a személyvédelem megfelel-e a vonatkozó jogszabálynak.*
- ⇒ *Fegyelmezési folyamat van-e*

5.1.4. Szerződések

- ⇒ *Végeznek-e a szerződni szándékozókkal kapcsolatos háttér ellenőrzést,*
- ⇒ *A harmadik felektől igénybevett szolgáltatások szerződései,*
  - ➢ *Outsourcing szerződés (erőforrás kihelyezés) tartalmazza-e (COBIT 4.1 alapján):*
    - *Mire vonatkozik a szerződés (külső fejlesztés, belső fejlesztés, üzemeltetés kiadása, munkaerőbérlés stb).*
    - *Köteles-e a felhasználó megbízásából elvégzett tevékenységeinél minden jogi követelményt, illetve szabályt alkalmazni,*
    - *Biztosítva van-e a szerződésben a felhasználó ellenőrzési jogosultsága a szolgáltató minden szerződéses tevékenységénél saját, és a szolgáltató telephelyein,*
    - *Van-e a szerződésben „biztonsági szolgáltatási szint megállapodás”, és megfelel-e legalább a Felhasználó Biztonsági Politikájának.*
    - *Ki van-e kötve a felhasználó humán politikai irány elveinek alkalmazási kötelezettsége.*
    - *Ki van-e kötve a szolgáltatói tevékenység folyamatos monitoringja.*

- *Ki van-e kötve a felelősség, a felelősök a szerződés végrehajtásáért.*

➢ *Az outsourcing szerződéseknél vizsgálni kell továbbá*

- *Végez-e a szolgáltató a szerződésen kívül tevékenységet, fenn áll-e bármilyen nem szerződéses kapcsolat,*
- *A felelősök, munkatársak értik-e a felelősséget,*
- *A szolgáltató biztonsági politikája megfelel-e a felhasználóénak,*
- *Fenn áll-e a szolgáltató, és a felhasználó között a függetlenség,*
- *A hozzáférési jogosultságok a felhasználónál a szolgáltató munkatársainak a legkevesebb szolgáltatásra, és a legkevesebb jogosultságra vannak-e kiadva (szükséges tudás elve alapján),*
- *A hozzáférés-védelmi sw-hw-hez van-e hozzáférési jogosultsága a szolgáltatónak,*
- *Igénybe vesz-e a szolgáltató alvállalkozót.*

➢ *Szolgáltatási Szint Szerződés (SLA- SLM) karbantartásra, rendszerkövetésre*

A Service Level Agreement-nek a COBIT 4.1 szerint legalább az alábbiakat kell tartalmaznia, ezen kívül folyamatosan kell monitorozni a megvalósulását (Service Level Management) is. SLA köthető harmadikféllel, de belső szervezeti egységgel is. Ehhez össze kell állítani a szolgáltatások definícióit, és a szolgáltatási katalógust.

A szerződés minimum tartalmazza a következőket:

- *A szolgáltatás meghatározása*
- *A szolgáltatás költségei*
- *A minimális szolgáltatás mennyiségi meghatározása*
- *Az IT tevékenységek szintje*
- *Rendelkezésre állás, megbízhatóság, a növekedési kapacitás*
- *Katasztrófatervezés*
- *Biztonsági követelmények*
- *A szerződés bármely pontjának megváltoztatása*
- *Írott, és formálisan jóváhagyott megállapodás a szállító, és a felhasználó között*
- *Érvényes periódus, és új periódus áttekintése /megújítása / meg nem újítása*
- *a teljesítési jelentés tartalma, és gyakorisága, és a szolgáltatás díjazása*
- *A díj reálisan összehasonlítandó a múlttal, az iparral, és a legjobb gyakorlattal*
- *A díjak számítása*
- *A szolgáltatásfejlesztésnek a kötelezettsége*
- *Az SLA-nak tartalmaznia kell a SLM-hez az OLA, Operating Level Agreementet is (mind belső, mind külső féllel történő megállapodás esetére)*

- *Biztonsági követelmények a szerződésekben*
  a cél: fenntartani az informatikai biztonságot akkor is, ha a szervezet információfeldolgozási felelősségét (részben, vagy egészében) más szervezetnek alvállalkozásba adták, ezért az MSZ ISO/IEC 17799 szerint biztosítani kell
  - *hogyan fogják a jogi követelményeket kielégíteni, pl. az adatvédelmi szabályozást,*
  - *milyen rendelkezéseket kívánnak foganatosítani annak garantálására, hogy az erősforrás kihelyezésben /alvállalkozásba adásban/ résztvevő valamennyi fél, a további alvállalkozókat is beleértve, tudatában van saját felelősségének,*
  - *hogyan lesz fenntartva és vizsgálva a szervezet üzleti vagyonának sértetlensége és bizalmassága/titkossága,*
  - *milyen fizikai és logikai* óvintézkedéseket *fognak alkalmazni arra, hogy korlátozzák és behatárolják a jogosult használóknak a hozzáférését a szervezet biztonság érzékeny üzleti információihoz /adataihoz,*
  - *hogyan lesz fenntartva a szolgáltatások rendelkezésre állása katasztrófa esetében,*
  - *milyen fizikai biztonsági szinteket ajánlatos ellátni az erőforráskihelyezésben/alvállalkozásba adásban érintett berendezések esetében,*
  - *(miben áll és kire hárul) az átvilágítás/auditálás joga.*

- *A kockázat áthárítási szerződések (biztosítások)*
  - *Vagyoni kárra*
  - *Nem vagyoni kárra*
  - *Az üzleti tevékenység megszakadására vonatkoznak-e*

5.1.5. A szolgáltatási szint megállapodás megfelelősség

A COBIT 4.1 előírja, hogy az outsourcing szerződésben szerepelni kell az SLA-nak (Service Level Agreement), azaz legalább az alábbi követelményeknek:

- a szolgáltatás meghatározása
- a szolgáltatás költsége
- a számszerűsíthető minimális szolgáltatási szint
- az informatikai funkció által nyújtott támogatás szintje
- rendelkezésre állás, megbízhatóság, bővítési kapacitás
- az üzemfolytonosság tervezése
- biztonsági követelmények
- megállapodás bármely pontjának módosítása esetén a követendő eljárás
- az érvényességi idő és annak felülvizsgálata/megújítása/ a megújítás kizárása
- a teljesítési jelentések gyakorisága és tartalma, valamint a szolgáltatási díjfizetések, azok reális volta
- a díjtételek számításának módja
- a szolgáltatás javítására tett kötelezettségvállalás.

Az MSZ_E_15000 magyar elő szabvány szerint a szolgáltatási szintet tervezni és azt végrehajtani kell (SLM= service level management).

5.1.6. A biztonsági események kezelésének rendje

⇒ *Szabályozva van-e a jelentés, értékelés, intézkedés, és a bizonyítékok őrzése.*
⇒ *Szabályozva van-e az üzletment zavarai, és megszakadása kezelése.*

5.2. TECHNIKAI KOCKÁZATFELMÉRÉS

5.2.1. Erőforrások

⇒ *IR erőforrások leltára*

⇒ *Adatállomány (adatbázisok, adat fileok)*

⇒ *HW architektúra*

- *Blokkséma (core system, hálózatok, végpontok, mobil adathordozók portjai)*
- *Távközlési csatlakozások (külső hálózatok, dial in portok, on line diagnosztika csatlakozások)*

⇒ *Rendszer sw-ek adatai*

- *Az alkalmazott rsw-ek típusa, rendeltetése, verziója*
- *A rsw szállítója*
- *Eredeti példány van-e, és hol*
- *Dokumentáció*
- *A rsw biztonságértékelési minősítése (TCSEC, ITSEC, CC)*
- *Fejlesztő sw.-ek*

⇒ *Alkalmazói sw-ek*

- *Asw-ek listája (minősített adatok és alkalmazások feltüntetve)*
- *Asw-ek adatai (név, platform, szállító, az asw forráskódban kinél áll rendelkezésre, a tulajdonosok-rendszergazdák, és a felhasználók listája)*
- *Rendszerbe beépített ellenőrzések (teljesség, pontosság)*

⇒ *Az információ-rendszer integráltsága*

⇒ *Támogató eszközök*

- *Energiaellátás*
- *Légkondicionálás*
- *Adathordozó tárolás*
- *Papírfeldolgozás stb.*

⇒ *Dokumentációk*

- *Rendszer dokumentációk*
- *Felhasználói kézi könyvek*
- *Oktatási anyagok*

5.2.2. Fizikai hfv

5.2.2.1. Alkalmazzák-e a Titokvédelmi Utasítás osztályozását

5.2.2.2. Aktív támadás elleni fizikai védelem

5.2.2.2.1. A berendezések, rendszerek fizikai elhelyezésnek megválasztása biztonsági szempontból

⇒ *Figyelembe veszik-e a rendszerek, berendezések elhelyezésének megválasztásánál a biztonsági szempontokat,*

5.2.2.2.2. Belépés és mozgás ellenőrzés

⇒ *A fizikai biztonsági határ zóna ki van-e jelölve,*
⇒ *A belépés ellenőrző rendszer (-ek)*
- *működése, üzemeltetése, dokumentációja (naplózás),*
- *a rendszer kikre vonatkozik (saját munkatárs, látogató, karbantartók), és vonatkozik-e a be, és kilépésre, illetve az ott tartózkodásra egyaránt),*
- *a belépési engedély adathordozója életciklusának kezelése*
- *a beléptető, és mozgás ellenőrző rendszer megfelel-e a vonatkozó jogszabálynak.*

⇒ *Biztonság kritikus informatikai helyiségek belépés ellenőrzése*
⇒ *Értéktároló helyiségek belépés ellenőrzése*
⇒ *Őrzésvédelem élőerővel*
⇒ *Mozgás ellenőrző rendszer (videó, infra, egyéb)*
⇒ *A lokális hálózatok (LAN) fizikai hfv*
⇒ *Az országos távközlési hálózat (WAN) kilépési pontjainak fizikai hozzáférés-védelme*
⇒ *Az egyéb országos (világ) hálózat (-ok) felé a távközlési hálózat kilépési interfészeinek fizikai hozzáférés-védelme*
⇒ *A terminálok fizikai hozzáférés-védelme*
⇒ *A hordozható (mobil), és off site számítástechnikai eszközök (laptop, CD, DVD, pen drive, PDA) csatlakoztatási lehetőségének, és alkalmazásának szabályozása, és fizikai hozzáférés-védelme a védett, és a nem védett környezetben, eszközök áthelyezésének szabályozása, külső eszközök használati jogosultsága (lásd 4.4 pontot is)*
⇒ *Az eltávolítható adathordozók védelme*
⇒ *Kábelezés védelme*
⇒ *Takarítás rendszere*

5.2.2.2.3. Behatolás-védelem

⇒ *A behatolás jelző rendszereknek a biztonsági fokozatba sorolása, és a védett helyiségek védelmi osztályba sorolása.*
⇒ *Számítóközpontok behatolás-védelme*
⇒ *Értéktároló helyiségek behatolás-védelme*
⇒ *Értékszállítás védelme*

5.2.2.2.4. Információk, eszközök ellopás elleni védelme

⇒ *Van-e üres íróasztal, és képernyő politika*
⇒ *Az informatikai vagyontárgyak mozgatásának, áthelyezésének rendje*

5.2.2.3. Passzív támadás elleni fizikai védelem

5.2.2.3.1. Elektromágneses kisugárzás

⇒ *EMC védelem van-e, és hol*
⇒ *Miből áll, megfelelően van-e méretezve*

5.2.2.3.2. Akusztikus kisugárzás

⇒ *Hol, és milyen akusztikus kisugárzás védelmet alkalmaznak*

5.2.2.3.3. Hulladékmegsemmisítés

⇒ *A számítástechnikai kellékek (pl. festék lepedők, festék patronok) fizikai kezelése, megsemmisítése (szabályozás, és gyakorlat)*
⇒ *Papír alapú adathordozók fizikai kezelése, tárolása, megsemmisítése (szabályozás, és gyakorlat)*
⇒ *Eszközök (médiák) selejtezési, újrafelhasználási rendje*

5.2.3. Fizikai rendelkezésre állás

5.2.3.1. Energiaellátás

⇒ *A szünetmentes áramellátás, és vízellátás rendszere*
⇒ *Az energiahordozók alternatív betáplálása*
⇒ *A villamos energia ellátás zavarszűrése*

5.2.3.2. Tűzvédelem

⇒ *Telepítési terv,*
⇒ *Tűzoltó készülékek, rendszerek elhelyezési listája,*
⇒ *Az utolsó karbantartás, illetve ellenőrzés időpontja*

5.2.3.3. Villámvédelem

⇒ *A villámvédelmi rendszer*
⇒ *A védőföldelési rendszer*

5.2.3.4. Klimatizálás

⇒ *Alkalmaznak-e klimatizálást, és ha igen a paraméterek*

5.2.3.5. Számítóközpont stratégiai elhelyezése

⇒ *A számítóközpont elhelyezése megfelel-e a biztonsági követelményeknek*

5.2.3.6. Megbízhatóság

⇒ *Eszközök megbízhatósága*
⇒ *Háttér hw erőforrások (eszköz redundancia)*

5.2.3.7. Beszéd kommunikációs eszközök

⇒ *A beszéd hálózat, beszéd kommunikációs lehetőségek*

5.2.3.8. Dokumentáció

⇒ *Hw dokumentációk*

5.2.3.9. Karbantartást ellátók

⇒ *Karbantartás rendszere (a biztonsági követelmények érvényesítése)*
⇒ *Karbantartók (belső és/vagy külső)*

5.2.3.10. Felügyeleti rendszer

⇒ *Épület felügyeleti rendszer felépítése, elemei, üzemeltetése*
⇒ *Biztonsági felügyeleti rendszer felépítése, üzemeltetése*
⇒ *Integrált-e az épület, és a biztonság felügyeleti rendszer.*

5.2.4. Logikai hfv

5.2.4.1. Alkalmazzák-e a Titokvédelmi Utasítás osztályozását

5.2.4.2. Aktív támadások elleni védelem

5.2.4.2.1. Jelszó és jogosultsági rendszer

⇒ *Az objektumok, és szubjektumok minősítési rendszere*
⇒ *A szereplők (felhasználó, rendszergazda, biztonsági adminisztrátor, biztonsági auditor)*
⇒ *A jelszavas hfv-i rendszer*
  - *A login rendszer*
  - *A hfv.-i sw*
  - *A hfv.-i sw biztonsági osztálya (nemzetközi minősítés)*

⇒ *A felhasználó azonosítás menedzsment*
  - *ID adminisztráció*
    - *Megadás*
    - *Bevezetés*
    - *Csere*
    - *Törlés*
    - *érvényesség*
  - *Az ID felépítése*
  - *Van-e vállalati szintű azonosítási rendszer (enterprise wide identity management system)*
  - *Tárolás*
  - *Jelentés a felhasználói jogosultságokról*

⇒ *A jelszó menedzsment*
  - *A jelszó típusa*
  - *A jelszó felépítése*
  - *A jelszó megválasztása*
  - *Egy felhasználó jelszó használata, és követelményei, jelszavainak száma*

- *Alkalmaznak egy jelszavas beléptetési rendszert (SSO, single sign on)*
- *A jelszó tárolás módja*
- *Adminisztráció*
  - *Megadás*
  - *Bevezetés*
  - *Csere*
  - *Törlés*
  - *érvényesség*

⇒ *A jogosultság menedzsment*
- *Rendszer jogosultságok*
- *A tevékenységek*
  - *Rendszer tevékenységek*
  - *Speciális tevékenységek (pl. nyilvánosságra hozás, és az ezzel kapcsolatos módosítás jogosultsága)*
- *A szereplők jogosultságai*
  - *Rendszergazda*
  - *Felhasználó*
  - *Account adminisztrátor*
  - *Audit adminisztrátor*
  - *Van-e kiváltság menedzselés*
- *A jogosultság megadása*
  - *Bevezetés*
  - *Tárolás*
  - *Csere*
  - *Törlés*
  - *Hozzáférés a forrás nyelvi könyvtárhoz*
- *Account adminisztrátornak van-e külön felhasználói accountja*

⇒ *A file szintű biztonság*
- *Van-e aktív felhasználó jelszó nélkül*
- *Van-e több felhasználónak azonos jelszava*
- *Rendszerbeállítások*
- *Érzékeny adatok, alkalmazások osztályozás szerinti jogosultsága*
- *A felhasználók home directoryjának elérése korlátozott-e*

⇒ *Eszköz szintű biztonság*
- *Van-e automatikus terminál azonosítás*
- *Van-e terminál bejelentkezés*
- *Az eszköz használat korlátozva van-e*

⇒ *Van-e vállalati szintű azonosítás menedzsment (enterprise identity management, IdM) rendszer*

⇒ *Naplózás*
- *Felhasználók, a szereplők tevékenységeit rögzítik-e*
- *A biztonsági esemény menedzsment*
  - *Feltárás*
  - *Jelentés*
  - *Értékelés*
  - *Intézkedés*
  - *Az utolsó egy év eseményei*

⇒ *Objektum újra felhasználás szabályozott-e*

⇒ *Hozzáférési útvonalak*
- *Operátor konzol*
- *On line terminálok*
- *Batch feldolgozás*
- *A biztonság érzékeny rendszerek el vannak-e szigetelve*
- *Távközlési csatlakozások védelme*
  - *Különféle hálózatok (X 25, VSAT, Internet stb.)*
  - *Dial in portok*
  - *On line diagnosztika*

⇒ *Van-e kényszerítés alatti bejelentkezés riasztás*

⇒ *Van-e behatolás védelem (IDS, IPS)*

5.2.4.2.2. A hozzáférés-védelem a minősített rendszerszoftvereknél

AZ ISMS SW CHECKLIST alapján készítendő kérdések WNT, UNIX, ORACLE, SAP R3 esetében.

5.2.4.2.3. Tartalomhitelesítés

⇒ *A hitelesítéshez használt hash algoritmus, képzése, elosztása,*

⇒ *Az alkalmazott rejtjelezési módszer, a kulcsképzése, és elosztása,*

⇒ *Az eljárás fizikai, és logikai védelme biztosítva van-e (lásd FIPS 140-1),*

⇒ *A forrás hitelesség, a pontosság, és a teljesség védelme az inputoknál,*

⇒ *A pontosság, a teljesség védelme a feldolgozás során,*

⇒ *Elő van-e írva*
- *a partner hitelesítése (bizalmas jelszó, és kulcs csere),*
- *a tranzakciók hitelesítése (rejtjelezés az aláírásnál, és az aláírás érvényesítésnél)*
- *a kulcs menedzsment (kulcsok elosztása, felfedés esetén visszavonása),*
- *a pénzügyi, és biztonságkritikus input, feldolgozás alatti, output, tárolt, és archivált adatok hitelesítése.*

⇒ *Van-e PKI (tanúsítási rendszer, letagadhatatlanság biztosítás, stb)*

5.2.4.2.4. Time out

⇒ *A log off követelmény a terminálóknál*

⇒ *Time out eljárás*

⇒ *A kapcsolati idő limitálása*

5.2.4.2.5. Logikai behatolás jelzés

⇒ *Alkalmaznak-e logikai behatolás jelző, vagy védelmi rendszert (Intrusion Detection, Protection System).*

5.2.4.3. Passzív támadás elleni hfv

⇒ *Alkalmazott rejtjelezési eljárás (politika)*
- *A kulcsképzés, és elosztás*
- *Az eljárás, berendezés fizikai, és logikai védelme (FIPS PUB 140-2)*

- *A kulcs menedzsmentet fenyegető veszélyforrások (MSZ ISO/IEC 11770-1 A melléklet, valamint az I kötet 7.4.2..3 pontban) fennállnak-e*

⇒ *Emberileg olvasható output előállítás korlátozása*

5.2.5. Logikai rendelkezésre állás

5.2.5.1. Vírus (rosszindulatú sw-ek elleni) védelem

⇒ *Feladat, felelősségi körök a vírusvédelemmel kapcsolatban*
⇒ *Általános munkaköri kötelességek, felelősségek, retorziók*
⇒ *Külső hozzáférések*
⇒ *Üzemeltetés központosítása*
⇒ *Tartanak-e a vírussal elkövetett számítógépes visszaélésektől*
⇒ *Van-e vírusvédelmi szempontból kritikus folyamat*
⇒ *Adatforgalom hogyan zajlik*
⇒ *Elektronikus levelezés*
⇒ *Új anyagok, programok feltelepítésének a rendje*
⇒ *Vírusvédelmi megoldások (több szintű-e a védelem, aktív-e, és van-e kém sw, és kéretlen reklám elleni védelem))*
⇒ *Vírusvédelmi szoftverek frissítésének mechanizmusa*
⇒ *Hozzáférési jogosultságok kiosztásánál figyelembe vesznek-e vírusvédelmi megfontolásokat*
⇒ *Hálózat- vagy általános karbantartói munkák vírusmentes körülményeinek biztosítása*
⇒ *Van-e rejtett csatorna elleni védekezés*
⇒ *Biztonsági mentések, visszaállítások megfelelnek-e a vírusvédelmi követelményeknek*
⇒ *Vírusirtás módszertana*
⇒ *Teljes visszaállítás módszertana*
⇒ *Megtörtént vírusfertőzések és azok nyilvántartása*
⇒ *Vírusvédelmi oktatás*

5.2.5.2. Mentés, újraindítás

⇒ *Eredeti és háttér példány megőrzés*
⇒ *Programok forrásnyelvi változatai*
⇒ *Feladat, felelősségi körök a biztonsági mentésekkel kapcsolatban*
⇒ *Általános munkaköri kötelességek, felelősségek, retorziók*
⇒ *Üzemeltetés központosítása*
⇒ *Követelmények részlegenként, folyamatonként*
⇒ *Mentések rendszeressége, módja*
⇒ *Mentések terjedelme*
⇒ *Alkalmazott eszközök*
⇒ *Hibatűrő rendszerek*
⇒ *Mentések tárolása*
⇒ *Visszaállítás módja*

⇒ *Események nyilvántartása*
⇒ *Belső ellenőrzések*
⇒ *Kritikus alkalmazások rendelkezésre állásának biztosítása*
⇒ *Az alkalmazói rendszerek folyamatos működésének biztosítása*
⇒ *Az alkalmazói rendszerek rendszerkövetése és javítása,*

5.2.5.3. Logikai rombolás

⇒ *Van-e logikai rombolás elleni védelem*
⇒ *Hol, és a módszer*

5.2.5.4. Dokumentáció

⇒ *A rsw-ek dokumentáció*
⇒ *Az asw-ek dokumentációi*
- *Rendszerterv*
- *Üzemeltetési rend (program csere mgm)*
- *Felhasználói kézikönyv*
- *Ügyviteli szabályzat*
- *Újraindítási utasítás*

⇒ *A dokumentumok naprakészen tartása, verziókövetés*
⇒ *A dokumentumok tőpéldányainak őrzése*

5.2.6. Hálózatok

5.2.6.1. Típusok, alkalmazási helyük

⇒ *A távközlési hálózat struktúrája (térkép a nyomvonalakról, kimutatás)*
⇒ *Van-e távközlési hálózatok szolgáltatásaira vonatkozó követelményrendszer (rendelkezésre állás, hibaarány, kapcsolat felépítési idő, stb.) a hang, a fax, és videó távközlést beleértve*
⇒ *Amennyiben igen, a követelmények alrendszeremként azonosak, vagy különbözőek*
⇒ *Milyen távközlési hálózatot használnak a cég különböző egységeiben (központ, igazgatóság, fiók), illetve hálózataiban? (kapcsolt beszéd, bérelt beszéd, bérelt digitális vonalak, X.25, intranet, internet, extranet stb.)*
⇒ *Van-e hálózat ellenőrzés*

5.2.6.2. Nem bizalmas hálózati kapcsolatok

⇒ *Milyen külső távközlési csatlakozások vannak a vállalati belső információrendszeréhez (pl. bankok, ügyfelek, szervizek, saját munkatársak, külföldi kapcsolatok, INTERNET), azok milyen típusúak [kapcsolt (pl. kapcsolt hálózat dial in porton), bérelt vonal, X25 stb].*
⇒ *Kivel van szerződés a távközlési szolgáltatásra (MATÁV, helyi szolgáltatók, stb) és a szerződések*
⇒ *Van-e port védelem*

5.2.6.3. Védelem a LAN-ban

⇒ *A check list összeállításához lásd a 7.4.5. pontban megadott 41 LAN veszélyforrást is.*

⇒ *Hozzáférés-védelem*
- *Fizikai hozzáférés a hálózati elemekhez (szerver, hub, kábelezés)*
- *Illegális csomópont beépítési lehetősége*
- *Logikai jelszó, és jogosultsági rendszer*
- *Tartalmi hitelesség védelem*
- *Adatforgalom elemzés elleni védelem*
- *Adatok leszívása elleni védelem*
- *Time out*
- *Supervisor account elérési lehetősége*
- *Naplózás*

⇒ *Rendelkezésre állás*
- *Redundans hálózati elemek (szerver, topológia)*
- *Aktív elemek áramellátása*
- *Légállapot megfelelőssége a szállító előírásainak*
- *Dokumentáció*
- *Vírusvédelem*
- *Rsw mentés, újraindítás*

⇒ *Biztonsági események az utolsó három évben*

⇒ *Vezeték nélküli LAN (WLAN, Wireless LAN)*
- *logikai hozzáférés védelem (lehallgatás elleni védelem)*
- *jogosulatlan belépés elleni védelem*
- *alkalmaznak-e WI-FI Protected Access Point védelmet a jogosulatlan hozzáférés ellen,*
- *a szolgáltatás megakadályozása elleni védelem*
- *a forgalom sértetlenségének védelem*
- *a környezeti interferenciás zavarok elleni védelem*

5.2.6.4. Védelem a WAN-ban

⇒ *A hálózati biztonság mgm (Intranet / Extranet / Internet) ellenőrzési szempontjai a ISACF (lásd [40]) alapján.*
- *Az adatok osztályozva vannak-e, meg van-e határozva a minimális védelmi igény,*
- *A Felhasználó hitelesítési folyamat használja-e a kombinációját a három alapvető hozzáférés-védelmi rendszernek (ki vagy, mi van a birtokodban, mit tudsz),*
- *A szükséges tudás elvét alkalmazzák-e a hozzáférési jogosultságok megadásnál,*
- *Biztosítja-e a felhasználó adminisztráció a megfelelő időben történő felhasználói jogosultságok megadását, módosítását, visszavonását,*
- *Megtörténik-e a jogosultságok periodikus ellenőrzése,*
- *A hálózati adminisztrátor jogosultság megadása korlátozva van-e,*
- *A behatolás jelzésre használnak-e IDS-t,*
- *Az érzékeny, bizalmas adatok forgalmazására használnak-e rejtjelezést,*
- *Alkalmaznak-e digitális aláírást, üzenet kivonatot, és tanúsítást,*

- *A le nem tagadhatóságot (küldő, fogadó) biztosítják-e,*
- *A kulcs hálózati elemek (server, hub, switch) fizikai védelme megoldott-e, továbbá*
- *Védelem az Internet felé*

5.2.6.5. Beszéd hálózat

⇒ *Hozzáférés-védelem gyakorlata*
- *Lehallgatás elleni védelem*
- *Jogosultság korlátozás az on line diagnosztikánál*

⇒ *Rendelkezésre állás védelme*
- *Redundancia (alternatív beszéd hálózat)*

5.2.7. Védelem az IR életciklus során

5.2.7.1. Minőség biztosítás

⇒ *Van-e kidolgozott (fejlesztett), minőségbiztosítási rendszer, amelyet működtetnek, karbantartanak, ellenőriznek, annak érdekében, hogy az IT rendszer teljesítse az üzleti követelmények alapján meghatározott követelményeket.*

5.2.7.2. Fejlesztés

5.2.7.2.1. Fejlesztés indítása

⇒ *Meg vannak-e határozva az alkalmazással kapcsolatos biztonsági követelmények*
⇒ *Meg vannak-e határozva a fejlesztési környezettel kapcsolatos biztonsági követelmények*
⇒ *Az adatok érzékenységét vizsgálják-e*
⇒ *Az adatforrások pontosságát vizsgálják-e*
⇒ *A felhasználók kielégíthetően azonosíthatók, hitelesíthetők-e*
⇒ *A felhasználói interfészek elegendően korlátozhatók-e*
⇒ *Megfelelő-e a tervezendő sw szempontjából a biztonsági környezet, a fizikai biztonság, és a háttér eljárások.*
⇒ *Megfelelő gondossággal van-e a kapacitás megtervezve.*

5.2.7.2.2. Fejlesztési környezet

⇒ *A biztonsági követelmények érvényesítése a fejlesztési környezetben*
⇒ *A szabályok rögzítése*
⇒ *Van-e minősített fejlesztés*
⇒ *Fejlesztés belső és harmadikféllel szabályai*

5.2.7.2.3. Biztonsági követelmények a fejlesztendő rendszerekben

⇒ *A biztonsági követelmények érvényesítése a fejlesztés során*
- *A fejlesztendő alkalmazói rendszer interfészei az inf. rendszerben futó más rendszerekkel*
  - *Adatforrások,*
  - *Input előkészítés*

- *Adatbevitel*
- *Output elosztás*
- *Adatbázis adminisztráció*
- *Archiválás, mentés, üzemeltetés, háttér eljárások*

➢ *Az egyes interfészekért a felelősök*
➢ *Feladatszétválasztás személyekre, és a fejlesztés fizikai, és logikai leválasztása az üzemeltetésről,*
➢ *Biztonság érzékeny objektumok, és tevékenységek meghatározása*
➢ *A rendelkezésére állás követelményei, hibatűrő képesség, kapacitástervezés*
➢ *Szellemi tulajdonjogok védelme megoldott-e*

⇒ *Felesleges programozási lehetőségek a felhasználóknál*
⇒ *Letiltott interfészek*
⇒ *Az alkalmazás adatai, kódjai meg vannak-e osztva más alkalmazásokkal*
⇒ *A biztonság kritikus kódok el vannak-e szigetelve (pl. programok digitális aláírásának titkos kulcsai, biztonságkritikus kódok csak read only memoriban)*
⇒ *Biztonsági tudatosság biztosítása*
⇒ *Biztonsági naplózás ellenőrzése*
⇒ *A fejlesztés mentése, háttér eljárásai*
⇒ *Tesztelési terv (statikus, dinamikus)*
⇒ *Kapacitástervezés van-e*
⇒ *Médiák, eszközök szállítás alatti védelme, van-e*

5.2.7.3. Átadás/átvétel

⇒ *A beépített biztonsági követelmények ellenőrzése*
⇒ *Fejlesztők jogosultságainak visszavonása*
⇒ *Biztonsági követelmények az átvételi, és üzembe helyezési eljárás során*
⇒ *Rendszer teszt adatok védelme*
⇒ *Rendszer sw ellenőrzése*

5.2.7.4. Üzemeltetés

⇒ *Programcsere (adatcsere) menedzsment szabályozása, és gyakorlata, a vészhelyzet esetére is.*
⇒ *Konfiguráció mgm szabályozása, és gyakorlata (az erőforrások infrastruktúra elemek cseréje szabályozva van-e, a számon kérhetőség biztosítása mellett).*
⇒ *Input biztonsági ellenőrzése*
⇒ *Adatbázis biztonsági ellenőrzése*
⇒ *Hw karbantartás biztonsági ellenőrzése*
⇒ *Program változat követés gyakorlata*
⇒ *A biztonsági események követésének rendje*
⇒ *A biztonsági események követésének gyakorlata*
⇒ *Az üzemeltetési tevékenységek dokumentálva vannak-e*
⇒ *Az elmúlt év biztonsági eseményei*
⇒ *A papíralapú irodai tevékenység védelme meg van-e oldva*

- *az irodai rendszerekben az információ sérülékenységét, például a telefonhívások és a konferenciabeszélgetés rögzítését, a hívások*

bizalmasságát/titkosságát, a faxüzenetek tárolását, levelek felbontását és a levélkiosztást tekintve,

- *az információ megosztás menedzselését szolgáló szabályzatokat és alkalmas* óvintézkedéseket*, például a vállalati elektronikus hirdetőtábla használatát,*
- *az érzékeny üzleti információ egyes kategóriáit kizárják-e, ha a rendszer nem nyújt elegendő védelmi szintet,*
- *a kiválasztott egyének naptári információjához való hozzáférés korlátozását, például olyan személyzet esetén, akik érzékeny projekteken dolgoznak,*
- *az üzleti alkalmazásokat futtató, vagy más módon megválasztott rendszerek alkalmasságát, amelyek például megrendeléseket vagy feljogosításokat közölnek (*kommunikációs csatornán kommunikálnak*),*
- *a személyzet, a szerződő vagy az üzleti partnerek kategóriáit, osztályait, akiknek engedélyük van a rendszer használatára és arra a helyre, ahonnan a rendszerhez hozzáférhetnek,*
- *meghatározott használói kategóriáknak, osztályoknak, a választott eszközök használatának korlátozását,*
- *a használók státusának azonosítását, feltüntetését például a névtárakban (*directory*) a szervezet alkalmazottai vagy szerződő partnerei esetében, a többi használó előnyére,*

⇒ *A cserélhető adathordozók fizikai védelme meg van-e oldva, tárolás, vagy szállítás esetén*

⇒ *Az információ (adatkezelési) eljárások a Titokvédelmi Utasításban kitérnek-e az üzemeltetési környezetre*

⇒ *Rendszerdokumentációk, újraindítási eljárások leírásai védettek-e.*

5.2.7.5. Selejtezés

⇒ *Számítástechnikai eszközök, és kellékek selejtezése*

- *A selejtezés rendje (jegyzőkönyv, bizottság, egyedi érvénytelenítés, egyedi megsemmisítés)*
- *Az adathordozók törlése megsemmisítés előtt*
- *A szigorú számadás alá vont adathordozók (például mágnes, chip kártyák) visszavonás utáni közvetlen érvénytelenítése*

5.3. SZÁMON KÉRHETŐSÉG

⇒ *A szervezeten belüli információs rendszerek órajeleit szinkronizálják-e, a számon kérhetőség biztosítása céljából,*

⇒ *Elrettentést alkalmaznak-e*

⇒ *A szerepek, felelősségek allokálva vannak-e*

⇒ *Audit trailt használnak-e*

⇒ *Account audit log a TCB-ben van-e*

⇒ *Behatolás jelzők logjait értékelik-e*

⇒ *Van-e fizikai belépés (mozgás) nyilvántartás*

⇒ *Ki vannak-e jelölve az informatikai, és egyéb (az üzleti rendszerben használt) eszközök leltárai, és felelősei (tulajdonosok)*

⇒ *Van-e általában eseménynaplózás, rendszer használatmonitorozás*

5.4. A MOBIL SZÁMÍTÁSTECHNIKAI ESZKÖZÖK

⇒ *Szabályozva van-e a mobil számítástechnikai eszközök vállalaton belüli, és nem védett külső környezetben történő kezelése, csatlakozási lehetőség alkalmazása (laptrop, CD, DVD, pen drive, PDA).*
⇒ *Van-e minden mobil eszköznek felelős gazdája*
⇒ *Biztosítva van-e a belső, és nem védett környezetben az eszköz folyamatos fizikai védelme*
⇒ *Meg van-e oldva a káros környezeti besugárzások elleni védelem*
⇒ *Megfelelő-e a hozzáférés védelem*
⇒ *Alkalmaznak-e rejtjelezést*
⇒ *A biztonság érzékeny sw-ek mobil eszközökre másolása, és a kivitele a vállalat területéről szabályozott-e*
⇒ *A különböző hálózatokhoz való csatlakozás védve van-e*

5.5. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

⇒ *A biztonsági események kezelése szabályozott-e*
(tevékenységek, szerepek, számon kérhetőség, célok)
⇒ *Van-e service desk (help desk)*
⇒ *A biztonsági esemény meg van-e egyértelműen határozva*
⇒ *A biztonsági események osztályozva vannak-e súlyuk, kiterjedésük, hatásuk alapján, és az egyes osztályokhoz hozzá vannak-e rendelve az elhárító folyamatok*
⇒ *A biztonsági események jelentésének gyakorlata*
⇒ *A biztonsági események, trendjük, kiterjedésük értékelése, elemzése,*
⇒ *Vizsgálják-e felhasználóknak, az elhárítási tevékenységekkel kapcsolatos elégedettségi szintjét.*

5.6. BIZTONSÁGI ÉRETTSÉGI SZEMPONTOK

A COBIT4.1 Management Guidelines alapján. Ezek az átvilágítási szempontok azt a célt szolgálják, hogy az ellenőrzési listát, a figyelembevételükkel, amennyiben szükséges módosítsák, vagy kiegészítsék.

5.6.1. *Kritikus sikertényező* (a mgm irányítása, és ellenőrzése az IT-N)

⇒ Biztonsági dokumentációk vannak-e
⇒ Tudatos biztonsági fejlesztési terv van-e
⇒ A védelmi intézkedések a top mgm felelőssége-e
⇒ A mgm, és az alkalmazottak megértik-e a védelem szükségességét, és a saját felelősségüket
⇒ Van-e rendszeres külső audit
⇒ Folyamatos-e a biztonsági (a biztonsági kultúra) képzés
⇒ A biztonsági eseményeket kezelik-e

⇒ Központosított jelszó, és jogosultság mgm van-e.

5.6.2. *Kulcs célmutatók* (a megvalósulás?)

⇒ Volt-e nyilvános zavaró esemény
⇒ A kritikus eseményeket azonnal jelenti-e
⇒ A hfv.-i jogosultságok össze vannak-e hangolva a szervezeti felelősségekkel
⇒ *Biztonsági okokból késtek-e implementációk*
⇒ *Van-e eltérés a biztonsági követelményektől*
⇒ *Voltak-e események jogosulatlan hozzáférés, információvesztés, vagy felfedés miatt.*

5.6.3. *Kulcs teljesítménymutatók* (hogyan valósult meg?)

⇒ Minimális-e a biztonsági szervizhívás, zavar
⇒ Mennyi a biztonsági események miatt kiesett idő
⇒ A behatolás jelzések száma
⇒ A biztonsági események feltárásra fordított idő
⇒ A biztonsági események jelzése, jelentése, és kezelése közötti késedelmi idő
⇒ A biztonsági tudatosság oktatásra fordított napok száma.

5.7. A RENDSZER BIZTONSÁGI SZINTJÉNEK MÉRÉSE

5.7.1. Mutatók

A biztonsági rendszer, az IT biztonsági alrendszer biztonsági szintjének értékelése, az Átvilágítási jelentés végén, a kockázatok csökkentésére javasolt védelmi intézkedések realizálása esetére feltétlenül szükséges. Előnyös, ha a kiinduló, feltárt helyzetet is értékeljük. Az értékelés eszköze a COBIT érettségi modell lehet az előzőpont alapján, és amely felhasználása előtt célszerű a COBIT 4.1-ben, a 34 folyamathoz megadott mérési módszereket is felhasználni. A COBIT 4.1 a „DS5 Gondoskodás a rendszer Biztonságáról” pontban megadott mérései a következők:

Kulcs teljesítmény mutatóknak a mérése:

⇒ Az észlelt biztonsági események jelentése, és gyakorisága
⇒ Az idejétmúlt accountok (beléptetés tárolók) típusa, és száma
⇒ A törölt jogosulatlan IP címek, portok, forgalom típusok, és számuk
⇒ A kompromittált, és visszavont rejtjelezési kulcsok száma
⇒ A megadott, visszavont, zárolt, és cserélt hozzáférési jogosultságok száma

A folyamatok kulcs cél indíkátorainak mérése:
⇒ A feltételezett, és tényleges jogosulatlan hozzáférések típusa, és száma
⇒ A feladat szétválasztás elvéve megsértéseinek száma
⇒ A jelszó kezelés szabályait be nem tartó felhasználók %-a.

⇒ A feltárt rosszindulatú kódok típusa, és száma

Az IT kulcs cél mutatók mérése:

⇒ Az üzleti hatással járó biztonsági események száma
⇒ A biztonsági követelményeknek nem megfelelő rendszerek (alkalmazói rendszerek) száma
⇒ A hozzáférési jogosultságok engedélyezési, csere, és visszavonási ideje.

5.7.2. Biztonsági mértékek.

A mérések az IT rendszereknél, az IT biztonságnál, és általában a biztonságnál nemrég kerültek alkalmazásra. A COBIT 3 közli a rendszer érettségi modellt, míg a COBIT 4.1 34 érettségi modellt alkalmaz, a folyamatok, és tevékenységek mértékeinek összefoglaló értékelésére, és a 34 érettségi modell alapján készíthető általános érettségi modell, pedig a COBIT 3-ban megadott, valamint az egyes folyamatokhoz tevékenységekhez megad 379 mértéket, amelyekből az alábbiakban közöltek a biztonsággal kapcsolatosan felhasználandó mértékek.

Szükséges rögzíteni, hogy ma már a belső ellenőrzést, az auditálást csak mérésekre, mértékekre is támaszkodó vizsgálat alapján lehet kellően tényekkel alátámasztani (lásd ISACA auditorok etikai kodexében szereplő követelményt, amely szerint az auditornak tényekkel kell alátámasztani megállapításait). Ugyan ez mondható a kockázat elemzésre.

*A **mértékek** eszközök a teljesítmény és a számon kérhetőség, az adatokat meghatározó teljesítmények összegyűjtésének, elemzésének, és a jelentésének az elősegítéséhez.*

A sw fejlesztésben a mérték a program teljesítmény, és hatékonyság egyes jellemzőinek mértéke [4].

A mérés, és a mérték közötti különbség:

A **mérés** (measurement) egy időpontban, vizsgálja a speciális, diszkrét tényezőket, míg a mérték (metric) két vagy több méréssel, hosszabb időn át egy előre meghatározott irányvonal méréseinek összehasonlítása.

A COBIT 4.1-ben szereplő biztonsági mértékek, az alábbi pontokban találhatók:

P01.4	IT Strategic Plan
P01.5	IT Tactical Plan
P02.3	Data Classification Scheme
P02.4	Integrity Management
P03.2	Technological Infrastructure Plan
P04.6	Establishment Roles and Responsibilities
P04.7	Responsibility for IT Quality Assurance
P04.8	Responsibility for Risks, Security and Quality,
P04.9	Data and System Ownership
P04.11	Segregation Duty
P07	Manage IT Human Resources
P09	Asses and Manage IT Risks
AI1.2	Risk Analysis Report
AI3.2	Infrastructure Resource Protection and availability
AI6.1	Change Standards and Procedures
DS1.2	Definition of Services
DS1.3	SLA
DS2.3	Supplier Risk Management
DS3.1	Performance and Capacity Planning
DS3.4	IT Resources Availability
DS4	Ensure Continuous Service
DS5	Ensure System Security
DS7.1	Identification of Education and Training Needs
DS7.2	Delivery of Training and Education
DS7.3	Evaluation of Training Received
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10.1	Identification and Classification of Problem
DS10.2	Problem Tracking and Resolution
DS11.5	Back up and Restoration
DS11.6	Security Requirements for Data Management
DS12	Manage Physical Environment
DS13.4	Sensitive Documents and Output Devices
ME2.1	Monitoring of Internal Control Framework
ME3.3	Evaluation of Compliance with Regulatory Requirements
ME4.4	Resource management
ME4.5	Risk Management
ME4.6	Performance measurement
ME4.7	Independent assurance

6. KOCKÁZATFELMÉRÉSI JELENTÉS FELÉPÍTÉSE

A kockázat felmérési jelentés a fentiek alapján egyaránt tartalmazza a vállalati szintű, az üzleti-, és az információs rendszerben feltártakat, mind egyiket a megfelelő részben.

6.1. SZERVEZÉSI KOCKÁZATFELMÉRÉS

6.1.1. A vállalati üzleti stratégia (küldetés)

6.1.2. Szabályzatok

6.1.2.1. Szervezet és működés szabályozása

6.1.2.1.1. A vállalat, üzleti és/vagy az informatikai szervezet

6.1.2.1.2. Biztonsági infrastruktúra

6.1.2.1.3. A biztonság hatékonysága

6.1.2.1.4. Tűzvédelmi szervezet

6.1.2.1.5. Polgári védelmi szervezet

6.1.2.2. Biztonsági alapdokumentumok

6.1.2.3. Adat, és titokvédelem szabályozása

6.1.2.3.1. Személyes adatok

6.1.2.3.2. Adatok, értékek

6.1.2.3.3. Eszközök

6.1.2.3.4. Eljárások

6.1.2.3.5. Helyiségek

6.1.2.4. Iratkezelés szabályozása

6.1.3. Humánpolitikai intézkedések

6.1.3.1. Munkaviszony létesítés, és megszüntetés

6.1.3.2. Munkakör csere

6.1.3.3. Teljesítménykövetés

6.1.3.4. Karrier menedzsment

6.1.3.5. Feladatok meghatározása és szétválasztása

6.1.3.6. Biztonsági kultúra, biztonsági tudatosság képzés, propaganda

6.1.3.7. Oktatás

6.1.3.8. Csalás elleni politika

6.1.3.9. Ipari kémkedés elleni politika

6.1.4. Szerződések

6.1.4.1. Szerződés harmadikféllel

- *Outsourcing*
- *SLA_SLM*

6.1.4.2. Kockázat áthárítás

6.1.5. Biztonsági események kezelésének rendje

6.2. TECHNIKAI KOCKÁZATFELMÉRÉS

6.2.1. IR erőforrások

6.2.1.1. Adatok

6.2.1.2. HW architektúra

6.2.1.3. Rendszer sw-ek listája

6.2.1.4. Alkalmazói sw-ek

6.2.1.4.1. Asw-ek listája

6.2.1.4.2. Tulajdonosok, felhasználók listája

6.2.1.4.3. Asw-ek rsw igénye

6.2.1.4.4. Egyéb berendezések

6.2.1.5. Dokumentációk

6.2.2. Az üzleti rendszer erőforrásai

6.2.2.1. Adatok, értékek

6.2.2.2. Üzleti, és támogató folyamatok

6.2.2.3. Ügyvitel automatizálási eszközök

6.2.2.3.1. Pénztárgépek, pénzfeldolgozó berendezések

6.2.2.3.2. Sokszorosító gépek

6.2.2.3.3. Irattározási eszközök

6.2.2.3.4. Kommunikációs eszközök (fax, távbeszélő)

6.2.2.3.5. Hulladék megsemmisítő berendezések

6.2.2.3.6. Egyéb

6.2.2.4. Ember

6.2.2.5. Támogatások, létesítmények

6.2.2.5.1. Logisztikai berendezések

6.2.2.5.2. Épületek, raktárak, értéktárak

6.2.2.5.3. Árú szállító eszközök

6.2.2.5.4. Árú mozgató rendszerek, eszközök

6.2.2.5.5. Egyéb

6.2.2.6. Intelligens épület eszközei

6.2.2.6.1. Energiaellátás eszközei

6.2.2.6.2. Légkondicionáló rendszer

6.2.2.6.3. Személyközlekedést kiszolgáló berendezések

6.2.2.6.4. Egyéb kisegítő eszközök

6.2.3. Fizikai hfv

6.2.3.1. Aktív támadás elleni védelem

6.2.3.1.1. Épületautomatika

6.2.3.1.2. Belépés és mozgás ellenőrzés

6.2.3.1.3. Behatolás-védelem

6.2.3.1.4. Értéktárolás

6.2.3.1.5. Értékszállítás

6.2.3.1.6. Üres íróasztal, és képernyő politika

6.2.3.2. Passzív támadás elleni védelem

6.2.3.2.1. Elektromágneses kisugárzás, villámvédelem

6.2.3.2.2. Akusztikus kisugárzás

6.2.3.2.3. Hulladékmegsemmisítés

6.2.4. Fizikai rendelkezésre állás

6.2.4.1. Energiaellátás

6.2.4.2. Tűzvédelem

6.2.4.3. Klimatizálás

6.2.4.4. Megbízhatóság

6.2.4.5. Beszéd kommunikációs eszközök

6.2.4.6. Dokumentáció

6.2.4.7. Karbantartást ellátók

6.2.5. Logikai hfv

6.2.5.1. Aktív támadások elleni védelem

6.2.5.1.1. Jelszó és jogosultság mgm

6.2.5.1.2. A rendszerszoftverek

6.2.5.1.3. Tartalomhitelesítés

6.2.5.1.4. Hozzáférési útvonalak

6.2.5.1.5. Time out

6.2.5.1.6. Logikai behatolás jelzés

6.2.5.2. Passzív támadás elleni hfv

6.2.6. Logikai rendelkezésre állás

6.2.6.1. Vírusvédelem

6.2.6.2. Mentés, újraindítás

6.2.6.3. Logikai rombolás

6.2.6.4. Dokumentáció

6.2.6.5. Rendszerkövetés

6.2.7. Hálózatok

6.2.7.1. Típusok, alkalmazási helyük

6.2.7.2. Védelmi intézkedések (a helyi LAN , és WLAN hálózatokon)

6.2.7.3. Az ISMS INTERNET CHECKLIST a tűzfalakról készített anyag

6.2.7.4. Nem bizalmas hálózati kapcsolatok

6.2.7.5. Beszéd hálózat

6.2.7.6. Elektronikus kereskedelem ISMS INTERNET Checklist alapján

6.2.8. Védelem az IR életciklus során

6.2.8.1. Indítás

6.2.8.1.1. A rendszer szükségességének meghatározása

6.2.8.1.2. A rendszer céljának dokumentálása

6.2.8.2. Fejlesztés

6.2.8.2.1. Fejlesztési környezet

6.2.8.2.2. Biztonsági követelmények a fejlesztendő rendszerben

6.2.8.3. A harmadik félnél fejlesztett rendszer szállítása

6.2.8.3.1. A szállítás alatti biztonság biztosítása

6.2.8.4. Átadás/átvétel

6.2.8.4.1. Megfelelősség ellenőrzése

6.2.8.4.2. A védelmi intézkedések végrehajtásának ellenőrzése

6.2.8.5. Üzemeltetés

6.2.8.6. Selejtezés

6.3. SZÁMON KÉRHETŐSÉG

6.3.1. Elrettentés

6.3.2. Információk számon kérhetőségének biztosítása

6.3.2.1. Audit trail

6.3.2.2. Accountok audit logjai

6.3.2.3. Beléptető rendszerek naplói

6.3.2.4. Behatolás jelzőrendszerek logjai

6.3.3. A szerepek, felelősségek allokációja

6.3.4. Informatikai eszközök leltára

6.3.4.1. ***információ-vagyontárgyak:*** adatbázisok és adatállományok, rendszerdokumentáció, használói/kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, újraindítási eljárások, tartalékolási elrendezések, archivált információk,

6.3.4.2. ***szoftver-vagyontárgyak:*** alkalmazási szoftverek, rendszerszoftver, fejlesztési segédanyagok és eljárásrend

6.3.4.3. ***fizikai vagyontárgyak:*** *számítógépek és tartozékegységeik, mint processzorok, monitorok, hordozható számítógépek (*laptopok*), modemek; a távközlési berendezések, mint átirányítók (*routerek*),* al-központok (PABX-ek), távmásoló fax-gépek, telefon hívásfogadó és válaszoló berendezések; egyéb műszaki berendezések, mint a tápá-ram ellátó, vagy a légkondicionáló egységek; a bútorok és az egyéb kiszolgáló helyiségek berendezései,

6.3.4.4. ***szolgáltatások:*** *számítástechnikai és távközlési (*"számítóges" és "kommunikációs*") szolgáltatások, általános (köz)szolgáltatások, mint a fűtés, a világítás, a villamosenergia-ellátás, a légkondícionálás.*

6.3.5. Az üzleti rendszerhez alkalmazott eszközök számon kérhetősége, leltára

6.4. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

6.5. A MOBIL SZÁMÍTÁSTECHNIKAI ESZKÖZÖK VÉDELME

6.5.1. A mobil számítástechnikai eszközök védelme

6.6. HIVATKOZÁSOK

6.6.1. Elfogadó Nyilatkozat

6.6.2. Dokumentumok jegyzéke

6.6.3. Interjú alanyok jegyzéke

6.6.4. Szemlék jegyzéke

7. A VESZÉLYFORRÁS ELEMZÉS VÉGREHAJTÁSA

7.1. A VESZÉLYFORRÁS ELEMZÉS CÉLJA

A veszélyforrás elemzés célja, hogy a kockázatfelmérés alapján meghatározza az erőforrások bizalmasságát, sértetlenségét, és rendelkezésre állását, fenyegető gyengeségeket, amelyek következtében egy támadás eredményeképpen nem kívánt állapot jöhet létre, azaz azonosítsa a kockázatokat. A veszélyforrás elemzés során

- ⇒ *vizsgálni kell a védelmi intézkedések megfelelősségét, azaz azt, hogy a védelmi követelményeknek eleget tesznek-e, és a védelmi intézkedések megfelelő erősségűek-e. Amennyiben*
  - *korábban készült kockázat menedzsment, mi történt a feltárt veszélyforrásokkal,*
  - *van érvényes Biztonsági Politika, és Katasztrófaterv, a specifikált védelmi intézkedések kikényszerítik-e az azokban meghatározott védelmi követelményeket,*

- ⇒ *vizsgálni kell a megvalósítást, azaz azt, hogy*
  - *a védelmi intézkedések gyakorlata nem gyengíti-e a kitűzött védelmi követelményeket,*
  - *amennyiben van érvényes Biztonsági Szabályzat az a gyakorlatban végrehajtásra kerül-e, és*

- ⇒ *a feltárt védelmi gyengeségeket a jelentésben rögzíteni kell.*

7.2. A VESZÉLYFORRÁS ELEMZÉS ALAPJA

A veszélyforrás elemzést a kockázatfelmérés során rögzítettek alapján kell elvégezni. Ugyanakkor célszerű, a későbbi kockázatfelmérésekhez, és veszélyforrás elemzésekhez a már feltárt veszélyforrásokat egy adatbázisban összegyűjteni. Az adatbázisban egy veszélyforrásról a következő adatokat javasolt tárolni:

- ⇒ *A veszélyforrás neve*
- ⇒ *A veszélyforrás jelentkezésének leírása.*
- ⇒ *A feltárás helye (vállalat), és időpontja*
- ⇒ *A bekövetkezése mire jelent fenyegetést (C,I,A)*
- ⇒ *A bekövetkezés esetén a sebezhetőség (részleges, átfogó)*
- ⇒ *A támadás módszere (aktív, passzív)*

A veszélyforrás elemzést vállalati szinten, és az üzleti (illetve, ha van termelési) valamint informatikai folyamatokra is el kell végezni.

7.3. A VESZÉLYFORRÁS ELEMZÉS FELÉPÍTÉSE

A Jelentés felépítése a 8. fejezetben található, amely mindazon területeket tartalmazza, ahol gyengeségek, veszélyforrások lehetnek. Ezért amennyiben egy területen nem került veszélyforrás feltárásra, e tényt a Jelentésben fel kell tüntetni.

7.4. A VESZÉLYFORRÁS ELEMZÉS KÉSZÍTÉSE

7.4.1. A Veszélyforrás elemzés kidolgozása

A veszélyforrás elemzés folyamatábrája a következő oldalon található. A feltárt védelmi gyengeségeket úgy kell megadni, hogy minden veszélyforrásnak

- ⇒ *legyen egyedi azonosítója, amely a későbbiekben a hivatkozást lehetővé teszi,*
- ⇒ *általános szakmai magyarázat biztosítsa a Megbízó számára a gyengeségek megértését,*
- ⇒ *rá kell mutatni arra, hogy az adott vállalatnál miért léphet fel a veszélyforrás. Az ok lehet*
  - *védelmi intézkedés hiánya,*
  - *nem megfelelő védelmi intézkedés*
  - *megfelelő védelmi intézkedés, nem megfelelő végrehajtási gyakorlata.*

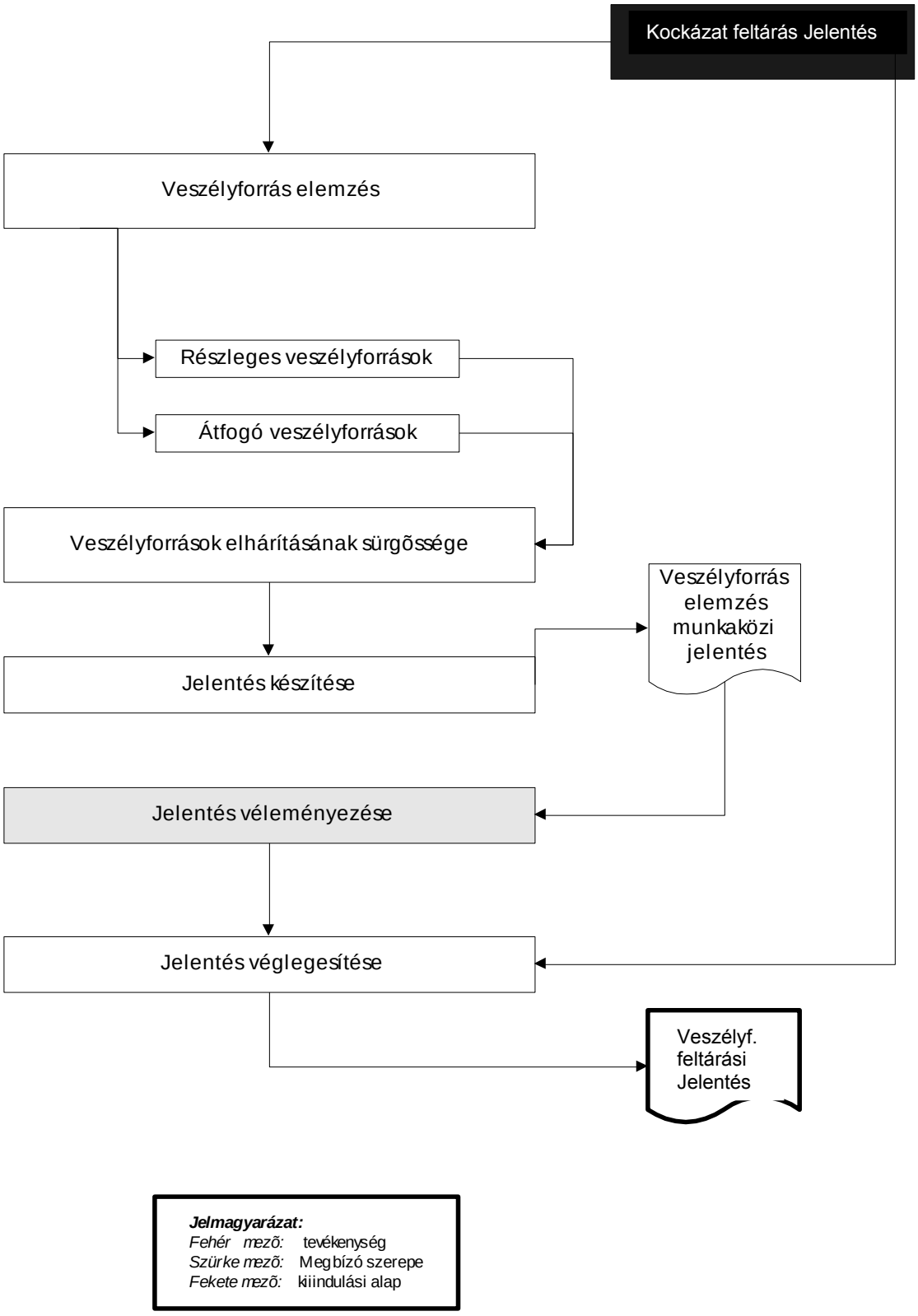
A veszélyforrás elemzés alapján az IR biztonsági érettségi szintjét (level 0-5) a COBIT3 DS5 ENSURE SECURITY Maturity Model alapján, az átvilágítás lezárásaként (a sok problémát okozó sürgősség helyett) meg kell adni, és ügyelni kell arra, hogy az MM szint nem mondhat ellent a későbbiekben meghatározandó ellenálló képességnek. Az összefüggések:

R Ellenálló képesség	MM Érettségi Modell
Nem ellenálló	Level 0,1
Nyilvánvalóan ellenálló	Legalább level 2
Mérsékelten ellenálló	Legalább level 3
Magasan ellenálló	Legalább level 4,5

7.4.2. A Megbízó szerepe

A Megbízónak nem lehet lehetőséget adni arra, hogy a szakértők véleményét megváltoztassa. A Megbízó mozgástere ott, van, hogy módjában lesz a veszélyforrás elemzés alapján elkészített kockázatelemzés ismeretében a kockázat felvállalásáról, azaz arról dönteni, hogy nem tesz védelmi intézkedést, vagy gyengébb védelmi intézkedést tesz. A Megbízó ellenvéleményét, azonban a Jelentésben szerepeltetni kell.

A VESZÉLYFORRÁS ELEMZÉS FOLYAMATÁBRÁJA


Kockázat feltárás Jelentés
Veszélyforrás elemzés
Részleges veszélyforrások
Átfogó veszélyforrások
Veszélyforrások elhárításának sürgõssége
Veszélyforrás elemzés munkaközi jelentés
Jelentés készítése
Jelentés véleményezése
Jelentés véglegesítése
Veszélyf. feltárási Jelentés
Jelmagyarázat:
Fehér mezõ: tevékenység
Szürke mezõ: Megbízó szerepe
Fekete mezõ: kiindulási alap

7.4.3. A kritikus pontok

A szakértőnek a következőkre kell figyelnie:

- ⇒ *nem lehet olyan veszélyforrást megadni, amelyet a Kockázat felmérési jelentés nem támaszt alá,*
- ⇒ *a veszélyforrások leírása nem tartalmazhat, de nem is utalhat konkrét védelmi intézkedésre,*
- ⇒ *a veszélyforrást annak tudatában kell meghatározni, hogy arra a Biztonsági politikában védelmi intézkedést kell javasolni,*
- ⇒ *a veszélyforrás elhárításának sürgőssége nem mondhat ellent a kockázat értékelésnél megadásra kerülő bekövetkezési valószínűségnek,*
- ⇒ *a sürgősség meghatározásánál nem lehet a védelmi intézkedés esetleges költségeit figyelembe venni. A hosszabb intézkedési idő csak a Megbízó tudatos kockázat vállalásán alapulhat,*
- ⇒ *A Kockázat menedzsmentet követően még a javasolt védelmi intézkedések nem állnak rendelkezésre, ezért ekkor még nem kívánatos védelmi intézkedést tenni, és erre a Megbízó figyelmét fel kell hívni. A gyakorlatban tapasztaltak szerint ugyanis a Megbízók a veszélyforrás elemzést megismerve azonnali intézkedési kényszert éreznek!!*

8. TIPIKUS BIZTONSÁGI VESZÉLYFORRÁSOK

8.1. VESZÉLYFORRÁS ADATBÁZIS

Célszerű a feltárt veszélyforrásokról adatbázist létrehozni, a későbbi munka segítésére. Az egyes veszélyforrásokról azok nevét, feltárási helyét, és leírását ajánlott rögzíteni. Az üzleti veszélyforrások általában

8.2. VÁLLALATI SZINTŰ BIZTONSÁGI VESZÉLYFORRÁSOK

A vállalati szintű biztonsági veszélyforrások alapvetően azzal függnek össze, hogy a biztonságszervezés nem rendszerszemlélettel történt. A vállalati szintű veszélyforrások:

- *belső (infrastruktúra, személyek, folyamatok, technológia),*
- *külső (politikai, gazdasági-pénzügyi, üzleti, szociális, természeti, technológiai).*

A biztonsági veszélyforrások a működési veszélyforrások közé tartoznak.

A fő vállalati szintű működési veszélyforrások:

- *A nem integrált biztonsági alrendszerek, az összehangolatlan fizikai, logikai, humán, védelmi intézkedések.*
- *A vállalati szintű biztonsági dokumentumok.*
- *A biztonsági események nem vállalati szintű értékelése, kezelése.*
- *A szervezeti kultúra, és ezen belül a biztonsági kultúra összehangolt kezelése.*
- *A vállalati szintű kockázat menedzsment (ERM [62]) hiánya.*

8.3. A VÁLLALATI VESZÉLYFORRÁSOK

A vállalati veszélyforrások lehetnek

- *Belső, és*
- *Külső veszélyforrások.*

Ezekre a COSO II. szerinti példák a következő oldalon olvashatók.

VESZÉLYFORRÁSOK	
KÜLSŐ	**BELSŐ**
GAZDASÁGI • *a tőke rendelkezésre állása* • *hitel* ➢ *kibocsátás* ➢ *feltételek* ➢ *összpontosítás* • *likviditás* ➢ *piac* ➢ *alapjuttatás* ➢ *készpénzforgalom* • *piac* ➢ *árak* ➢ *kamat %* ➢ *munkanélküliség* ➢ *indexek* ➢ *árfolyam* ➢ *részvényértékelés* ➢ *ingatlanok értéke* • *üzlet* ➢ *védjegy* ➢ *verseny* ➢ *vásárlói magatartás* ➢ *partnerek* ➢ *csalás* ➢ *szabványok* ➢ *tulajdonosi struktúra* ➢ *nyilvánosság* ➢ *termék fontossága* ***TECHNOLÓGIA*** • *e. kereskedelem* • *külső adatok* • *vészhelyzet technológia* ***TERMÉSZET, KÖRNYEZET*** • *biológiai változás* • *kibocsátás, pusztítás* • *energia* • *tűz* • *természeti katasztrófa* • *fenntartható növekedés* • *szállítás* • *víz* ***POLITIKAI*** • *kormányzat csere* • *jogalkotás* • *nyilvános politika* • *szabályozás* ***SZOCIÁLIS*** • *demográfia* • *közösséghez tartozás* • *környezeti gondoskodás* • *magánélet*	***INFRASTRUKTÚRA*** • *erőforrások rendelkezésre állása* • *erőforrások képességei* • *tőke hozzáférés* • *bonyolultság* • *vállalati fúzió* • *eszközbeszerzés* ***HUMÁN*** • *munkatársak képességei, tudásuk* • *csalás* • *egészség, életbiztonság* • *vélemény, nézet* • *biztonsági gyakorlat* • *értékesítési gyakorlat* ***FOLYAMATOK*** • *kapacitás* • *tervezés* • *végrehajtás* • *szállítók/függőségek* ***TECHNOLÓGIA*** • *adat* ➢ *hozzájutás* ➢ *karbantartás* ➢ *elosztás* ➢ *bizalmasság* ➢ *sértetlenség* • *adat, és rendszerrendelkezésre állása* • *kapacitás* • *rendszer* ➢ *kiválasztás* ➢ *fejlesztés* ➢ *telepítés* ➢ *megbízhatóság*

8.4. AZ ÜZLETI RENDSZER BIZTONSÁGI VESZÉLYFORRÁSAI

Az üzleti, és támogató folyamatok, képezte veszélyforrások biztonsági szempontból a működési veszélyforrások (kockázatok) közé tartoznak, amelyek elsősorban

- *nem megfelelően végrehajtott vagy*
- *kiesett üzleti folyamatok, és*
- *az infrastruktúra kiesése,*

amelyek emberek, rendszerek, és az üzleti folyamatok végzését lehetővé tevő infrastruktúra kiesése, vagy külső események miatt következnek be, és üzleti veszteséghez vezetnek.

A továbbiakban egyaránt szerepelnek az üzleti-, és az információs rendszer biztonsági veszélyforrásai (lásd a Bevezetésben megadott átfedéseket).

8.5. SZERVEZÉSI VESZÉLYFORRÁSOK (RÉSZLEGES)

8.5.1. Szabályzatok

8.5.1.1. Szervezet és működés nem a biztonsági követelmények szerint szabályozott

8.5.1.1.1. Szervezet, és a működési gyakorlat nem felel meg a biztonsági követelményeknek

+ *Az informatikai szervezet nem integrált, hanem követi a szigetmegoldásokat, az informatikai fejlesztés, üzemeltetés nem centralizált.*

8.5.1.1.2. Biztonsági szervezet és működés nem felel meg a biztonsági követelményeknek

+ *Nincs szervezet biztonsági infrastruktúra*
+ *A biztonsági szervezet vezetője nem az első számú vezető alárendeltségében van.*
+ *Az informatikai, és vagyonbiztonsági szervezet nem egységesen menedzselt.*
+ *Az IT biztonság, és a vagyonbiztonság az egységes szervezetben nem szétválasztott.*
+ *Az IT biztonság szakmai menedzsmentjét nem a biztonsági szervezet látja el.*
+ *Az IT biztonság hatékonyságának mérésére nincs kidolgozott módszer.*

8.5.1.1.3. Tűzvédelmi szervezet és működés nem felel meg a tv-nek

+ *A tűzvédelmi szervezet nem felel meg a hatályos jogszabályoknak.*

8.5.1.1.4. Polgári védelmi szervezet és működés nem felel meg a tv-nek

+ *A polgári védelem nem felel meg a hatályos jogszabályoknak.*

8.5.1.2. Biztonság naprakészen nem rendszerszervezett

+ *Nem állnak rendelkezésre a biztonsági dokumentumok, éspedig*

  - *Kockázat menedzsmenti jelentés,*
  - *Biztonsági Stratégia,*
  - *Biztonsági Politika,*
  - *Katasztrófaterv, és*
  - *Biztonsági Szabályzat.*

8.5.1.3. Titokvédelem szabályozása nem naprakész a biztonsági követelmények szerint

+ *A titokvédelem nem szabályozott.*

  - *Nincs Titokvédelmi szabályzat.*
  - *Nincs titokvédelmi felügyelő.*
  - *Az adatvédelem nem szabályozott, és nincs elválasztva a biztonsági szervezettől.*
  - *Az adatok, és/vagy értékek, és/vagy eljárások (informatikai alkalmazások), és/vagy eszközök, és/vagy helyiségek nincsenek biztonsági szempontból minősítve (osztályozva), azaz nem jelenik meg a védelem szükségessége, és a biztonság érzékenységgel arányos biztonsági meghatározása sincs a védelem tárgyai között kialakítva, valamint az osztályozás adathordozótól függetlenül nem kíséri az adatot teljes életciklusa során.*
  - *Az adatok tulajdonosai, és a felelősségük nincs meghatározva.*
  - *Az elektronikusan tárolt adatok sértetlenségének biztosítása nem szerepel a követelmények között.*
  - *Az osztályozás nincs az egész vállalatra elvégezve.*

8.5.1.4. Iratkezelés szabályozása nem naprakész, mind a papír, mind az elektronikus alapú iratoknál

+ *Az elektronikus iratok kezelése, megőrzése nem szabályozott.*
+ *Nem szabályozott a hitelesség biztosítás a papíralapú iratból az elektronikus iratra, és fordítva történő átmenetnél.*

8.5.2. Humánpolitikai intézkedések

8.5.2.1. Munkaviszony létesítés és megszüntetés naprakészen nem felel meg a biztonsági követelményeknek

+ *A munkaviszony létesítésénél a megbízhatóság ellenőrzése nem szabályozott vagy gyenge.*
+ *A munkaviszony megszüntetésénél a hozzáférési jogosultságok visszavonása nem szabályozott.*

8.5.2.2. Feladatok meghatározása és szétválasztása elméletben, és gyakorlatban nem felel meg a biztonsági követelményeknek

+ *Nincsenek munkaköri leírások, illetve nem fedik le a gyakorlatot.*
+ *A szerepek betöltői számára, nincs meghatározva a felelősségük, viszonyuk a menedzsment politikájához, a folyamatokhoz, a IT biztonsághoz, a belső ellenőrzéshez, és a szabályzatokhoz.*
+ *A biztonságkritikus feladatok nincsenek szétválasztva az informatika területén, az informatikai és biztonsági funkciók között, mint*

  - *az adatvédelmi, és az IT biztonsági munkakörök,*
  - *az IT biztonsági, és informatikai munkakörök,*
  - *informatikai fejlesztés, és üzemeltetés,*
  - *az informatikai üzemeltetés, és az adatellenőrzés,*
  - *az informatikai üzemeltetés, és karbantartás,*
  - *az informatikai üzemeltetés, és a felhasználás.*

8.5.2.3. Teljesítménykövetés nem terjed ki minden munkatársra

+ *A munkatársak életvitelében bekövetkező biztonságkritikus változásokat a teljesítményértékelés nem követi, nincs humánpolitikai intézkedési terv erre vonatkozólag.*
+ *Nincs kidolgozott módszer a bizalmasság védelmére a munkakörök cseréje, illetve megszüntetése esetére.*

8.5.2.4. A biztonsági kultúra szintje nem felel meg a vállalat meghatározott biztonsági szintjének

+ *Nincs folyamatos Biztonsági kultúra, biztonsági tudatosság program.*
+ *A biztonsági kultúra, és a biztonsági tudatosság nem felel meg a vállalat biztonsági szintjének.*
+ *A biztonsági kultúra, és ezen belül a biztonsági tudatosság nem egyenszilárdságú.*
+ *A munkatársak biztonsági tudatosságának láncolata nem képez ellenállóképes humán tűzfalat.*

8.5.2.5. Csalás elleni politika elméletben, és gyakorlatban nem felel meg a biztonsági követelményeknek

+ *Nincs csalás elleni politikája kidolgozva a vállalatnak.*

8.5.2.6. Az ipari kémkedés elleni politika nem megfelelő

+ *Nincs ipari kémkedés elleni politika vagy nem megfelelő*
+ *A politika nem jelenik meg az Adatvédelmi Utasításban, és annak alkalmazása nem terjed ki a humán, fizikai, logikai védelemre egyaránt.*

8.5.2.7. Oktatás nem naprakész

+ *Az oktatás nem követi a szakmai követelmények változásait.*
+ *A biztonsági tudatosság folyamatos biztosítása nem megoldott.*

8.5.2.8. Humán veszélyforrások a NIST Special Publication 800-30 alapján

A következő oldalon látható táblázat a humán veszélyforrások jó összefoglalását adja a bűntető jogi következményeket is magával vonható humán veszélyforrásoknak:

Veszélyforrás	Motiváció	Támadás
Hacker, Cracker	*Kihívás,* *Ego,* *Lázadás*	*Hacker támadás* *Megtévesztés (social engeneering)* *Behatolás,* *Jogosulatlan rendszer hozzáférés*
Számítástechnikai Bűnöző	*Információ,* *Illegális információ felfedés,* *Anyagi haszon,* *Jogosulatlan adat megváltoztatás,*	*Számítógépes bűnözés,* *Csalás,* *Megvesztegetés,* *Becsapás,* *Behatolás a rendszerbe,*
Terrorista	*Zsarolás,* *Rombolás,* *Haszonszerzés,* *Megtorlás,*	*Bomba,* *Információs hadviselés,* *Rendszer támadása,* *Behatolás a rendszerbe,* *Rendszer lehallgatás,*
Ipari kém (cégek, kormányok érdekében)	*Verseny előny,* *Gazdasági (üzleti) hírszerzés,*	*Gazdasági haszonszerzés,* *Információlopás,* *Magánéletbe behatolás,* *Rendszerbe behatolás,* *Megtévesztés,* *Jogosulatlan rendszer hozzáférés,*
Belső munkatárs (rosszul képzettek, elégedetlenek, tisztességtelenek, elbocsátottak)	*Kíváncsiság,* *ego,* *intelligencia,* *anyagi érdek,* *bosszúállás,* *véletlen hiba,*	*Munkatárs megtámadása,* *Zsarolás,* *Magán információk szerzése,* *Csalás, lopás,* *Megvesztegetés,* *Hamis adatok bevitele,* *Információ elfogás,* *Rosszindulatú kódok,* *Rendszer lehallgatás,* *Szabotázs,* *Jogosulatlan hozzáférés.*

8.5.3. Szerződések

8.5.3.1. Szerződés harmadikféllel nem felel meg a biztonsági követelményeknek

+ *Az outsourcing szerződések nem tartalmaznak biztonsági követelményeket a harmadikfél a szervezet területén munkát végző munkatársaira, tevékenységére, termékeire.*
+ *A biztonsági védelmi eszközök, és az informatikai termékek beszerzésénél, nincsenek érvényesítve biztonsági követelmények*
  - *a fejlesztési környezetre,*
  - *a termék veszélyforrás mentességének garantálására,*
  - *a jogtisztaságra.*
+ *A karbantartásnál, a rendszerkövetésnél, és az outsourcingnál nincsenek érvényesítve biztonsági követelmények*
+ *Nincs, vagy nem megfelelő az SLA-SLM. A minimális szolgáltatási szint megállapításánál nem vették figyelembe a küldetés kritikus folyamatok, alkalmazások sebezhetőségi ablakait.*
+ *Megfelel-e a COBIT 4.1 által előírt szolgáltatási szint megállapodás követelményeinek (SLA, lásd I. kötet. 4.1.7. pontban).*

8.5.3.2. Kockázat áthárítás nem naprakészen teljes körű

+ *A vagyonbiztosítás hiánya.*
+ *Az üzleti tevékenység megszakadására nincs biztosítás.*

8.5.3.3. Nincs a biztonsági események kezelése szabályozva

8.6. TECHNIKAI VESZÉLYFORRÁSOK (RÉSZLEGES)

8.6.1. Fizikai hfv

8.6.1.1. Aktív támadás elleni hozzáférés-védelem nem teljes körűen korlátozza a hozzáférést

8.6.1.1.1. Épületautomatika

+ *Nincs integrált épületautomatika felügyeleti rendszer.*
+ *Nincs, és/vagy nem egységesen menedzselt a biztonsági felügyelet az épület felügyelettel.*

8.6.1.1.2. Belépés és mozgás ellenőrzés

+ *Nincsen az objektumokon belül a helyiségeknek funkcióik alapján védelmi osztályozásuk.*
+ *A belépés, és mozgás ellenőrzés rendszere nem felel meg a helyiségek funkciói alapján meghatározott biztonsági osztályozásának.*

+ *A belépés ellenőrzés nincs kiegészítve mozgás ellenőrzéssel.*

8.6.1.1.3. Behatolás-védelem

+ *A behatolás védelem nem a helyiségek biztonsági osztályozása szerint van kiépítve, a behatolás jelző rendszerek nem megfelelő biztonsági fokozatba soroltak és/vagy a környezeti osztályozásuk nem megfelelő.*

8.6.1.1.4. Értéktárolás

+ *Nincs időzárás értéktárolás a pénzkezelésnél.*
+ *Az értékek tárolásának fizikai védelme nem felel meg a MABISZ előírásainak.*

8.6.1.1.5. Értékszállítás

+ *Az értékek szállítása (tipikusan a pénzszállítás) végponttól végpontig nem egyenszilárdságú (nem felel meg a MABISZ előírásainak).*

8.6.1.1.6. Mobil számítástechnikai eszközök védelme nem megfelelő

+ *A mobil eszközöknek nincs felelős gazdája*
+ *A mobil eszközök fizikai, és logikai védelme nem megoldott*
+ *A mobil eszközök, mobil adathordozók csatlakoztatási feltételei nem szabályozottak.*

8.6.1.1.7. Üres íróasztal politika, sötét képernyő

+ *Nem követelmény és/vagy gyakorlat, távollét esetén az író-, illetve munkaasztaloknak az üresen tartása, a számítógép kikapcsolása..*

8.6.1.2. Passzív támadás elleni hozzáférés-védelem nem teljes körűen korlátozza a hozzáférést

8.6.1.2.1. Elektromágneses kisugárzás

+ *A biztonságkritikus helyiségek (pl. számítógépterem) nem védettek vagy nem megfelelő frekvencia sávban védettek az elektromágneses kisugárzás ellen.*

8.6.1.2.2. Akusztikus kisugárzás

+ *A biztonságkritikus helyiségek (pl. felső vezetés tanácsterme) nem védettek akusztikus kisugárzás ellen.*

8.6.1.2.3. Hulladékmegsemmisítés

+ *A papíralapú adathordózók megsemmisítése, és selejtezése nem szabályozott, nem biztosított a megsemmisítés tényének tételes bizonyítása.*

8.6.2. Fizikai rendelkezésre állás

8.6.2.1. Energiaellátás nem biztosítja a folyamatos rendelkezésre állást

+ *Nem biztosított a kritikus eszközök szünetmentes áramellátása.*
+ *A többirányú betáplálás nem egyenszilárdságú.*

8.6.2.2. Tűzvédelem nem rendeltetésszerű

+ *A tűzvédelmi rendszer nem felel meg maradéktalanul a hatályos jogszabályoknak.*

8.6.2.3. Beszéd kommunikáció nem biztosítja rendeltetésszerűen a biztonsági követelményeket

+ *A karbantartó cég távdiagnosztizálási kötelezettsége, jogosultsága nincs biztonsági követelményeknek alárendelve.*
+ *Nincs rendszer redundancia a biztonságkritikus munkahelyek számára.*

8.6.2.4. Klimatizálás nem biztosítja a folyamatos rendelkezésre állást

+ *Nem alkalmaznak klímát a kritikus légállapotú helyiségekben, vagy nem megfelelőek az alkalmazott rendszer paraméterei.*

8.6.2.5. Megbízhatóság nincs megfelelő redundanciával biztosítva

+ *Nincs kidolgozva, és meghatározva a folyamatos működés megszakadásának tűrőképessége (sebezhetőségi ablak).*
+ *Az eszközök, különösen a biztonságkritikus eszközök, rendelkezésre állási követelményei nem felelnek meg, illetve nincs eszköz redundancia.*

8.6.2.6. Dokumentáció nem naprakész, és teljes körű

+ *Az értékrendszer, és az információs rendszer hardver elemeinek dokumentációja nem naprakész, és teljes.*

8.6.2.7. Karbantartást ellátókkal szemben nincsenek maradéktalanul érvényesítve a biztonsági követelmények

+ *A belső, és az outsourcing karbantartók, rendszerkövetőkkel szemben nincsenek érvényesítve a biztonsági követelmények.*

8.6.3. Logikai hfv

8.6.3.1. Aktív támadás elleni hozzáférés-védelem nem korlátozza megfelelően a hozzáférést

8.6.3.1.1. Jelszó és jogosultsági rendszer

+ *Nincs bizalmas számítástechnikai bázis vagy az erőssége a védendő titkok osztályozásának, nem felel meg.*
+ *A hozzáférés védelem megkerülhető (különösen kritikus nem integrált információ-rendszer esetében).*
+ *A hozzáférés -védelmi szoftver hozzáférés - védelme nem biztosított.*
+ *A hozzáférés -védelemmel kapcsolatos szerepek nincsenek egymástól, és az üzemeltetési feladatoktól szétválasztva.*
+ *A hozzáférés -védelmi szoftverek együttműködése (interoperabilitása) nem biztosított, mindegyik más védelmi szintet képvisel (pl. az adatbázis kezelő, és az operációs rendszer bizalmas számítástechnikai bázisa).*
+ *Nincs (pl. bankoknál) kényszer hatása alatti bejelentkezés riasztás.*
+ *Nincs az objektumok újra felhasználásánál felfedés elleni védelem*
+ *Njncs vállalati szintű azonosság kezelés, és egyszeri jelszó használat (SSO)*

8.6.3.1.2. Hitelességvédelem

+ *Nem alkalmaznak a belső, és/vagy külső levelezésben tartalmi hiteleség védelmet.*
+ *A hitelesség védelem eszközeinek védelme gyenge.*
+ *A hozzáférés -védelmi szoftver hitelesség-védelme nem biztosított.*

8.6.3.1.3. Time out

+ *Az aktivitás szünetelése esetén nem alkalmaznak, akár az alkalmazói szoftverbe, akár az adatbázis kezelő rendszerbe történő belépés engedélyezést követően, viszony megszakítást.*

8.6.3.1.4. Logikai behatolás védelem

+ *Nem alkalmaznak logikai behatolás jelző, vagy védelmi rendszert.*

8.6.3.2. Passzív támadás elleni hozzáférés –védelem nem felel meg a biztonsági követelményeknek

+ *A biztonságkritikus belső, illetve külső kapcsolatokban nem alkalmaznak rejtjelezést.*
+ *A rejtjelezési eszközök bizalmasságának védelme nem megoldott.*
+ *Az algoritmus erőssége nem felel meg a védendő titkok osztályozásának.*
+ *A kulcs menedzsment nem biztonságos*

3 *A kulcs vagy rejtjelezetlen, olvasható szöveg formátumú, amely védetlen és hozzáférhető, vagy rejtjelezett, és megfejthető.*

- *A kulcs vagy a kulcshoz kötődő adatok teljes, vagy részleges törlése.*
- *Egy érvényes kulcs közvetlen, szándékos vagy közvetett, véletlen eltávolítása.*
- *Jogosult felhasználó vagy entitás megszemélyesítése.*
- *A kulcsmenedzsment feladatok késleltetése:*
- *Visszaélés a kulcsokkal*
  - *A kulcsok jogosulatlan célú használata*
  - *Adatok jogosulatlan rejtjelezése vagy megfejtése.*
  - *A kulcs használata annak lejárata után.*
  - *A kulcs használata a megengedettől eltérő módon.*
  - *A kulcsok jogosulatlan fogadónak való kiszolgáltatása.*

Az MSZ ISO/IEC 117700-1 elő szabvány alapján.

8.6.4. Logikai rendelkezésre állás

8.6.4.1. Vírusvédelem nem biztosítja a rendelkezésre állást

+ *A vírusvédelem nem terjed ki a teljes rendszerre, nem aktív.*
+ *A vírusvédelmi szoftver frissítése nem rendszeres.*
+ *A vírusfertőzéseket nem naplózzák, a naplót nem értékelik, az értékelést nem követi védelmi intézkedés.*
+ *Globális vírusfertőzés esetére nem rendelkeznek védelmi intézkedési tervvel.*
+ *A vírusvédelem mellet, egyéb rosszindulatú sw-ek ellen nincs védekezés (mint pl. féreg, spam, spyware, szolgáltatás bénító támadás, trójai faló), vagy nem aktív.*
+ *A rosszindulatú sw-ek elleni védekezés nem többszintű, nincs védelem az IR határán.*

8.6.4.2. Mentés, újraindítás, erőforrás felhasználás nem biztosítja a rendelkezésre állást

+ *Nincs meghatározva a felhasználók folyamatos működés megszakadási tűrőképessége (sebezhetőségi ablak).*
+ *A mentés, újraindítás rendszere nem biztosítja az erőforrások folyamatos rendelkezésre állását.*
+ *A mentéseket tartalmazó adathordózók egy példányát nem tárolják az épületen kívül.*
+ *Nem rendelkeznek a szoftver(-ek) eredeti (sértetlen) szállítói példányával.*
+ *Az információ-rendszer folyamatos, és rendeltetésszerű működésének megszakadása esetére a visszaállítás feltételei nem biztosítottak.*

+ *A felhasználói profilokban (pl. adatbázis kezelő rendszerben) az erőforrás felhasználás nincs korlátozva azért, hogy az* erőforrások kisajátításával *ne akadályozhassák meg más felhasználók hozzáférését.*

8.6.4.3. Logikai rombolás elleni védelem nem teljes körű

+ *Az informatikai erőforrások nem védettek vagy nem megfelelő frekvenciasávban védettek (EMC) a logikai rombolás ellen.*

8.6.4.4. Dokumentáció nem naprakész, teljes körű

+ *A rendszer, és az alkalmazói szoftverek dokumentációja nem naprakész.*

8.6.4.5. Rendszerkövetés nem megfelelősen szervezett

+ *Nincs biztosítva a rendszerkövetés.*
+ *Nem áll rendelkezésre az alkalmazói programok forrásnyelvi változata.*

8.6.5. Hálózatok

8.6.5.1. LAN nem biztosítja megfelelően a biztonsági követelményeket

8.6.5.1.1. Jogosulatlan LAN hozzáférés

+ *az azonosítás és hitelesítés nem kielégítő, vagy hiányzik*
+ *jelszó többek által ismert (megosztás)*
+ *szegényes jelszó menedzsment, és egyszerű jelszó készítés*
+ *ismert rendszer hiányosságok használata,*
+ *egyszerű felhasználói PC-k, amelyek jelszóval nem védettek bootolásnál*
+ *A PC-k záró mechanizmusainak nem megfelelő alkalmazása*
+ *LAN hozzáférés i jelszavak batch fileba tárolva a PC-ken,*
+ *a LAN hálózati eszközök szegényes fizikai védelme,*
+ *nem védett modemek,*
+ *a time-out hiánya log in-nél és log off kísérletnél,*
+ *szétkapcsolás hiánya többszörös bejelentkezésnél és kijelentkezési kísérletnél*
+ *az "utolsó sikeres log in datum, időpont, és sikertelen bejelentkezési kísérletek naplózásának hiánya,*
+ *a felhasználó real time azonosítás hiánya (yédekezés a megszemélyesítés ellen)*

8.6.5.1.2. Helytelen LAN erőforrás hozzáférés (jogosulatlan, jogosult)

+ *rendszerhiba engedélyezés beállítás, amely túl engedékeny a felhasználók számára,*
+ *az adminisztrátor, és a LAN menedzser jogosultságainak helytelen használata,*
+ *tárolt adat nem megfelelő szintű védelemmel vagy a nélkül,*
+ *a felhasználói jogosultságok hiánya, vagy nem megfelelő használata,*

- *PC-k, amelyek file szintű hozzáférés védelmet nem használnak,*

8.6.5.1.3. Adatok felfedése

- *helytelen hozzáférés -védelem beállítás,*
- *biztonság érzékeny adatok nyílt szövegként való tárolása,*
- *alkalmazói forráskód nyílt szövegként való tárolása,*
- *látható monitorok nagy forgalmú helyeken,*
- *nyomtatók nagy forgalmú helyeken,*
- *adat, és software back up másolatok tárolása nyílt helyeken.*

8.6.5.1.4. Adatok, szoftverek módosítása jogosulatlanul

- *írás jogosultság megadása felhasználónak, aki csak olvasási jogosultsággal rendelkezik,*
- *nem szabályszerű, engedély nélküli módosítása szoftvernek,*
- *biztonság érzékeny adatok nyílt tárolása,*
- *jogosultsági mechanizmus, amely szükségtelen írás engedélyt ad,*
- *vírus védelem, és jelzés hiánya.*

8.6.5.1.5. LAN forgalom felfedése

- *nem megfelelő fizikai védelme a LAN eszközöknek, és hordozóknak,*
- *nyílt szövegek átvitele rádiós protokollal,*
- *nyílt szöveg átvitele LAN-on.*

8.6.5.1.6. LAN forgalom becsapása (spoofing)

- *LAN forgalom nyílt szöveggel,*
- *időbélyegzés hiánya (adás/vétel),*
- *digitális aláírás hiánya,*
- *real-time ellenőrzési mechanizmus hiánya (playback ellen).*

8.6.5.1.7. LAN Funkciók megszakítása

- *szokatlan forgalom felismerés hiánya (szándékos forgalomellehetetlenítés),*
- *hardware hiba esetén a forgalom más útvonalra irányítása,*
- *jogosulatlan rekonfigurálás (cím a munkaállomáson, router vagy hub konfiguráció)*
- *nem megfelelő karbantartás,*
- *nem megfelelő fizikai biztonság.*

8.6.5.1.8. WLAN védelem hiányosságai

- *Nyílt szöveg forgalmazása, lehallgathatóság*
- *Gyenge beléptetés korlátozás*
- *Gyenge szolgáltatásakadályozás védelem*
- *Gyenge sértetlenség védelem*
- *A környezeti interferenciás zavarok elleni védelem hiánya*

8.6.5.2. WAN nem biztosítja megfelelően a biztonsági követelményeket

+ *A bizalmasság, sértetlenség, és a rendelkezésre állás védelmére nincsenek vagy nem teljes körűek a védelmi intézkedések.*

8.6.5.3. Nem bizalmas hálózati kapcsolatok nem megfelelően védettek

+ *A külső távközlési kapcsolatoknál nem megoldott vagy gyenge a hozzáférés védelem (különösen Internet, on line diagnosztika, és dial in kapcsolatok)*
+ *Nincs tartalomhitelesítés*
+ *.A bizalmas, és nem bizalmas hálózat határán nincs hfv,nincs rosszindulatú sw-ek elelni védelem, az IR határa nem egyértelműen meghatározott..*

8.6.5.4. Beszéd hálózat nem megfelelően védett

+ *A biztonságkritikus kapcsolatok nem bizalmasság védettek.*

8.6.6. Az IR életciklus

8.6.6.1. Fejlesztés során nem érvényesülnek a biztonsági követelmények

8.6.6.1.1. Fejlesztési környezet

+ *A fejlesztési környezet fizikailag, és logikailag az üzemeltetéstől nem leválasztott.*
+ *A fejlesztési környezet fizikai, logikai védelme nem megoldott.*

8.6.6.1.2. Biztonsági követelmények a fejlesztendő rendszerben

+ *A fejlesztési cél meghatározásakor nem határozzák meg a biztonsági követelményeket.*

8.6.6.2. A harmadik félnél fejlesztett rendszereknek nincs biztosítva a szállítás alatti biztonsága

8.6.6.3. Átadás/átvétel során nem érvényesülnek a biztonsági követelmények megfelelően

8.6.6.3.1. Megfelelősség ellenőrzése

+ *A megfelelősséget nem ellenőrzik kellő gondossággal, mivel a fejlesztés az átvétellel nem fejeződik be.*

8.6.6.3.2. A védelmi intézkedések végrehajtásának ellenőrzése

+ *Az átadás/átvételkor nem ellenőrzik a biztonsági követelmények teljesítését.*
+ *A külső szállító nem köteles nyilatkozni, hogy az átadandó rendszer (eszköz) nem tartalmaz veszélyforrásokat.*

+ *A fejlesztők hozzáférés i jogosultságait az átvétel után nem vonják vissza.*

8.6.6.4. Üzemeltetés során nem érvényesülnek megfelelően a biztonsági követelmények

+ *Nem szabályozott a programcsere menedzsment*
+ *Nincs szabályozott program változat követés, nyilvántartás*
+ *A biztonsági rendszer belső, és külső rendszeres független auditálása nem megoldott.*
+ *Az információ-rendszer rendszeres auditálása nem megoldott.*
+ *A biztonsági események kezelésének rendje nem szabályozott.*
+ *A fizikai, illetve logikai hozzáférés -védelem naplóit nem értékelik, az eseményeket nem jelentik, illetve nem követi védelmi intézkedés (a biztonság ellenőrzés hiánya).*

8.6.6.5. Selejtezés nem biztosítja a biztonságkritikus anyagok bizalmas megsemmisítését

+ *A számítástechnikai eszközök, adathordozók selejtezése (törlés, megsemmisítés) nem szabályozott.*

8.6.6.6. A biztonsági technológia védelmének hiánya, vagy meg nem felelőssége.

+ *A védelmi eszközök realizálását szolgáló intézkedések, eszközök védelmének hiányosságai..*

8.7. ÁTFOGÓ VESZÉLYFORRÁSOK

Ez a pont a könnyebb kezelhetőség érdekében megismétlésre kerül a folyamatos működés tervezésénél (a II. kötetben). A folyamatos működés és elérhetőség biztosítását fenyegető veszélyforrások:

8.7.1. Szervezési

8.7.1.1. Szervezet és működés nem biztosítja a biztonsági követelményeket

+ *Az egységes, központilag irányított biztonsági szervezet hiánya.*

8.7.1.2. Humánvédelem nem biztosítja a folyamatos működés humán feltételeit

+ *A biztonsági tudatosság hiánya.*
+ *A tömegdemonstráció következményei elleni védelem gyengeségei.*
+ *A sztrájkra történő felkészülés hiánya.*
+ *A bombariadó megelőzése, és következményei elleni védelem hiánya.*

8.7.1.3. Szerződések nem érvényesítik megfelelően a biztonsági követelményeket

+ *Az üzleti tevékenység megszakadása elleni biztosítás hiánya.*
+ *Szállítói rendelkezésre állási szerződés(-ek) hiánya.*

8.7.2. Fizikai

8.7.2.1. Fizikai hozzáférés -védelem nem véd megfelelően

+ *A fizikai vandalizmus elleni védekezés gyengeségei.*

8.7.2.2. Fizikai rendelkezésre állás nem biztosítja a növelt rendelkezésre állást

+ *A háttér központ hiánya.*
+ *Távközlési redundancia hiánya (adat, és beszéd távközlés).*
+ *Áramellátó rendszer komplett leállása elleni védelem hiánya.*
+ *Klíma rendszer komplett leállása elleni védelem hiánya.*
+ *Tűz védelem gyengeségei.*
+ *Természeti katasztrófa elleni védelem gyengeségei (villámvédelem).*
+ *Vízbetörés (árvíz, illetve a vízvezetékrendszer megsérülése következtében keletkező csőrepedés) elleni védelem hiánya.*

8.7.3. Logikai

8.7.3.1. Logikai hozzáférés –védelem nem megfelelő színvonalú

+ *A számítógépes vandalizmus elleni védelem hiánya vagy gyengesége.*

8.7.3.2. Logikai rendelkezésre állás nem biztosítja a megfelelő növelt rendelkezésre állást

+ *Rendszerszoftver rendelkezésre állásának gyengeségei.*
+ *Alkalmazói szoftvereknek a rendelkezésre állása gyengeségei.*
+ *Vírusfertőzés.*
+ *Elektromágneses rombolás.*

8.7.4. A számon kérhetőség nem megfelelően biztosított

9. VESZÉLYFORRÁS ELEMZÉS FELÉPÍTÉSE

9.1. A VÁLLALATI SZINTŰ VESZÉLYFORRÁSOK

9.1.1. Külső veszélyforrások

9.1.2. belső veszélyforrások

9.2. SZERVEZÉSI VESZÉLYFORRÁSOK

9.2.1. Szabályzatok

9.2.1.1. Szervezet és működés szabályozása

9.2.1.1.1. Szervezet

9.2.1.1.2. Biztonsági infrastruktúra

9.2.1.1.3. A biztonság hatékonyságának mérése

9.2.1.1.4. Tűzvédelmi szervezet

9.2.1.1.5. Polgári védelmi szervezet

9.2.1.2. Biztonsági alapdokumentumok

9.2.1.3. Titokvédelem szabályozása

9.2.1.3.1. Személyes adatok

9.2.1.3.2. Adatok, értékek

9.2.1.3.3. Eszközök

9.2.1.3.4. Eljárások

9.2.1.3.5. Helyiségek

9.2.1.4. Iratkezelés szabályozása

9.2.2. Humánpolitikai intézkedések

9.2.2.1. Munkaviszony létesítés és megszüntetés

9.2.2.2. Feladatok meghatározása és szétválasztása

9.2.2.3. Teljesítménykövetés

9.2.2.4. Karrier menedzsment

9.2.2.5. Oktatás

9.2.2.6. Megtévesztés elleni (social engineering) elleni védekezés

9.2.3. Szerződések

9.2.3.1. Szerződés harmadikféllel

9.2.3.2. Kockázat áthárítás

9.2.4. A biztonsági események kezelésének szabályozása

9.3. TECHNIKAI VESZÉLYFORRÁSOK

9.3.1. Az üzleti rendszer veszélyforrásai (amelyek nem szerepelnek az alábbiakban).

9.3.2. Fizikai hfv

9.3.2.1. Aktív támadás elleni hozzáférés -védelem

9.3.2.1.1. Épületautomatika (ÜR, és IR)

9.3.2.1.2. Belépés és mozgás ellenőrzés

9.3.2.1.3. Behatolás-védelem

9.3.2.1.4. Értéktárolás

9.3.2.1.5. Értékszállítás

9.3.2.1.6. Üres íróasztal politika

9.3.2.2. Passzív támadás elleni hozzáférés -védelem

9.3.2.2.1. Elektromágneses kisugárzás

9.3.2.2.2. Akusztikus kisugárzás

9.3.2.2.3. Hulladékmegsemmisítés (selejtezés)

9.3.3. Fizikai rendelkezésre állás

9.3.3.1. Energiaellátás

9.3.3.2. Tűz

9.3.3.3. Beszéd kommunikáció

9.3.3.4. Klimatizálás

9.3.3.5. Megbízhatóság

9.3.3.6. Dokumentáció

9.3.3.7. Karbantartást ellátók

9.3.4. Logikai hfv

9.3.4.1. Aktív támadás elleni hozzáférés -védelem

9.3.4.1.1. Jelszó és jogosultság

9.3.4.1.2. Hitelességvédelem

9.3.4.1.3. Time out

9.3.4.1.4. Logikai behatolás jelzés

9.3.4.2. Passzív támadás elleni hozzáférés -védelem

9.3.5. Logikai rendelkezésre állás

9.3.5.1. Vírus, rossz indulatú sw-ek elleni védelem

9.3.5.2. Mentés, újraindítás

9.3.5.3. Logikai rombolás

9.3.5.4. Dokumentáció

9.3.5.5. Rendszerkövetés

9.3.6. Hálózatok

9.3.6.1. LAN

9.3.6.2. WAN

9.3.6.3. Nem bizalmas hálózati kapcsolatok

9.3.6.4. Beszéd hálózat

9.3.7. Az IR életciklus

9.3.7.1. Fejlesztés

9.3.7.1.1. Fejlesztési környezet

9.3.7.1.2. Biztonsági követelmények a fejlesztendő rendszerben

9.3.7.2. A harmadik félnél fejlesztett rendszer szállítás alatti biztonsága

9.3.7.3. Átadás/átvétel

9.3.7.3.1. Megfelelősség ellenőrzése

9.3.7.3.2. A védelmi intézkedések végrehajtásának ellenőrzése

9.3.7.4. Üzemeltetés

9.3.7.5. Selejtezés

9.4. VESZÉLYFORRÁSOK A SZÁMON KÉRHETŐSÉG BIZTOSÍTÁSA TERÜLETÉN

9.4.1. Elrettentés

9.4.2. A szerepek, és felelősségek nem megfelelő biztosítása

9.4.3. Az adatok számon kérhetőségének biztosítása (audit trail)

9.4.4. Tevékenységek számon kérhetősége (audit log, behatolási log, fizikai beléptetési napló)

9.4.5. Információk leltára

9.4.6. Informatikai eszközök leltára

9.4.7. Az üzleti tevékenységhez szükséges eszközök leltára

9.5. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

9.6. AZ IR MM ÉRETTSÉGI SZINTJE

A veszélyforrás elemzés és a II. kötet 10.3 pont alapján meg kell adni az érettségi szintet, amely a biztonsági rendszer <u>általános értékeléseként</u> fog szerepelni, megfelelő lezárásaként a kockázat menedzsmentnek. A kockázat értékelést követően kidolgozott ellenálló képességi értékek ezzel szemben majd a konkrét gyengeségekre mutatnak rá.

10. A KOCKÁZAT ÉRTÉKELÉS KÉSZÍTÉSE

10.1. A KOCKÁZAT ÉRTÉKELÉS

10.2. KOCKÁZAT ÉRTÉKELÉS KOCKÁZATI MÁTRIX FELHASZNÁLÁSÁVAL

A kockázat az erőforrások bizalmassága és/vagy sértetlensége és/vagy rendelkezésre állása sérülésének valószínűsége.

Chikán Attila szerint „a kockázat egy cselekvési változat (alternatíva) lehetséges negatívan értékelt következményeinek teljes leírása, beleértve a következmények súlyának, és bekövetkezési valószínűségének megmutatását is." Továbbá a kockázat bizonytalanság (információ hiány) következménye, ha a döntés valamennyi következményét ismernénk, nem lenne kockázat.

Az üzleti, és informatikai folyamatok kockázatai a gazdasági szervezet működési kockázatai közé tartoznak. A működési kockázat meghatározása:

A működési kockázat annak a veszteségnek a kockázata, amely a nem megfelelő vagy kiesett belső folyamatok, emberek, és rendszerek vagy külső események miatt következik be [58].

A kockázat értékelés célja, hogy veszélyforrásonként meghatározzuk a veszélyforrás realizálódása, milyen következményekkel járhat, és ennek alapján eldöntsük a szükséges védelmi intézkedést, azaz a kockázat kezelését.
A kockázatok elemzésénél figyelembe kell venni azok egymásra hatását, és a kockázat értékelési jelentésnek az audit trailek, és a belső ellenőrzés méréseit is fel kell használnia.
A kockázatot meghatározó tényezők a fenyegetettség, a bekövetkezési valószínűség, és a sebezhetőség. Ezek a következők:

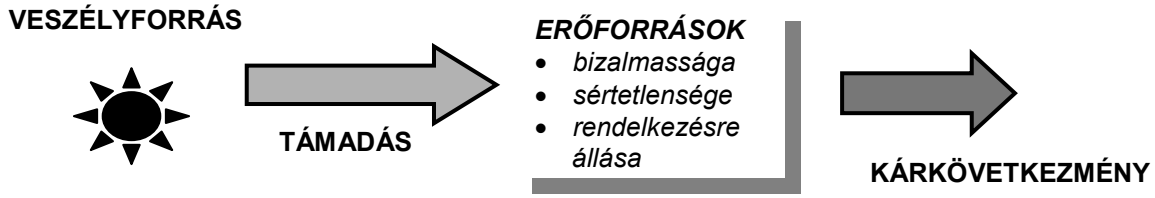
⇒ *A fenyegetettség (T).*

- A fenyegetés a támadás lehetősége a támadás tárgyát képező erőforrásra.
- A fenyegetettség olyan állapot, amelyben az erőforrások felfedésre (bizalmasság), módosításra (sértetlenség) vagy elpusztításra kerülhetnek (rendelkezésre állás).
- A támadás egy veszélyforrásból kiinduló, az erőforrások bizalmassága és/vagy sértetlensége és/vagy rendelkezésre állása ellen irányuló folyamat.

A támadás eredménye, amennyiben az sikeres, az erőforrások biztonságának sérülése, amely a kárkövetkezmény. A támadás módszere lehet aktív vagy passzív.

Az *aktív támadási módszer* behatol a rendszerbe, és ott fejti ki tevékenységét. A *passzív támadási módszer* a rendszer környezetre gyakorolt akusztikus, illetve elektromágneses hatását használja ki, nem hatol be a rendszerbe, és gyakorlatilag észrevétlenül valósul meg.

A fenyegetést az alábbi ábrán értelmezzük:



A fenyegetés összetevői a következők:

- ⇒ a *veszélyforrás*, amely lehet szervezési, fizikai (természeti), logikai,
- ⇒ a *támadás célja*, amely irányulhat az erőforrás(-ok) bizalmassága és/vagy a sértetlensége és/vagy rendelkezésre állása ellen,
- ⇒ a *támadási potenciál*, amely a támadó motivációja a támadásra,
- ⇒ a *kárkövetkezmény*, amely az erőforrások sebezhetősége.

A sikeres támadás eredményeként fellépő kárkövetkezmény, pedig érinthet egy erőforrást vagy az egész rendszert. A fentiek alapján kell megállapítani, hogy a fenyegetettség a bizalmasságra (C) és/vagy a sértetlenségre (I) és/vagy a rendelkezésre állásra (A) vonatkozik-e.

⇒ *A bekövetkezési valószínűség (P).*

Bekövetkezési valószínűségen azt értjük mekkora az esélye annak, hogy a veszélyforrás képezte fenyegetettség támadás formájában realizálódjon, azaz bekövetkezzen. A bekövetkezési valószínűség lehet:

- *igen kicsi* ***(VS),***
- *kicsi* ***(S),***
- *közepes* ***(M)*** *vagy*
- *nagy* ***(L),***
- *igen nagy* ***(XL)***

A [63]-ban a bekövetkezési valószínűség mértékei:

SZINT	LEÍRÁS	RÉSZLETES LEÍRÁS (PÉLDA)
VS	Kivételes	Kivételes körülmények esetén
S	Nem valószínű	Egyes időpontokban bekövetkezhet
M	Lehetséges	Egyes időpontokban lehetséges, hogy bekövetkezik
L	Valószínű	A legtöbb körülmény között valószínű, hogy bekövetkezik
XL	Szinte biztos	Legtöbb körülmény között várható a bekövetkezés

A technikai *bekövetkezési valószínűséget* a támadási potenciálból (amely valójában a támadó motivációjáról szól) kiindulva, a CEM (Common Evaluatin Methodology) [37]) szerint, egzakt módszerekkel meghatározni igen nehéz. Továbbá a bekövetkezett támadásokról nem áll rendelkezésre statisztika (egyrészt nem vezetnek statisztikát, másrészt nem hozzák azt nyilvánosságra), így idősor hiányában a valószínűség számítási módszer sem alkalmazható. Ebből következik, hogy a bekövetkezési valószínűséget kénytelenek vagyunk becsülni.

A *támadási potenciálból* a sikeres **technikai** támadás bekövetkezési valószínűsége könnyebben megbecsülhető. A támadási potenciál a CEM szerint a következő tényezőktől függ:

- $\Rightarrow$ a támadó motivációjától (a védelem erőssége, a támadási cél értéke)
- $\Rightarrow$ a sikeres támadáshoz szükséges szakértelemtől,
- $\Rightarrow$ a sikeres támadáshoz szükséges erőforrásoktól (eszköz, idő).

A támadási cél *védelmének erőssége* a támadás esélyeit meghatározza.
A támadás cél ér*téke* azt fejezi ki, hogy érdemes-e a támadást végrehajtani.

A támadó *szakértelme* lehet:

- *laikus (amatőr),*
- *profi* (aki ismeri a rendszer tulajdonságait, programozási tudással rendelkezik, és összetett technikákat alkalmaz),
- *szakértő* (aki részleteiben felderíti, ismeri a támadási célt képező rendszerben alkalmazott védelmi intézkedéseket, és fejlett tudással, eszközökkel rendelkezik a támadáshoz).

A támadás *erőforrásai: a támadás eszköze, és az idő*.
Az eszköz lehet *nem támogatott* (azaz nem szükséges eszköz a támadáshoz), *házi* (azaz a támadás célját képező rendszer egy erőforrása), és *speciális eszköz* (amely nem kapható civil forgalomban). A sikeres támadáshoz folyamatosan felhasználható *időtartam* lehet: kevesebb, mint egy *óra*, kevesebb, mint egy *nap*, legalább egy *hónap*.
A támadási potenciál összetevőit sem lehet egzakt módszerrel meghatározni. A CEM például az értékről azt mondja, hogy az szubjektív valami, amely nagy mértékben függ attól, hogy az adott esetben, milyen értéket képvisel. Hasonlóképen igaz ez a támadási potenciált meghatározó további tényezőkre is.
A támadási potenciál **a technikai veszélyforrások** bekövetkezési valószínűségének meghatározásához segédeszköz.

A támadási potenciál, és összetevőinek becsült értékei:

T_p ÖSSZETEVŐ	*1.szint*	*2.szint*	*3.szint*
ÉRTÉK	*Kicsi*	*Közepes*	*Nagy*
VÉDELEM ERŐSSÉGE	*C1 (EAL2)*	*C2 (EAL3)*	*B1 (EAL4)*
SZAKÉRTELEM	*Laikus*	*Profi*	*Szakértő*
ESZKÖZ	*Nem támogatott*	*Házi*	*Speciális*
IDŐTARTAM	*Napok*	*<1óra*	*<1perc*

A támadási potenciál annál kisebb mennél

- ⇒ kisebb a támadási cél értéke (motiváció),
- ⇒ *kisebb* a védelem erőssége (motiváció),
- ⇒ *kisebb* a támadáshoz szükséges szakértelem,
- ⇒ egyszerűbb a sikeres támadáshoz szükséges eszköz (erőforrás),
- ⇒ *nagyobb* a sikeres támadás végrehajtásához rendelkezésre álló idő (erőforrás).

Azaz az 1.-es szint esetében kis támadási potenciál is elég a sikeres támadáshoz, amely a támadót a végrehajtásra motiválja.

A becsléssel történő elemzés alapján a támadási potenciál (T_p):

- *igen kicsi* ***(VS),*** ***ha az összetevő*** *mind 1-es szint,*
- *kicsi* ***(S),*** ***ha az összetevők többségében1****.-esek,de lehet 2és/vagy 3.-as is,*
- *közepes* ***(M),*** ***ha az összetevők*** *mind 2.-es szint,*
- *nagy* ***(L),*** ***ha az összetevők*** *többségében 2-esek, de 3-as szint is lehet,*
- *gyakorlat feletti* ***(XL). ha az összetevők*** *mind 3.-as szint.*

A bekövetkezési valószínűség (P) pedig annál nagyobb, mennél kisseb **a sikeres** támadáshoz szükséges támadási potenciál (T_p). Az összefüggés az alábbi táblán található:

P	T_p
XL	VS
L	S
M	M
S	L
VS	XL

⇒ *A sebezhetőség (V, kárkövetkezmény, üzleti hatás).*

A sebezhetőség sikeres támadás esetén az erőforrások lehetséges sérülése. A támadás bekövetkezésekor a teljes rendszer vagy egy eleme sérülhet (a lehetséges kárkövetkezmény). Így a sebezhetőség lehet

- *globális* ***(G)*** *azaz az összes erőforrás folyamatos működése szakad meg, amely lehet kicsi (S), közepes (M), és nagy (L) , vagy*
- *részleges* ***(R),*** *amely lehet kicsi (S), közepes (M), és nagy (L), azaz egyes erőforrások sérülnek.*

⇒ *A kockázat (K).*

*A kockázatot (**K**) ezek után az alábbi táblázat (általános) segítségével, a bekövetkezési valószínűség (P) és a sebezhetőség (V) becsült értékeinek egybevetésével kaphatjuk meg. A K kockázati értékek a táblázatban a szürke mezőkben vannak feltüntetve.*

P \ V	R			G		
	S	***M***	***L***	***S***	***M***	***L***
VS	***VS***	***S***	***S***	***S***	***S***	***M***
S	***VS***	***S***	***M***	***S***	***M***	***L***
M	***S***	***M***	***L***	***M***	***L***	***L***
L	***M***	***L***	***L***	***L***	***L***	***XL***
XL	***L***	***L***	***L***	***L***	***XL***	***XL***

Például
K egyes értékeinél,
ha V=R L erős, M közepes, S gyenge, VS nem szükséges védelmi intézkedés,
ha V=G XL igen erős, L erős, M közepes, S nem szükséges védelmi intézkedés.
A védelmi intézkedések pontos meghatározása a Biztonsági Politikában, vagy a Katasztrófatervben történik.
A kockázat tehát egy kárkövetkezmény bekövetkezési valószínűségét fejezi ki.

A **kárkövetkezmény** lehet vagyoni, és nem vagyoni kár. A vagyoni kár a vállalat adatai alapján becsülhető, a nem vagyoni kár (pl. piacvesztés, kártérítési igények, image romlása, tőzsde árfolyamesés) nem becsülhető. Ezért a megoldás, hogy ilyen igény esetén kockázatonként külön adunk választ a vagyoni, és a nem vagyoni kárra. A vagyoni kár osztályozása természetesen függ a vállalat állóeszközeinek összértékétől. Tehát például egy nagyvállalatnál a vagyoni kár lehet:

RS	0-5MFt	GS	0-10MFt
RM	5-50MFt	GM	10-100MFt
RL	>50MFt	GL	>100MFt

⇒ A nem vagyoni kár nem függ össze a vagyoni kár nagyságával, mert lehet egy kis vagyoni kár mellett igen jelentős nem vagyoni kár. Ezért a nem vagyoni kárt külön adjuk meg, amely lehet kismértékű (RS, vagy GS), jelentős (RM, vagy GM), és igen jelentős (RL, vagy GL). A kárkövetkezmény megállapításánál mindig a nagyobbat kell figyelembe venni, tehát, ha a vagyoni kár például GS, a nem vagyoni kár GM, akkor a kárkövetkezmény GM.

A kárkövetkezmény, a kockázat bekövetkezése hatásának mértékei, a [63] szerint értelmezve, amelyhez szervezetenként kell az értékeket hozzárendelni:

SZINT	*LEÍRÁS*	*RÉSZLETES LEÍRÁS*
VS	*Nem jelentős*	*Alacsony pénzügyi veszteség*
S	*Kicsi*	*Közepes pénzügyi veszteség*
M	*Közepes*	*Magas pénzügyi veszteség*
L	*Nagy*	*Nagyobb pénzügyi veszteség*
XL	*Katasztrofális*	*Katasztrofális pénzügyi veszteség.*

⇒ *A kockázat értékelés végrehajtása*
A kockázatelemzést az előbbi pont szerint veszélyforrásonként kell elvégezni, célszerűen annak a szakértőnek, aki a veszélyforrást megállapította.

<u>Egy veszélyforrás kockázat értékelése következőket tartalmazza:</u>
⇒ *Veszélyforrás kódja és neve:*

⇒ *Fenyegetettség:* *minősítés (C, I , A)*
⇒ *A minősítés indoklása:*
⇒ *A bekövetkezési valószínűség:* *minősítés (VS,S,M,L, XL)*
⇒ *A minősítés indoklása:* *rövid indoklás védelmi intézkedés megadása nélkül*
⇒ *A kárkövetkezmény (sebezhetőség)* *minősítés (RS,RM,RL, vagy GS,GM,GL)*
⇒ *A minősítés indoklása:* *rövid indoklás védelmi intézkedés megadása nélkül*
⇒ *A kockázat:* *minősítés (VS,S,M,L,XL)*
⇒ *A kockázat kezelése: :* *javasolt védelmi intézkedés, A válasz lehet: igen erős, erős, közepes, gyenge, nem javasolt*

A technikai bekövetkezési valószínűségek minősítéseinek indoklásánál célszerű a sikeres támadáshoz szükséges támadási potenciálról megállapítottakat felhasználni.

A kockázati szintek értelmezése

KOCKÁZATI SZINT	A KCKÁZAT LEÍRÁSA	A KOCKÁZAT ÉRTELMEZÉSE, HATÁSA
XL	Csökkentendő, biztosítás kötése	Üzletmenet súlyos megszakadása
L	Csökkentendő	Üzletmenet megszakadása
M	Mérséklendő	Üzletmenet zavara
S	Elfogadható	Rendszertechnikailag áthidalható
VS	Elviselhető	Nem jelentős

A kockázat értékelés eredményét egy táblázatban lehet összefoglalni (konkrét kockázati mátrix) (lásd a következő pontban).

⇒ *Kockázati mátrix*

A kockázati mátrixot az eddig megállapított becsült értékekből állítjuk össze, mint veszélyforrás fenyegetés, bekövetkezési valószínűség, kockázat, és ezekből megállapítjuk a javasolt védelmi intézkedést, valamint az annak megvalósítása után fenn álló maradék kockázatot.

Veszély-forrás neve	Mit fenyeget	Bekövet-kezési valószínűség	Kár-következ-mény	Kockázat	Javasolt Védelmi Intézk.	Maradék kockázat

A kockázati mátrix segítségével a Megrendelő eldöntheti (javaslatunkra), hogy miként kívánja a kockázatokat kezelni, azaz milyen erősségű védelmi intézkedést kíván tenni.
A kockázati mátrix, tehát a bekövetkezési valószínűség, és az üzleti hatás függvényében meghatározott kockázatokat ábrázolja, egyben osztályozza nagyságuk szerint. Ezzel lehetőséget teremt a kockázatok kezelésének eldöntése, a védelmi intézkedés szükségességének, és erősségének eldöntésére.

MEGJEGYZÉS!

⇒ A Biztonsági Politika **a részleges, és az *átfogó szervezési, és részleges és átfogó*** veszélyforrások bekövetkezési valószínűségének minimálisra csökkentése érdekében teendő védelmi intézkedésekkel foglalkozik, az ***átfogó technikai*** veszélyforrásokkal a Katasztrófaterv foglalkozik.
*Ugyanis azoknál **a részleges veszélyforrásoknál**, amelyeknek a bekövetkezése esetén az erőforrások bizalmassága, illetve az adatok, és a humán erőforrások sértetlensége átfogóan sérül, **a folyamatos működés nem szakad meg**.*
A veszélyforrások, és a sebezhetőség (kárkövetkezmény) összefüggései a következők:

VESZÉLYFORRÁS	***SEBEZHETŐSÉG***

RÉSZLEGES veszélyforrás az,

amely bekövetkezése esetén sérül

- *az erőforrások bizalmassága*
  - ✓ *egy vagy* — *R*
  - ✓ *minden erőforrás elemnél* — *G*
- *a z adatok, és humán erőforrások sértetlensége*
  - ✓ *egy vagy* — *R*
  - ✓ *minden erőforrás elemnél* — *G*
- *a technológia, illetve az alkalmazások sértetlensége*
  - ✓ *egy erőforrás elemnél* — *R*
- *a rendelkezésére állás*
  - ✓ *egy erőforrás elemnél* — *R*

ÁTFOGÓ veszélyforrás az, amely
bekövetkezése esetén a rendszer folyamatos működése megszakad, azaz a rendszer

- *sértetlensége és/vagy rendelkezésére állása sérül*
  - ✓ *minden technikai elemnél* — *G*

(technológia, alkalmazások, támogatások, létesítmények)

10.3. A BIZTONSÁGI BERUHÁZÁS MEGTÉRÜLÉSE

A védelmi intézkedésekkel kapcsolatos döntés, azaz megtesszük-e, milyen erős védelmi intézkedést teszünk, vagy nem teszünk védelmi intézkedést ahhoz célszerű felhasználni a költség/haszonelemzést, a megtérülés vizsgálatát. A most készülő

ISACA szabvány tervezete szerint a biztonsági beruházásnak a megtérülése (Return on Security Investment, ROSI) a következő képlet szerint (egy évre) számítható:

$$ROSI = \frac{\textbf{(kockázat x a csökkentés \%-a)- a biztonsági beruházás költsége}}{\textbf{biztonsági beruházás költsége}}$$

A képlet azonban csak becslésen alapuló elemet is tartalmaz, mint a kockázat, ahol a nem vagyoni, nem tárgyiasult kár kockázatát csak becsülni lehet. Továbbá a NIST SP 800-30 USA szabvány, ajánlás szerint egy biztonsági megtérülés elemzésnél azt is figyelembe kell venni, hogy mit eredményezhet az, ha a védelmi intézkedést nem tesszük meg. Így a számítás szükséges, orientáló adatot eredményez.

10.4. A BIZTONSÁGI RENDSZER MINŐSÍTÉSE

A biztonsági alrendszert a kockázat értékelés alapján minősíteni kell. A minősítés azt a célt szolgálja, hogy a menedzsment a védelmi intézkedések megítéléséhez, pontosabban azok szükségességének eldöntéséhez, a működő biztonságról összefoglaló áttekintést kapjon.

A kockázat értékelés során minden veszélyforrásról megállapítottuk, hogy egy feltételezett támadás esetén, figyelembe véve a támadási módszerek ismert színvonalát, részlegesen, illetve átfogóan sebezheti-e az erőforrásokat (az üzleti, és az információ-rendszer erőforrásait), mérlegeltük a bekövetkezési valószínűséget, és kidolgoztuk a kockázatát.
A veszélyforrások a hozzájuk rendelt kockázati értékek alapján öt kockázati osztályba és azokon belül kockázati csoportokba (lásd 1.sz. táblázatot) sorolhatók. A veszélyforrásokhoz hozzárendelt kockázati értékekből megállapíthatjuk a kockázati csoportok kockázati értékeit (a feltárt veszélyforrások kockázati értékeit a veszélyforrás elemzésből kaphatjuk meg az 1. sz. táblázathoz). Ezután a kockázati osztályok kockázati értékeiből minősítjük a biztonsági rendszer ellenálló képességét. (2.sz. táblázat).

A biztonsági rendszert az ellenálló képesség (E) minősíti, amely azt fejezi ki, hogy az alrendszer milyen szakértelemmel és erőforrásokkal rendelkező lehetséges támadásokat tud visszaverni, azok sikerét megakadályozni.

A csoportok, és az osztályok kockázati értékeit, valamint a biztonsági rendszer ellenálló képességének a minősítését az egyenszilárdság elve alapján kell megállapítani. Ez azt jelenti, hogy a csoportok, és az osztályok minősítése mindig a csoportban, illetve az osztályban előforduló legnagyobb kockázati érték. A biztonsági alrendszer minősítését pedig mindig az öt kockázati osztály kockázati értéke közül a nagyobb kockázati érték alapján állapítjuk meg. Azaz a legnagyobb kockázathoz a leggyengébb minősítés tartozik, *tehát növekvő kockázat esetén csökken az ellenálló képesség, és fordítva.*

- ⇒ ***NEM ELLENÁLLÓ**, ha a rendszerben gyakorlatilag nincsenek védelmi intézkedések.*
- ⇒ ***NYILVÁNVALÓAN ELLENÁLLÓ,** ha a védelmi intézkedések egyszerű szakértelemmel, és erőforrásokkal rendelkező nyilvánvaló, illetve véletlen támadás ellen védenek.*

⇒ ***MÜRSÉKELTEN ELLENÁLLÓ****, ha a védelmi intézkedések, korlátozott alkalmakkal, és szakértelemmel, illetve erőforrásokkal rendelkező, közepes támadás ellen védenek.*

⇒ ***MAGASAN ELLENÁLLÓ,*** *ha a védelmi intézkedések magas, kifinomult szakértelemmel, és erőforrásokkal rendelkező támadás ellen védenek.*

Az alábbi táblázaton bemutatjuk a támadási potenciál (T_p), a bekövetkezési valószínűség (P), a kockázat (K), és az ellenálló képesség összefüggését (E).

↓ T_p	↑ P	↑ K	↓ E
VS	XL	XL	***NYILVÁNVALÓ***
S	L	L	***NYILVÁNVALÓ***
M	M	M	***MÜRSÉKELT***
L	S	S	***MAGAS***
XL	VS	VS	***MAGAS***

A nyilak a növekedés irányát mutatják, azaz ***annál nagyobb (T_p)*** szükséges a sikeres támadáshoz

⇒ ***mennél nagyobb*** a támadás visszaverésének ellenálló képessége ***(E).***

Az eljárás során feltételezzük azt, hogy minden veszélyforrás feltárásra került.
A kockázati értékeket az alábbi táblázatban kell összegyűjteni.

1. sz. táblázat. ***A KOCKÁZATI ÉRTÉKEK***

Kockázati osztály *Kockázati csoport*	*A veszélyforrás jele*	*A veszély-Forrás Kockázata*	*A veszélyforrás mit fenyeget (C=bizalmasság, I=sértetlenség, A=rendelkezésre állás)*	*A kockázati csoport kockázati értéke***	*A kockázati osztály kockázati értéke***
Szervezési	—	—	—	—	*Szervezési*
Szabályzatok	—	—	—		—
				—	—
				—	—
Humánpolitika	—	—	—		—
				—	—
				—	—
Szerződések	—	—	—		—
				—	—
				—	—
Technikai	—	—	—	—	—
Fizikai hozzáférés			—		*fizikai*
				—	—
				—	—
Fizikai rendelkezésre állás	—	—	—		—
				—	—
				—	—
Logikai hozzáférés	—	—	—		*Logikai*
				—	—
				—	—
Logikai rendelkezésre állás	—	—	—		—
				—	—
				—	—
Hálózat	—	—	—		*Hálózati*
				—	—
				—	—
IR életciklus	—	—	—		*Életciklus*
				—	—
				—	—

Az üres sorokban (szükség esetén a sorok számát növelve) kell az adott kockázati csoportba tartozó veszélyforrások adatait megadni.
*** A kockázati csoportok, illetve a kockázati osztályok kockázati értékeit a csoportba, illetve az osztályba tartozó elemek legnagyobb kockázati értékeiből állapítjuk meg .A kockázati osztályok négyzeteibe értelemszerűen az értékek kerülnek beírásra.*

Az öt kockázati osztály értékei alapján a biztonsági rendszer helyzete ábrázolható is.

2.sz. táblázat. ***A biztonsági rendszerellenálló képességének minősítése:***

A szervezési kockázati osztály kockázati értéke:

A technikai kockázati osztályokban:

A fizikai kockázati osztály kockázati értéke:
A logikai kockázati osztály kockázati értéke:
A hálózati kockázati osztály kockázati értéke:
Az életciklus kockázati osztály kockázati értéke:

A biztonsági rendszer ellenálló képességének minősítése*:*
(A kockázati értékek és az ellenálló képesség összefüggését feltüntető táblázat szerint, az öt kockázati *osztályban a legnagyobb kockázati értéket figyelembe véve)*

10.5. A MENEDZSMENT DÖNTÉSE

A veszélyforrásonként megállapított kockázatok csökkentésére teendő védelmi intézkedések megtételéről, vagy a kockázat felvállalásáról, illetve a védelmi intézkedés erősségéréről, a menedzsment joga, és kötelessége a döntés. A döntést a menedzsment a következők figyelembevételével hozza meg:

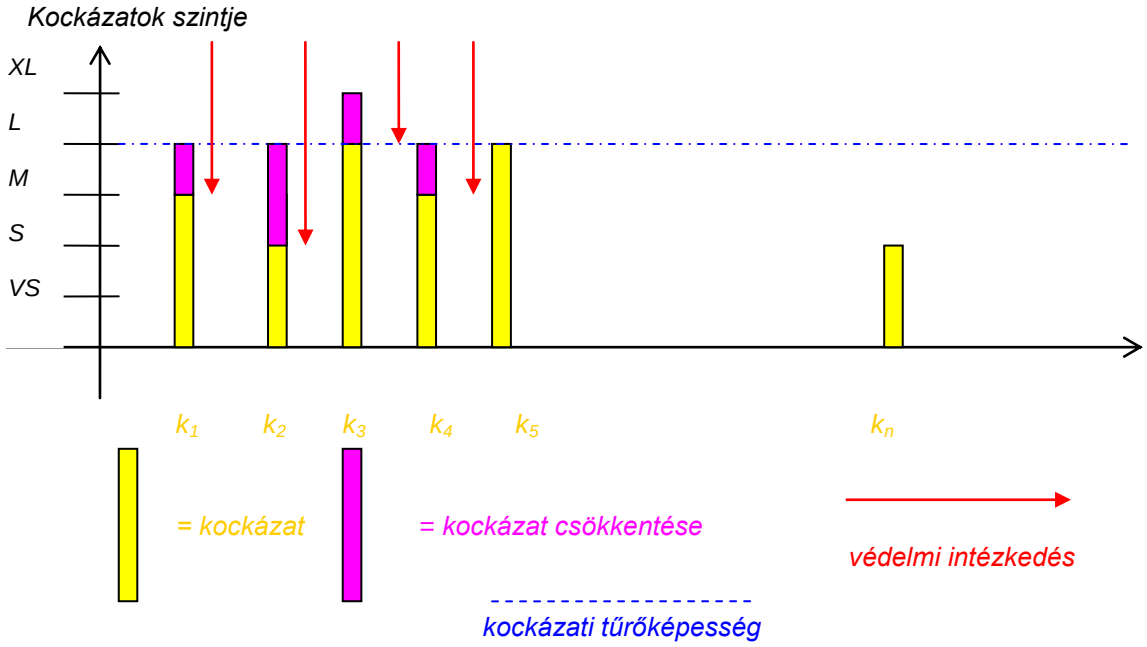
- ⇒ A kockázat szintje,
- ⇒ A szervezet kockázat étvágya és tűrőképessége,
- ⇒ A javasolt védelmi intézkedés ROSI mutatója.
- ⇒ A veszélyforrás képezte fenyegetés céljának biztonság érzékenysége, és az üzleti cél összevetése.

A kockázat menedzsmentnél, a döntésnél tehát figyelembe kell venni, hogy a vállalati stratégia meghatározza a vállalat ***kockázati tűrő képességét*** *(risk tolerance), amely az egyes kockázatok nagyságának a maximumát határozza meg, amelyet a vállalat még elfogad céljai teljesítéséhez. Valójában ez a kockázat csökkentésére tett védelmi intézkedés minimális erősségének meghatározása,* ***az egyenszilárdság elve*** *(lásd még: 10.6). Továbbá figyelembe kell venni* ***a kockázati étvágyat*** *(risk appetite), amely a vállalat vagy más szervezet küldetése, víziója elérésének a szempontjából a kockázatok elfogadható összege. Ezek a fogalmak az ERM-ben (Enterprise Risk Management, Vállalati Szintű Kockázatmenedzsment) jelennek meg először.*

A vállalati szintű kockázat menedzsment egy vállalatirányítási folyamat, a vállalati stratégia kidolgozáshoz, és az átfogóan a szervezetre hatást gyakorló potenciális események azonosítására, és a kockázatok menedzselésére a szervezet kockázati étvágyán belül, a szervezet céljai elérésének ésszerű biztosítására. [62].

A döntés nem végérvényes, azt a rendszeresen ismételt kockázat menedzsmentek, illetve a biztonsági események értékelésekor felül kell vizsgálni. A kockázati tűrőképességet a következő oldalon, lévő ábrán mutatjuk be.

A KOCKÁZATI TŰRŐKÉPESSÉG



A döntés, tehát a kockázat csökkentéséről a [62] szerint lehet:

- **Elkerülés**. A kockázatot jelentő tevékenység megszüntetése.
- **Csökkentés.** Védelmi intézkedés a kockázat csökkentésére.
- **Megosztás.** A kockázat csökkentésének áthárítása illetve egy részének megosztása (például biztosítás megkötése, a tevékenység kiszervezése, a tranzakciók korlátozásnak összekapcsolása.
- **Elfogadás.** A kockázat csökkentésére nem tenni intézkedést.

11. A KOCKÁZAT ÉRTÉKELÉS FELÉPÍTÉSE

11.1. A KOCKÁZAT ÉRTÉKELÉS

11.1.1. A kockázat értékelés célja

11.1.2. A kockázat értékelés alkalmazott módszere

11.1.3. Az egyes veszélyforrások kockázatának azonosítása

11.1.3.1. Vállalati szintű kockázatok

11.1.3.2. A szervezési kockázatok

11.1.3.3. A technikai kockázatok

11.1.4. A kockázati mátrix

11.1.5. A rendszer biztonsági minősítése

11.1.5.1. A kockázati értékek táblázata

11.1.5.2. A biztonsági rendszer ellenálló képességének minősítése

11.1.6. A menedzsment döntése

12. BIZTONSÁGI STRATÉGIA KIDOLGOZÁSA

12.1. A BIZTONSÁGI STRATÉGIA CÉLJA

- ⇒ *a Megbízó döntése, és elkötelezettsége a kockázatok értékelése, és a „kockázat tudatos vállalása”, valamint a kockázati étvágy, és tűrőképesség alapján, a szükséges, és elégséges védelemről,*
- ⇒ *a biztonsági cél meghatározása, és*
- ⇒ *a biztonsági követelmények meghatározása.*

12.2. A KIDOLGOZÁS ALAPJA

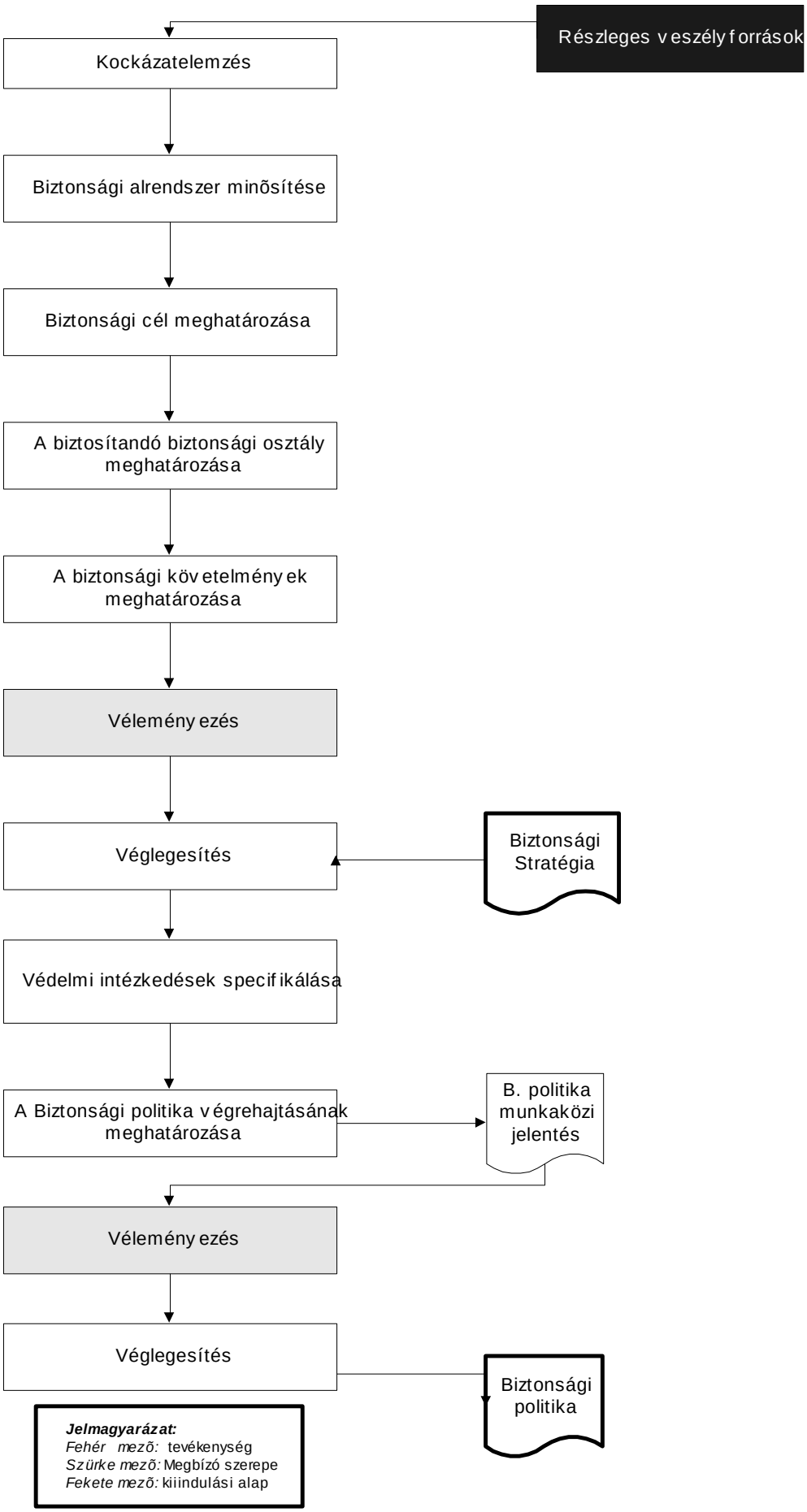
A Biztonsági Stratégia a veszélyforrás elemzésben feltárt veszélyforrások, az azonosított kockázatok értékelésén alapul, és meghatározza a kockázatok csökkentésének tervezési, és szervezési elveit, míg a Biztonsági Politika (biztonsági taktika) meghatározza a Stratégiában kitűzöttek megvalósításának eszközeit, a védelmi intézkedéseket.

12.3. A BIZTONSÁGI STRATÉGIA, ÉS POLITIKA FOLYAMATÁBRÁJA

A biztonsági Stratégia, és Politika készítésének folyamatábrája a következő oldalon található.

12.4. A BIZTONSÁGI STRATÉGIA FELÉPÍTÉSE

A Biztonsági stratégia tartalmát, felépítését a következő fejezetben adjuk meg.


Részleges veszélyforrások
Kockázatelemzés
Biztonsági alrendszer minõsítése
Biztonsági cél meghatározása
A biztosítandó biztonsági osztály meghatározása
A biztonsági követelmények meghatározása
Véleményezés
Véglegesítés
Biztonsági Stratégia
Védelmi intézkedések specifikálása
A Biztonsági politika végrehajtásának meghatározása
B. politika munkaközi jelentés
Véleményezés
Véglegesítés
Biztonsági politika
Jelmagyarázat:
Fehér mezõ: tevékenység
Szürke mezõ: Megbízó szerepe
Fekete mezõ: kiindulási alap

12.5. A KIINDULÓ FELTÉTELEK RÖGZÍTÉSE

A Biztonsági Stratégia a Megbízó igénye szerint készülhet csak az információ-rendszerre. Ebben az esetben ezt kiinduló feltételként rögzíteni kell, mivel az egyenszilárdság elvét sérti, ha nincs a vagyonbiztonságra Biztonsági Politika. Amennyiben van, rá kell mutatni a két Biztonsági Politika kölcsönös összefüggéseire.

12.6. A BIZTONSÁGI STRATÉGIA TARTALMA

12.6.1. A biztonsági cél

A biztonsági cél a menedzsment szándék nyilatkozata a vagyon-, és az IT biztonságot fenyegető veszélyforrások elleni védekezésről, a Biztonsági Politika elemeinek terjedelme, és a biztonsági cél, valamint követelmények kidolgozásához (lásd még 11.6.4.1 pont).
Az MSZ ISO/IEC 15408 szerint pedig:
A biztonsági cél:
Szándéknyilatkozat, azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági politikáknak és feltételezéseknek való megfelelésről.

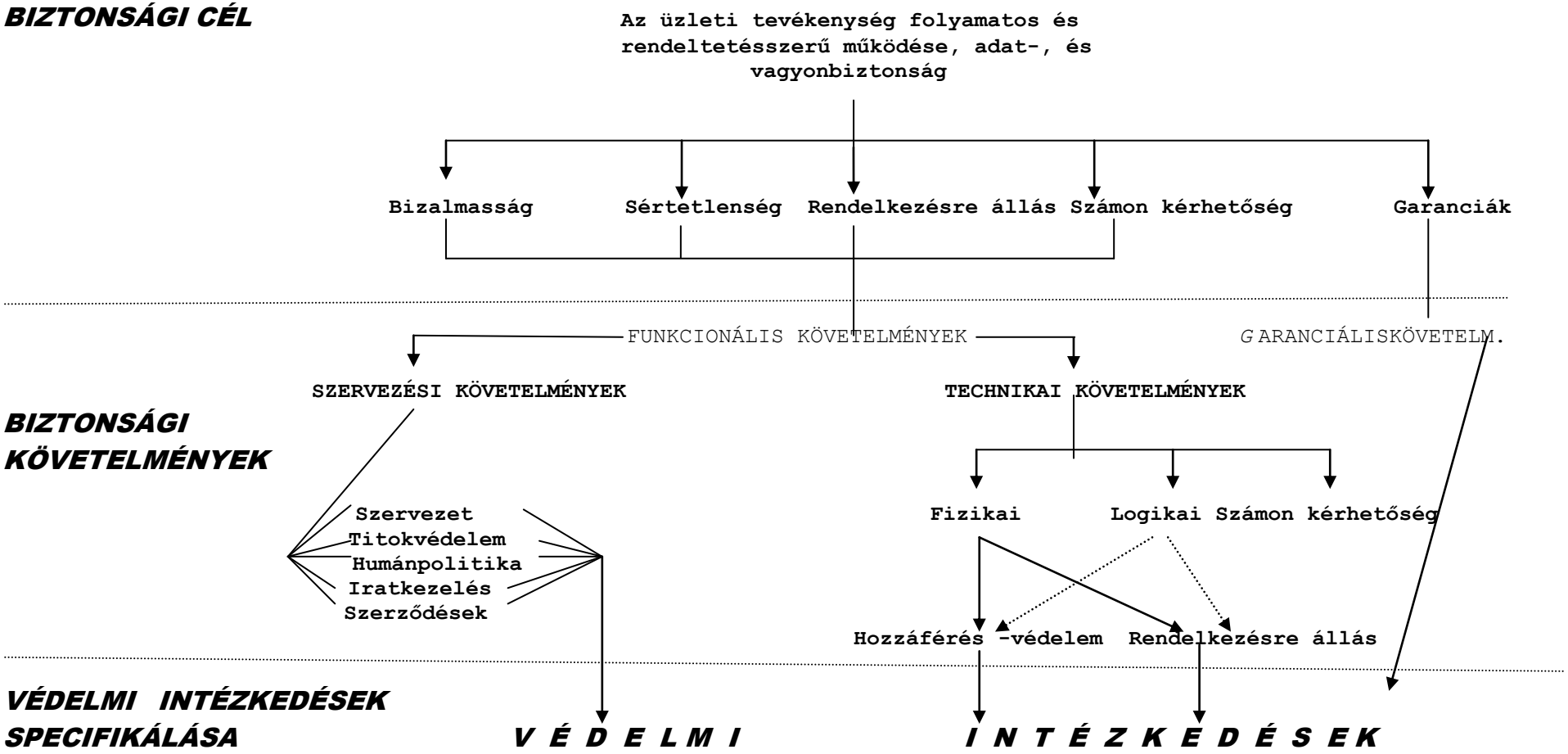
12.6.2. A biztonsági követelmények

A biztonsági követelményeket a bizalmasság, a sértetlenség, és a rendelkezésre állás minimális fenyegetettségének biztosításához szükséges elvárások képezik, azaz a Szervezési, és Technikai Biztonsági Politika. A biztonsági követelményeket nem veszélyforrásonként, hanem magas szinten kell meghatározni (lásd 9.9.4.. pont). A hozzáférés -védelmi követelmények kidolgozásához a CC 2.0-át célszerű felhasználni

<u>Az egyes követelményeknek a következőket kell tartalmazni:</u>

- ⇒ *a követelmény kódja, és rövid neve:*
- ⇒ *a követelmény meghatározása:*
- ⇒ *a követelmény mit véd? : lehetséges válaszok: C, I, A*

12.6.3. A Biztonsági Stratégia és Politika elemeinek terjedelme



12.6.4. A biztonsági cél, és a biztonsági követelmények (minta)

12.6.4.1. A biztonsági cél

⇒ *a vállalat üzletpolitikai követelményeinek teljesítése, az érték, és az információ-rendszer folyamatos és rendeltetésszerű működésének biztosítása az erőforrások bizalmassága, sértetlensége, és rendelkezésre állása fenyegetettségének a minimumra csökkentése, a számon kérhetőség, és a garanciák biztosítása. (Gazdasági szervezeteknél).*

⇒ *a szervezet a hatályos jogszabályokban meghatározott küldetésének teljesítése, az érték, és az információ-rendszer folyamatos és rendeltetésszerű működésének biztosítása az erőforrások bizalmassága, sértetlensége, és rendelkezésre állása fenyegetettségének minimumra csökkentése, a számon kérhetőség, és a garanciák biztosítása. (Igazgatási szervezeteknél).*

⇒ *A feltárt kockázatok el nem fogadása, védelmi intézkedések meg nem tétele, azaz a maradék kockázatok felvállalása bármely okból, például kis vállalatoknál, (amelyek humán, és anyagi erőforrásai korlátozottak) csak a szervezet biztonságáért felelős felső vezető dokumentált, és indokolt döntése alapján lehetséges (ISO/IEC 27001:2006, 1.2 pont szerint).*

12.6.4.2. Funkcionális biztonsági követelmények

⇒ *A **biztonsági követelmények** a biztonsági célok finomítására, meghatározására szolgálnak, és lehetnek funkcionális, és garanciális követelmények.*

12.6.4.2.1. Szervezeti, vállalati biztonsági követelmény

⇒ ***a követelmény kódja, és rövid neve:** KV-1. Vállalati biztonság*

- ***a követelmény meghatározása:** A szervezet, vállalat biztonságszervezését rendszer szemlélettel az egész vállalatra a biztonsági alrendszereket (vagyon, üzem, informatikai) összehangoltan kell meghatározni, megvalósítani.*
- **a követelmény mit véd? :** *C(bizalmasság), I(Sértetlenség), A (rendelkezésre állás)*

12.6.4.2.2. Szervezési biztonsági követelmények

Általános követelmény

⇒ ***a követelmény kódja, és rövid neve:** KÁ-1. IR határai.*

- ***a követelmény meghatározása:** Az IR területét, fizikai, és logikai külső, és belső határait, meg kell határozni, az üzleti tevékenység, a szervezet, az elhelyezés, az erőforrások, és a technológia függvényében.*
- **a követelmény mit véd? :** *C(bizalmasság), I(Sértetlenség), A (rendelkezésre állás)*

⇒ **a követelmény kódja, és rövid neve***: KÁ-2. Ellenálló képesség.*

- **a követelmény meghatározása:** *A biztonsági rendszer ellenálló képességére vonatkozó követelmény.*
- **a követelmény mit véd? :** *C(bizalmasság), I(Sértetlenség), A (rendelkezésre állás)*

Szervezet és működés

⇒ **a követelmény kódja, és rövid neve***: KSZ-1. Biztonsági szervezet.*

- **a követelmény meghatározása:** *Központosított biztonsági szervezet a vagyon, és az IT biztonság menedzselésére, a vállalat (szervezet) egész területére vonatkozó hatáskörrel.*
- **a követelmény mit véd? :** *C(bizalmasság), I(Sértetlenség), A (rendelkezésre állás)*

Titokvédelem

⇒ **a követelmény kódja, és rövid neve***: KSZ-2. Titokvédelem*

- **a követelmény meghatározása:** *A személyes, és a bankoknál: banktitkot, illetve értékpapírtitkot, valamint általában üzleti titkot képező adatok bizalmassága, sértetlensége, és rendelkezésre állása fenyegetettségének minimumra csökkentése. (*Gazdasági szervezetnél).
- **a követelmény mit véd? :** *C, I.*

⇒ **a követelmény kódja, és rövid neve***: KSZ-3. Üzleti titkok védelme.*

- **a követelmény meghatározása:** *Az üzleti titkot képező erőforrások védelme, az erőforrások bizalmassága, és sértetlensége fenyegetettségének minimumra csökkentése. (*Gazdasági szervezetnél).
- **a követelmény mit véd? :** *C, I.*

⇒ **a követelmény kódja és rövid neve:** *KSZ-4. Titokvédelem.*

- **a követelmény meghatározása:** *A hatályos jogszabályok, szabványok alapján a titokvédelem körét képező adatok, helyiségek, eszközök bizalmassága, sértetlensége, és rendelkezésre állása fenyegetettségének minimumra csökkentése. (*Igazgatási szervezetnél).
- **A követelmény mit véd:** *C,I.*

⇒ **a követelmény kódja és rövid neve:** *KSZ-5. A szolgálati érdekek védelme.*

- **a követelmény meghatározása:** *Az erőforrások védelme a szervezet küldetéséből következő, az erőforrás bizalmassága, és sértetlensége védelméhez fűződő méltányolható érdeke alapján. (*Igazgatási szervezetnél).
- **A követelmény mit véd:** *C,I.*

Humánpolitika

⇒ **A követelmény kódja és rövid neve:** *KSZ-6. Megbízhatóság.*

- **A követelmény meghatározása:** *A munkatársak munkaviszonyának létesítésénél a megbízhatósági követelmény érvényesítése, a munkaviszony alatt a megbízhatóság fenntartása, a munkaviszony megszüntetésekor pedig a bizalmasság védelme.*

- **A követelmény mit véd:** *C*.

⇒ **A követelmény kódja és rövid neve:** *KSZ-7. Munkaköri feladatok.*
- **A követelmény meghatározása:** *Az üzleti, informatikai, és biztonsági munkakörök nem foglalhatnak magukban biztonsági szempontból egymást kizáró feladatokat. tekintettel a biztonságkritikus munkakörökre.*
- **A követelmény mit véd:** *C.*

⇒ **A követelmény kódja és rövid neve:** *KSZ-8. Tudatosság.*
- **A követelmény meghatározása:** *Az informatikusok (munkatársak), és a felhasználók között a biztonsági tudatosság, és a biztonsági kultúra a vállalati biztonság szintjének megfelelő biztosítása.*
- **A követelmény mit véd:** *C.*

Iratkezelés

⇒ **A követelmény kódja és rövid neve:** *KSZ-9. Iratkezelés.*
- **A követelmény meghatározása:** *A papír alapú, és az elektronikus iratok, adatok kezelésének, archiválásának, és megsemmisítésének szabályozása a bizalmasság, a sértetlenség fenyegetettségének minimumra csökkentése céljából.*
- **A követelmény mit véd:** *C,I.*

Szerződések

⇒ **A követelmény kódja és rövid neve:** *KSZ-10. Szerződés.*
- **A követelmény meghatározása:** *A harmadikféllel kötött szerződésekben a szolgáltatásokkal szemben a bizalmasság, és a sértetlenség védelmének érvényesítése.*
- **A követelmény mit véd:** *C,I.*

12.6.4.2.3. Technikai biztonsági követelmények

Hozzáférés -védelem (fizikai, és logikai)

⇒ **A követelmény kódja és rövid neve:** *KT-1. Azonosítás.*
- **A követelmény meghatározása:** *A felhasználók azonosítása a belépés előtt, a jogosulatlan hozzáférés kizárása érdekében.*
- **A követelmény mit véd:** *C,I.*

⇒ **A követelmény kódja és rövid neve:***KT-2. Hozzáférés.*
- **A követelmény meghatározása:** *Az authorizált felhasználók hozzáférési jogosultságainak korlátozása, "az a jogosultság engedélyezhető, amely a munkakör ellátásához szükséges" elv, és a titokvédelemnél meghatározott védelmi szintek alapján.*
- **A követelmény mit véd:** *C,I.*

⇒ **A követelmény kódja és rövid neve:** *KT-3. Behatolás.*
- **A követelmény meghatározása:** *Megfelelő a helység védelmi osztályozásának megfelelő biztonsági fokozatú fizikai, és logikai behatolás jelzés, védelem.*
- **A követelmény mit véd:** *C,I,A.*

⇒ **A követelmény kódja és rövid neve:** *KT-4. Megkerülhetőség.*

- **A követelmény meghatározása:** *A hozzáférés -védelmi rendszer meg nem kerülhetőségének biztosítása.*
- **A követelmény mit véd:** *C,I.*

⇒ **A követelmény kódja és rövid neve:** *KT-5. Számon kérhetőség.*
- **A követelmény meghatározása:** *A hozzáférés -védelemben az események, tevékenységek számon kérhetőségének biztosítása.*
- **A követelmény mit véd:** *C,I.*

⇒ **A követelmény kódja és rövid neve:** *KT-6. Hfv-i rendszer védelme.*
- **A követelmény meghatározása:** *A hozzáférés -védelmi rendszer fizikai, és logikai védelme.*
- **A követelmény mit véd:** *C,I.*

Rendelkezésre állás védelme (fizikai, és logikai)

⇒ **A követelmény kódja és rövid neve:** *KT-7. Rendelkezésre állás.*
- **A követelmény meghatározása:** *Az erőforrások működőképességének, és a megfelelő helyen és időbeni elérhetőségének biztosítása, mind részleges mind átfogó sérülésük esetére.*
- **A követelmény mit véd:** *A.*

Hálózatok védelme

⇒ **A követelmény kódja és rövid neve:** *KT-8. Hálózat.*
- **A követelmény meghatározása:** *A bizalmasság, a sértetlenség, és a rendelkezésre állás fenyegetettségének minimumra csökkentése a hálózatban, és a csatlakoztatható más hálózatok felé.*
- **A követelmény mit véd:** *C,I,A.*

⇒ **A követelmény kódja és rövid neve:** *KT-9. Bizalmas útvonal*
- **A követelmény meghatározása:** *A biztonság kritikus információk bizalmas cseréje a felhasználók között, a felhasználók és rendszerek között, és a rendszerek között.*
- **A követelmény mit véd:** *C,I.*

⇒ **A követelmény kódja és rövid neve:** *KT-10. A másik fél, és a tranzakciók hitelesítése.*
- **A követelmény meghatározása:** *A jelszavak, tokenek, rejtjelezési kulcsok bizalmas cseréje, és a tranzakciók aláírása, valamint az aláírás hitelesítése.*
- **A követelmény mit véd:** *C,I.*

Számon kérhetőség biztosítása

⇒ **A követelmény kódja és rövid neve:** *SZ-1. Számon kérhetőség biztosítása.*
- **A követelmény meghatározása:** *A tevékenységek, információk, informatikai, és üzleti eszközök számon kérhetőségét, és a feltárt biztonsági események után a bizonyítékokat biztosítani kell. A tevékenységek naplóinak választ kell adnia 7W-re. Ki, mit, mikor, hol,*

honnan, hová, és min? A naplókat (log analysis) folyamatosan (tekintettel a keresztösszefüggésekre) elemezni kell.

- **A követelmény mit véd:** *C,I,A.*

A biztonsági technológia védelme:

⇒ **A követelmény kódja és rövid neve:** *A biztonsági technológia védelme*

- **A követelmény meghatározása:** *A biztonsági technológiát védeni kell a felfedés, megváltoztatás, és megsemmisítés ellen.*
- **A követelmény mit véd:** *C,I,A.*

12.6.4.3. Garanciális biztonsági követelmények

⇒ **A követelmény kódja és rövid neve:** *KG-1. Garancia.*

- **A követelmény meghatározása:** *A biztonsági környezetnek az érték (üzleti), és az információ-rendszer életciklusa minden fázisában biztosítania kell, hogy a védelmi intézkedések kikényszerítsék a biztonsági követelményeket, és összhangot az üzleti követelményekkel.*
- **A követelmény mit véd:** *C,I,A.*

⇒ **A követelmény kódja és rövid neve:** *KG-2. Teljes körűség.*

- **A követelmény meghatározása:** *A biztonsági követelményeket az üzleti, és az információs rendszer minden pontján érvényesíteni kell, figyelem bevéve az egyenszilárdság elvét, a vállalat kockázat tűrőképességét.*
- **A követelmény mit véd:** *C,I,A.*

⇒ **A követelmény kódja és rövid neve:** *KG-3. Ellenőrzés.*

- **A követelmény meghatározása:** *Rendszeres belső, és független külső ellenőrzés.*
- **A követelmény mit véd:** *C,I,A.*

⇒ **A követelmény kódja és rövid neve:** *KG-4. Biztonsági események*

- **A követelmény meghatározása:** *A biztonsági eseményeket kezelni kell, és a kezelés rendjének betartását ellenőrizni.*
- **A követelmény mit véd:** *C,I,A.*

⇒ **A követelmény kódja és rövid neve:** *KG-5. Életciklus.*

- **A követelmény meghatározása:** *Az indítási fázis, az erőforrások fejlesztése/beszerzése, szállítása, és kapacitás tervezése, átadás/átvétele, üzemeltetése, és selejtezése során a bizalmasság, és sértetlenség fenyegetettségének minimumra csökkentése*
- **A követelmény mit véd:** *C,I.*

⇒ **A követelmény kódja és rövid neve:** *KG-6. Konfiguráció.*

- **A követelmény meghatározása:** *A konfiguráció menedzsmentnek biztosítani kell, hogy az eredeti állapotát jogosulatlanul ne lehessen megváltoztatni.*
- **A követelmény mit véd:** *C,I.*

13. A BIZTONSÁGI STRATÉGIA FELÉPÍTÉSE

13.1. A BIZTONSÁGI CÉL

13.2. A BIZTONSÁGI KÖVETELMÉNYEK

13.2.1. Általános követelmény

13.2.1.1. Vállalati szintű, összehangolt védelem.

13.2.1.2. Az elérendő védelmi szint

13.2.2. Funkcionális követelmények I. Szervezési követelmények

13.2.2.1. Szervezet és működés

13.2.2.2. Titokvédelem

13.2.2.3. Humán politika

13.2.2.4. Iratkezelés

13.2.2.5. Szerződések

13.2.3. Funkcionális követelmények II. Technikai követelmények

13.2.3.1. Fizikai, és logikai hozzáférés védelem

13.2.3.2. Fizikai, és logikai rendelkezésre állás

13.2.3.3. Hálózati védelem

13.2.3.4. Számon kérhetőség

13.2.4. Garanciális követelmények

13.2.4.1. Garancia

13.2.4.2. Életciklus

13.2.4.3. Ellenőrzés

13.2.4.4. Biztonsági események kezelése

13.2.4.5. Teljes körűség

13.3. A BIZTONSÁGI STRATÉGIA KARBANTARTÁSA

13.4. A BIZTONSÁGI STRATÉGIA OKTATÁSA

13.5. AKCIÓ TERV

14. A BIZTONSÁGI POLITIKA KÉSZÍTÉSE

14.1. A BIZTONSÁGI POLITIKA CÉLJA

A Biztonsági Politika célja a biztonsági követelmények alapján a megfelelő részleges védelmi intézkedések kidolgozása, a kockázatok csökkentése érdekében (az üzleti-, és az információs rendszerre egyaránt).

14.2. A BIZTONSÁGI POLITIKA KÉSZÍTÉSÉNEK ALAPJA

A Biztonsági Politika készítésének alapja a Biztonsági Stratégia

14.3. A BIZTONSÁGI POLITIKA TARTALMA

A Biztonsági Politika valójában a biztonsági politikák (pl. hozzáférés védelmi, hálózati, humán politikai, stb. összessége.)

14.3.1. A védelmi intézkedések specifikálása

Védelmi intézkedések specifikálása, a védelmi követelményeket megvalósító védelmi intézkedéseknek a leírása. A lehetséges védelmi intézkedések típusait a 11.3.3 pont tartalmazza. A védelmi intézkedéseket az alábbiak figyelembe vételével kell specifikálni.

- ⇒ *Minden veszélyforráshoz az azt feltáró szakértőnek kell a védelmi intézkedést meghatározni.*
- ⇒ *Egy veszélyforráshoz több védelmi intézkedés is tartozhat, illetve egy védelmi intézkedés több veszélyforrásra is vonatkozhat.*
- ⇒ ***A védelmi intézkedés nem lehet konkrét termék meghatározása.***
- ⇒ *Egyes esetekben elképzelhető (a Biztonsági Politika első változatában) alternatív javaslat, de ekkor a változatok előnyeit, és hátrányait is meg kell adni.*
- ⇒ *A megfelelő védelmi intézkedéseket, az általános védelmi követelmény (KA-1) alapján kiválasztott biztonsági osztályba sorolt védelmi intézkedések képezik.*
- ⇒ *Az üzleti érdekek, célok, a védelmi intézkedések költségeinek figyelembevétele.*

14.3.1.1. A védelmi intézkedések költséghatékonysága

*A védelmi intézkedések megvalósítása, üzemeltetése jelentős költségekkel jár. Ugyanakkor **alkalmazásuk eredménye, a biztonság**, amelynek értékét exakt számokkal egyértelműen nem lehet megadni.*

Tekintettel arra, hogy olyan hazai illetve nemzetközi statisztika nem valószínű, hogy található, vállalati még kevésbé, amely egy időszakra a nem megfelelő védelem által okozott károkat kimutatja, ez az út nem járható. A hatékony védelem úgy mérhető, hogy értékeljük a biztonsági események egyes időszakokra vonatkozó naplóját, és levonjuk azt a következtetést, hogy szükséges-e a maradék

kockázatokat, illetve az újonnan keletkezett kockázatokat csökkenteni. Azaz a költséghatékonyság a biztonság, a gazdasági szervezet védelmére úgy mutatható ki, hogy megállapítható-e a biztonság minimális fenyegetettsége egy időszakra (pl. egy évre) a bekövetkezett biztonsági eseményekből (a biztonsági események száma, és súlyossága alapján).

Járható út az is, ha a kockázat értékelésnél megadott becsült kárértéket, hasonlítjuk össze a kockázat csökkentésre tett védelmi intézkedések költségeivel.

E mellett azonban a biztonságszervező nem hagyhatja figyelmen kívül a gazdasági szervezet érdekeit, a mennél kevesebb költség, és mennél nagyobb biztonságban. Ezért az alábbi osztályozások alapján a védelmi intézkedések meghatározásakor, a megvalósítás költségeit figyelembe kell venni, és adott esetben a gazdasági szervezet kívánságára, és felelősség vállalása mellett gyengébb, kevesebb költséggel járó védelmi intézkedéseket kell specifikálni. Rá kell mutatni arra, hogy az alábbi összefüggés áll fenn a költségek és a védelmi intézkedések között:

KÖLTSÉG CSÖKKENTÉS
⬇
A VÉDELEM ERŐSSÉGÉNEK CSÖKKENÉSE
⬇
A MARADÉK KOCKÁZAT NÖVEKEDÉSE

14.3.1.2. A biztonsági technológia védelme

A biztonsági technológiát, azaz a védelmi intézkedéseket, és az azokat realizáló hw, és sw eszközöket védeni kell felfedés, megváltoztatás és megsemmisítés ellen.
Ilyen eszközök például: a fizikai, és logikai belépés, és behatolás védelem eszközei, mint például a bizalmas számítástechnikai bázis (hw, és sw eszközök, amelyek kikényszerítik egy szervezet biztonsági politikáját), az audit trail, audit log, a naplók, és általában a védelmi intézkedéseket realizáló eszközök, intézkedések).

14.3.2. A biztonsági osztályok és az alkalmazók

A következő táblázat a biztonsági osztályokat határozza meg az adatok titokvédelmi osztályozását, és az információ-rendszert figyelembe véve. Továbbá megadja az egyes osztályok javasolt alkalmazóit. A biztonsági osztályok növekvő biztonsági szintek szerint: D, C, B, A; az indexek: $_A$–alacsony; $_K$–közepes, $_M$–magas.

Biztonsági osztályok	Az alkalmazások védelmi osztályba sorolása*	Az információ-rendszer jellemzői	A tipikus alkalmazó szervezet
Egyszerű biztonság (D_K)	➢ 4	➢ Hálózatba nem kötött PC-k	➢ Kis hazai cég
Alap biztonság (D_M)	➢ Jellemző: 3	➢ LAN, szigetmegoldások	➢ Kis hazai cég ➢
Védett biztonság (C_A)	➢ Jellemző: 3 ➢ Kivétel: 2	➢ LAN, szigetmegoldások	➢ Kis bank ➢ Közepes hazai cég
Auditált biztonság (C_K)	➢ Jellemző: 2 ➢ Kivétel: 1 (üzleti titkok)	➢ WAN, részlegesen integrált rendszer	➢ Közepes és nagy bank ➢ Nagy hazai cég ➢ Közepes nemzetközi cég ➢ Államigazgatási szervezetek ➢ Önkormányzatok
Megerősített biztonság (C_M)	➢ Jellemző: 1 (üzleti titkok)	➢ WAN, integrált rendszer	➢ Nagy hazai cég ➢ Nagy nemzetközi cég ➢ államtitkokkal dolgozó szervezetek
Strukturált biztonsági kategóriák (B)	➢ 1 (államtitok)	➢ WAN integrált rendszer	➢ Minisztériumok ➢ Fegyveres testületek
Biztonságos fejlesztés (A)	➢ 1 (államtitok)	➢ WAN, integrált rendszer ➢ Szigorúan titkos fejlesztés	➢ Nemzetbiztonsági szervezet

** a védelmi osztályozást lásd e fejezet k. pontjában*

Mivel polgári felhasználásra a $D_A - C_M$ biztonsági osztályokat indokolt használni, ezért a következőkben csak ezekkel foglalkozunk.

14.3.2.1. A biztonsági osztályok ismertetése

Egyszerű (D_K) biztonsági osztály

A szervezet biztonságtechnikai szempontból alacsony szintű, minimális védelmi intézkedésekkel igyekszik biztosítani erőforrásainak a védelmét. Nincs biztonsági rendszer, így sem az információ-rendszer, sem az üzleti rendszer ellenálló képessége nem értelmezhető.

Alap (D_M) biztonsági osztály

A védelmi követelmény az amatőr színvonalú támadások elleni védekezés.

Nincs biztonsági rendszer, így az üzleti-, és az információ-rendszer ellenálló képessége nem értelmezhető.

Védett (C_A) biztonsági osztály

A védelmi követelmény az egész szervezetet, és tevékenységet átfogó, a veszélyforrások bekövetkezési valószínűségét tudatosan csökkentő olyan biztonsági rendszer, amely az üzleti-, és az információ-rendszernek a nyilvánvaló (ismert) támadási potenciálú támadásokkal szembeni ellenálló képességét biztosítja.

Auditált (C_k) biztonsági osztály

A védelmi követelmény az egész szervezetet, és tevékenységet átfogó, a veszélyforrások bekövetkezési valószínűségét tudatosan csökkentő olyan biztonsági rendszer, amely az üzleti-, és az információ-rendszernek korlátozott alkalmakkal, és erőforrásokkal, a közepes támadási potenciálú támadásokkal szembeni ellenálló képességét biztosítja.

A szervezet külső auditorokat von be a védelmi szint ellenőrzése, és fenntartása érdekében.

Megerősített (C_M) biztonsági osztály

A védelmi követelmény az egész szervezetet, és tevékenységet átfogó, a veszélyforrások bekövetkezési valószínűségét csökkentő olyan biztonsági rendszer, amely az üzleti, és az információ-rendszernek a kifinomult támadási potenciálú támadásokkal szembeni ellenálló képességét biztosítja.

Az egyes biztonsági osztályok, és a biztonsági rendszer ellenálló képessége közötti összefüggés a következő:

D ➔ nem ellenálló,
C_A ➔ nyilvánvalóan ellenálló,
C_K ➔ mérsékelten ellenálló, és
C_M ➔ magasan ellenálló.

14.3.2.2. A védelmi intézkedések az egyes biztonsági osztályokban

Az alábbi táblázatban megadjuk az egyes biztonsági osztályokhoz mely védelmi intézkedések tartoznak. A (-) jelölés azt jelenti, hogy nincs védelmi intézkedés, az (NÚ) jelölés pedig azt, hogy nincs új (plussz). C_M-től növekvő irányban, a szereplő védelmi intézkedések a korábban megadottakat magukban foglalják, tehát csak a pluszokat adjuk meg. A gyakorlatban előfordulhat, hogy egy biztonsági osztályba sorolt rendszernél magasabb biztonsági osztályba tartozó védelmi intézkedést is alkalmaznak.

Biztonsági osztály➔ Védelmi intézkedés➘	D_K	D_M	C_A	C_K	C_M
Szervezési ***Biztonsági szervezet***	—	Egyes témákra felelősök	Külön vagyon, és IT biztonsági szervezet, az adatvédelem leválasztva	Integrált, centralizált adat, és vagyonbiztonsági szervezet	Elosztott IT biztonsági szervezet
Biztonságszervezés	—	Adatvédelmi utasítás	Kockázat menedzsment Biztonsági Politika	Katasztrófaterv Biztonsági Szabályzat	NÚ
Humánvédelem	Munkaviszony létesítésénél	NÚ	Megbízhatóság védelme a munkaviszony létesítésénél, alatt, és megszüntetéskor	Feladatszétválasztás	NÚ
Titokvédelem	Általános követelmények	NÚ	Adatok és alkalmazások osztályozása	Eszközök , és helyiségek osztályozása	Növelt számú védelmi osztályok
Kockázat áthárítás	Vagyonbiztosítás	NÚ	NÚ	Üzleti tevékenység megszakadására biztosítás	NÚ
Biztonság ellenőrzése	Belső ellenőrzés	NÚ	NÚ	Független auditálás	NÚ
Technikai Fizikai hfv	Élőerős védelem	Belépés ellenőrzés helyenként Sziget megoldások az épület, illetve a biztonság felügyeleti rendszerben	Belépés, és mozgás ellenőrzés Behatolás védelem Épület felügyeleti rendszer Biztonság felügyeleti rendszer	Integrált épület-, és biztonság felügyeleti rendszer Harmadik fél korlátozása az eszköz karbantartásban, és a védelmi intézkedések üzemeltetésében	Erős jelszó rendszer (biometriai azonosítás) Harmadik féllel szemben a Biztonsági Politika érvényesítése
Fizikai rend. állás	Tűzvédelem Polgári védelem Villámvédelem	Szünetmentes áramellátás Géptermek klimatizálása	Részleges eszköz rendundancia	EMC védelem Komplett, és háttér tárolt dokumentációk	Hibatűrő rendszer
Biztonsági osztály➔	D_K	D_M	C_A	C_K	C_M

Védelmi intézkedés ↓					
Logikai hfv	Egyszerű jelszó rendszer	NÚ	CC-CS1-2 (DAC) Tevékenységek számon kérhetősége (account) Tartalmi hitelesség védelem a levelezésben	CC-CS3 (RBAC) Audit trail Rejtjelezés (RSA) Behatolás védelem Biztonsági események kezelése	CC-Labeled Security Protection Profile (MAC) Egy jelszavas hfv. (SSO) Rejtjelezés(DES) Védelmi intézkedések hfv-e
Logikai rend. állás	Eseti mentések Vírusvédelem	NÚ	Rendszeres mentés	Help desk Alkalmazói, és rendszerszoftver mentések, és a forrásnyelvi változatok háttér tárolása Aktív vírusvédelem, vírus védelmi rendszer EMC védelem Naprakész dokumentációk Forró háttér	Döntés támogatott help desk Lokális, vagy távoli hibatűrő rendszer Vírus katasztrófa védelem
Hálózat védelem	—	—	Fizikai védelem Részleges redundancia	Üzenet rejtjelezés (RSA) Üzenetek tartalmi hitelesség védelme Hfv. a nem bizalmas csatlakozások felé (tűzfal, jelszó)	Bizalmas útvonal Üzenet rejtjelezés (DES) Kulcselosztás, RSA PKI
Életciklus védelem	—	—	Logikailag leválasztott fejlesztés A selejtezés szabályozása	Védelmi követelmények a fejlesztési célban Fizikailag, és humán szempontból leválasztott fejlesztés Átadás/átvétel biztonsági ellenőrzés Programcsere menedzsment Harmadikfél korlátozása a rendszerkövetésben	Garnciák arra, hogy a védelmi intézkedések kikényszerítsék a védelmi követelményeket Beszerzésnél biztonsági intézkedések Szállítás biztonsági ellenőrzése, ,és szállítói biztonsági nyilatkozat Harmadikfélnél a Biztonsági Politikának megfelelő követelmények érvényesítése

Az egyes védelmi intézkedéseknél a következőket kell megadni:

- ⇒ *a védelmi intézkedés azonosítója és neve (rövid),*
- ⇒ *a védelmi intézkedés specifikációja,*
- ⇒ *mely biztonsági követelményt realizálja,*
- ⇒ *mely veszélyforrás(-ok) ellen véd.*

14.3.3. Védelmi intézkedések köre I (funkcionális)

A. RÉSZLEGES VÉDELMI INTÉZKEDÉSEK
I.SZERVEZÉSI

1. Vállalati szintű, összehangolt védelem
1.1. Integrált biztonsági alrendszerek
1.2. Vállalati szintű kockázat menedzsment
2. szabályozás
2.1. adat védelem, és titokvédelmi osztályozás
2.2. biztonsági szervezet
2.3. Iratkezelés
3. humán politikai védelmi intézkedések
3.1. megbízhatóság munkaviszony létesítéskor, megszűntekor
3.2. megbízhatóság alkalmazás alatt
3.2.1. teljesítménykövetés
3.2.2. feladat szétválasztás
3.2.3. oktatás,
3.2.4. biztonsági kultúra, biztonsági tudatosság
3.2.5. humán tűzfal,
3.2.6. megtévesztés elleni védelem
4. szerződések
3.2. vagyonbiztosítás
3.2. biztonsági követelmények a harmadikfél felé
3.2. SLA-SLM

II. TECHNIKAI

1. fizikai védelmi int.-ek

1.1. aktív támadás elleni hfv

1.1.1. objektum védelem
1.1.2. belépés és mozgás ellenőrzés
1.1.3. behatolás védelem
1.1.4. értéktárolás védelem
1.1.5. értékszállítás védelem
1.1.6. mobil eszközök védelme
1.1.7. üres íróasztal, és képernyő politika

1.2. passzív támadás elleni hfv

1.2.1. kisugárzás elleni védelem (akusztikus, el. mágneses)

1.3. rendelkezésre állás

1.3.1. megbízhatóság
1.3.2. redundancia
1.3.3. energiaellátás
1.3.4. villámvédelem
1.3.5. tűzvédelem
1.3.6. dokumentáció

2. logikai védelmi int.-ek

2.1. aktív tám. elleni hfv

2.1.1. jelszó mgm
2.1.2. SSO
2.1.3. jogosultság mgm
2.1.4. vállalati szintű ID kezelés
2.1.5. hitelesítés
2.1.6. tanúsítás
2.1.7. időbélyegzés
2.1.8. behatolás védelem
2.1.9. tűzfal

2.2. passzív tám. elleni hfv

2.2.1. rejtjelezés
2.2.2. titokmegosztás

2.3. rendelkezésre állás

2.3.1. mentés, újraindítás
2.3.2. vírusvédelem
2.3.3. logikai rombolás
2.3.4. dokumentáció
2.4. Számon kérhetőség

3. Hálózat védelem

3.1. logikai hfv

3.1.1. *személyhitelesítés*
3.1.2. *tartalomhitelesítés*
3.1.3. letagadhatatlanság
3.1.4. *eszközhitelesítés*
3.1.5. eredet, tulajdonság tanúsítás, pki
3.1.6. bizalmas útvonal
3.1.7. tűzfal
3.1.8. behatolás jelzés

3.2. fizikai hfv.

3.3. rendelkezésre állás

3.3.1. fizikai r. áll.
3.3.2. logikai r. á.

4. IR életciklus véd.

4.1. fejlesztés
4.2. átadás/átvétel
4.3. üzemeltetés
4.4. selejtezés

5. A biztonsági technológia védelme

5.1. A bizalmas számítástechnikai bázis fizikai, és logikai védelme
5.2. A rejtjelező eszközök, kulcsok fizikai, és logikai védelme
5.3. Fizikai, és logikai naplók védelme

14.3.4. Védelmi intézkedések köre II (funkcionális).

B. ÁTFOGÓ VÉDELMI INTÉZKEDÉSEK

I. SZERVEZÉSI *II. TECHNIKAI*

1. szabályozás
- *1.1.katasztrófa minősítés*
- *1.2.katasztrófa teamek szervezése*
- *1.3.A katasztrófa- terv karbantartása*
- *1.4.oktatás*

2. szerződés
- *2.1.biztosítás a folyamatos működésre*
- *2.2.üzemi háttérszerződés*
- *2.3.szállítói háttérszerződés*

1.rendelkezésre állás
- *1.1.visszaállítás*
- *1.2.hátterek, háttér eljárások*
- *1.3.Katasztrófa kezelő központ*
- *1.4.helyreállítás*

A BETŰTÍPUSOK JELENTÉSE
(a védelmi intézkedés mit véd?):

Ariel black = címsor

Ariel = bizalmasság

Ariel = sértetlenség

ARIEL = bizalmasság és sértetlenség

Courier new = rendelkezésre állás

Courier new = mind a három

14.3.5. Védelmi intézkedések köre III (garanciális).

1. **A védelmi intézkedéseket úgy kell meghatározni, hogy azok kikényszerítsék a biztonsági követelményeket.**
2. **Meg kell határozni, és alkalmazni kell, a védelmi intézkedések erősségének specifikálásánál, a kockázat tűrőképességet.**
3. **Biztosítani kell a rendszeres belső, és külső független ellenőrzést,**
4. **A rendszerek életciklusának minden fázisában a biztonsági cél elérésére védelmi intézkedéseket kell tenni.**
5. **A konfiguráció menedzsment minden fázisában az eredeti állapotot megfelelően kezelni kell.**

14.3.6. A védelmi osztályozás (minta)

Az informatikai biztonság szervezésénél, adatokra, alkalmazásokra, eszközökre és helyiségekre, míg a vagyonbiztonság szervezésénél adatokra, anyagokra, eljárásokra, eszközökre, és helyiségekre kell az osztályozást elvégezni. Az MSZ ISO/IEC 17799 előírja, hogy az adatokat biztonság érzékenységük szerint osztályozni kell, míg a helyiségeket rendeltetésük biztonság érzékenysége, az eszközöket szintén rendeltetésük biztonság érzékenysége szerint arányos védelemben kell részesíteni, amihez osztályozni kell őket a biztonság érzékenységük szerint. A védelmi osztályba sorolást a védendő a jogszabályokban meghatározott kötelezettségei, illetve a vállalat üzleti érdekei lapján meghatározott bizalmassági, és sértetlenségi követelményei alapján kell elvégezni. Az osztályozás célja a védelmi intézkedések specifikálásához a védelem erősségének, mint követelménynek a meghatározása. A védelmi osztályok a következők:

Védelmi osztályok	***Védendő***		***Hozzáférés***	
	Bizalmasság	***Sértetlenség***	***Belső***	*Külső*
1.	***Igen kritikus***	***Életbevágó***	***Erősen korlátozott***	***Erősen korlátozott***
2.	***Kritikus***	***Életbevágó***	***Korlátozott***	***Erősen korlátozott***
3.	***Nem kritikus***	***Fontos***	***Nem korlátozott***	***Korlátozott***
4.	***Nem kritikus***	***Nem életbevágó***	***Nem korlátozott***	***Nem korlátozott***

*Az adatok osztályozása a titokvédelemre kötelezett szervezeteknél a titokvédelmi minősítés, a titokvédelemre nem kötelezett gazdasági szervezeteknél pedig az üzleti titokról („üzleti titok mind az, aminek a védelméhez a gazdasági szervezetnek méltányolható érdeke fűződik, és **a védelmére a gazdasági szervezet intézkedéseket tett**"), és a személyes adatok, illetve a banktitok, és az értékpapírtitok védelméről szóló jogszabályok végrehatása érdekében védelmi osztályozást kell készíteni.*

⇒ **Adatok védelmi osztályai:**

- **1. Osztály. Titkos adatok**. Ide sorolandók azok az adatok, amelyekhez a belső, és külső hozzáférés t erősen korlátozni kell, és a sértetlenségük életbevágó. Pl.:
  - ***az államtitkok***,
  - az erősen védendő üzleti titkok,
  - az erősen védendő ügyféladatok (bank-, biztosítási, értékpapírtitok).
- **2. Osztály Bizalmas adatok**. Ide sorolandók azok az adatok, amelyekhez a belső, és külső hozzáférést korlátozni kell, és sértetlenségük életbevágó. Pl.:
  - ***a szolgálati titkok***,
  - a közepesen védendő üzleti titkok,
  - az ügyféladatok (banktitkok, biztosítási titok, értékpapír titok),

- a munkatársak személyes adatai.

➢ **3. Osztály. Belső adatok.** Ide sorolandók azok az adatok, amelyeknek a felfedése nem kritikus, csak a külső hozzáférés t kell korlátozni. A sértetlenségük fontos, de nem életbevágó. Pl.:
- ***a csak belső felhasználásra szolgáló szolgálati adatok,***
- a csak belső felhasználásra szolgáló üzleti adatok,
- a harmadik felek munkatársainak adatai.

➢ **4. Osztály. Nem osztályozott adatok.** Ide sorolandók azok az adatok, amelyeknek a felfedése nem kritikus, sebezhetőségük nem életbevágó. Pl.:
- a védelmet nem igénylő adatok.

Az állam-, és a szolgálati titok a titokvédelmi törvény alapján minősítésre kötelezett szervezetekre vonatkozik.
Az osztályozást az adat megőrzi teljes életciklusa alatt, és akár papír, akár elektronikus adathordozón van rögzítve, fel kell tüntetni.

⇒ **Folyamatok, alkalmazások védelmi osztályai.**
A védelmi osztályokba a folyamatokat, az alkalmazásokat a szerint kell besorolni, hogy az alkalmazások által kezelt, illetve előállított adatok milyen védelmi osztályba vannak sorolva. Amennyiben az alkalmazás több védelmi osztályba sorolt adatot kezel a legerősebb védelmi osztály a mértékadó.

⇒ **Helyiségek védelmi osztályai:**

➢ ***1. Osztály. Zárt helyiségek****, ahová csak erősen korlátozott számú személyek léphetnek be, akiknek erre jogosultságuk van. Ide tartoznak, a számítóközpontok, adathordozó raktárak, az épület felügyeleti és biztonsági felügyeleti rendszer központi berendezéseinek helyiségei. A zárt terület csak ellenőrzött területről nyílhat.*

➢ ***2. Osztály. Kiemelten ellenőrzött helyiségek,*** *ahová a saját munkatársak belépése korlátozva van. Például LAN-ok szerverei elhelyezésre szolgáló helyiségek, az üzemi helyiségek, energiaellátó berendezések, távközlési és energiaellátó kábelek csatlakozási pontjai és az elosztók, raktárak, klimatizáló berendezések helyiségei, dokumentumtárak, pénztárak.*

➢ ***3. Osztály. Ellenőrzött helyiségek,*** *ahová a munkatársak, illetve a látogatók ellenőrzés után léphetnek be. Például az irodák.*

➢ ***4. Osztály. Nem osztályozott helyiségek,*** *ahová bárki minden további nélkül beléphet. Idetartoznak az ügyfélszolgálatot ellátó irodák, bankfiókok ügyfélkiszolgáló helyiségei.*

⇒ **Eszközök, eljárások, értékek védelmi osztályai:**

➢ ***1. Osztály. Titkos eszközök****. Ide tartoznak azok a speciális eszközök, berendezések, amelyek hozzáférés e kiemelten korlátozott kell legyen. Pl. rejtjelező gépek.*

➢ ***2. Osztály. Bizalmas eszközök.*** *A fizikai, és a logikai hozzáférés - védelmi szoftver. Egyes eljárások (pl. know how alapján alkalmazott eljárás, gyártási titok, fejlesztés, új üzletág), és az azokat realizáló*

eszközök, berendezések, valamint értékek (anyagok, félkész, és késztermékek, készpénz, értékpapírok, értéktárgyak).

- ***3. Osztály. Belső használatra szolgáló eszközök.*** *Egyéb hw, és rsw-ek.*
- ***4. Osztály. Nem osztályozott eszközök.*** *Nyilvános helyen üzemeltetett berendezések.*

14.3.7. A védelmi osztályozás alkalmazása

A védelmi osztályozást a fizikai hozzáférés-védelemnél, valamint a logikai hozzáférés védelemnél kell alkalmazni. Mégpedig a következőképen

⇒ A fizikai hozzáférés védelemnél a helyiségek védelmét az osztályozás alapján legalább az egyes osztályokban a következőképpen kell kialakítani:

Védelmi Osztály	*Belépés ellenőrzés*	*Mozgás ellenőrzés*	*Behatolás védelem*	*Tűz-Védelem*	*Légálla-pot vé-Delem*	*EMC EMI véd.*	*Felügyelet*
I. zárt	*E*	*E*	*E*	*E*	*T*	*T*	*T*
II. kiemelt	*R*	*R*	*R*	*N*	*R*	*-*	*T*
III. ellenőrzött	*M*	*M*	*M*	*N*	*R*	*-*	*T*
IV. nem oszt.	*É*	*M*	*-*	*N*	*-*	*-*	*É*

A jelölések: E= erősített, É= élőerővel, M= minimális, N= normál, R= részleges, T= teljes.

Az objektumok informatikai területeinek, illetve helyiségeinek védelmi osztályba sorolása (példa):

- ***I. zárt terület:*** számítóközpont, integrált felügyeleti központ, távközlési központ,
- ***II. kiemelt terület*****:** terminál szobák**,** elektronikus adathordozó, és berendezés raktár, szünetmentes áramellátó, klíma központ, energia és távközlési becsatlakozások, elosztók, papír alapú adathordozó raktár, pincék, expedíció,
- ***III. ellenőrzött terület:*** irodák, folyosók, emeleti előterek, udvar,
- ***IV. nem osztályozott terület:*** főbejárati előtér, ügyfélszolgálat

A zárt, és a kiemelt terület nem nyílhat nyílt területről. Az I-III. kategóriájú területen belül meg engedett további azonos vagy más I-III. kategóriába sorolt terület kialakítása, a belépési jogosultságok korlátozása, a belépés, és a mozgás ellenőrzése céljából.

A belépés ellenőrzés az egyes védelmi osztályokban:

I. Zárt terület.
A zárt terület hátárán kétirányú elektronikus, és mechanikai ellenőrzés, a területen belül leválasztott zárt területeken kétirányú elektronikus ellenőrzés.
II. Kiemelt terület.
Kétirányú elektronikus ellenőrzés.
III. Ellenőrzött terület.
A belépés elektronikus ellenőrzése.
IV. Nem osztályozott terület.
Ellenőrzés élőerővel.

A mozgás ellenőrzés az egyes védelmi osztályokban:

I. Zárt terület.
Teljes körű térvédelem. Zártláncú videó rendszerhez csatlakozó videó kamerák a terület határán, és a biztonságkritikus pontokon.
II. Kiemelt terület.
Részleges térvédelem. A terület határán videó kamerák.
III. Ellenőrzött terület.
A terület határán videó kamerák.
IV. Nem osztályozott terület.
A terület videó kamerákkal ellenőrzött.

Fizikai behatolás védelem az egyes védelmi osztályokban:

I.Zárt terület.
Erősített felületvédelem,
II. Kiemelt terület.
Minimális felületvédelem utcai fronton, és szomszédos épülettel közös falon.
III. Ellenőrzött terület.
Felületvédelem a szomszédos épülettel közös falon.
IV. Nem osztályozott terület.
Nincs behatolás védelem.

Tűzvédelem az egyes védelmi osztályokban:

A hatósági előírások szerint.

Elektromágneses kompatibilitás védelem az egyes védelmi osztályokban:

A zárt területen.

Integrált felügyeleti rendszer az egyes védelmi osztályokban:

Az integrált felügyeleti rendszer irányítja, és ellenőrzi az épületautomatikai, és a biztonságtechnikai felügyeleti rendszert, és a következőket foglalja magába:

Épületautomatika:

- *Villamos energiaellátó rendszer,*
- *szünetmentes áramellátó rendszer,*
- *fő-, és installációs elosztó berendezés ellenőrzése,*
- *villamos kapcsolások, liftek,*
- *fogyasztásmérés, energiaoptimalizálás,*
- *hő központ, hűtési rendszer,*
- *fűtési rendszer,*

- *füst, és tűzjelző rendszer,*
- *automatikus tűzoltó rendszer.*

Biztonsági rendszer:

- *belépés ellenőrző rendszer,*
- *mozgás ellenőrző rendszer,*
- *behatolás védelmi rendszer,*
- *zártláncú videó rendszer,*
- *kapcsolat a hatóságok felé (rendőrség, tűzoltók, mentők).*

Az integrált felügyeleti rendszer központja az egyes rendszer elemekkel strukturált univerzális hálózattal kacsolódik. A hálózat, és végpontok elemeit fizikai hozzáférés védelemmel kell ellátni. A felügyeleti rendszer központ számítástechnikai erőforrásai logikai hozzáférés-védelmére, és a részleges rendelkezésre állásának a biztosítására intézkedéseket kell tenni.

⇒ *A logikai hozzáférés védelemnél az egyes védelmi osztályokban a jelszórendszer, és a jogosultsági rendszer erősségét a következőképpen kell meghatározni:*

Védelmi osztályok	***Hozzáférés***	
	Belső	*Külső*
1.	***Erősen korlátozott***	***Erősen korlátozott***
2.	***Korlátozott***	***Erősen korlátozott***
3.	***Nem korlátozott***	***Korlátozott***
4.	***Nem korlátozott***	***Nem korlátozott***

A belső hozzáférés korlátozása azt jelenti, hogy

az 1. Véd. osztályban legalább egyszer használatos jelszót, államtitkok esetén titokmegosztást is alkalmazni kell, a jogosultsággal csak szűk kör rendelkezhet a betekintési jogokat figyelembe véve, ami az emberileg olvasható outputok elérésének korlátozását, valamint elérési jogosultság esetén a hard copyk kezelésének szigorú szabályozását jelenti.

A 2. Véd. osztályban alkalmazható többször használatos jelszó, de a szükséges tudás elve alapján adott jogosultságokkal.

A külső hozzáférés korlátozása azt jelenti, hogy

Az erősen korlátozott esetben (a minősített adatoknál az 1. Védelmi osztályban) nem férhet hozzá senki, a korlátozott adatoknál (például dial in porton keresztül) csak egyszer használatos jelszóval, és az emberileg olvasható outputok kinyomtatási, illetve adathordozóra másolási jogosultsága nem engedhető meg. A 2. védelmi osztályban

külső hozzáférés szigorú felhasználó azonosítás (egyszer használatos jelszó), és a port védelme mellett engedélyezhető.

14.3.8. A titokvédelemmel és biztonsággal foglalkozó hatályos jogszabályok, és szabványok

⇒ *A biztonsággal kapcsolatos szabványok*
- *MSZ-ISO/IEC 27001:2005 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.*
- *MSZ-ISO / IEC 17799-2003, Információ technika. .Az informatikai biztonság eljárás rendje.*
- *MSZ-ISO / IEC 15408-1,2,3 Információ technika. Az IT biztonság értékelési szempontjai.*
- *MSZ-EN 50131-1 riasztó rendszerek. Behatolás jelző rendszerek.*
- *FIPS PUB 140-2 Security Requirements for Cryptographic Modules*
- *BS 7799-1:2000, Information technology — Code of practice for information security management.*
- *BS 7799-2:2002, Information security management systems — specification with guidance for use.*
- *MSZ ISO/IEC 11770-1. Informatika. Biztonság. Kulcsgondozás (elő szabvány).*
- *ISO/IEC 13335-1,2,3,4,Information Technology-Guidelines for the Management of IT Scurity.81996-2000).*

⇒ *A titokvédelemmel kapcsolatos törvények:*
- *1995. évi LXV. tv. .Az államtitokról és a szolgálati titokról.*
- *1992. évi LXIII. tv. A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.*
- *43/1994.(III. 29.) Korm. r. A rejtjeltevékenységről.*
- *1992.évi LXXII. tv. a távközlésről*
- *a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. Évi LXVI. tv.*
- *az üzleti titok a Büntető törvénykönyvről szóló 1978. évi IV. tv.-ben.*

⇒ *A pénzintézetekkel kapcsolatos jogszabályok:*
- *a banktitok meghatározása a hitelintézetekről és pénzintézeti vállalkozásokról szóló 1996. CXII. tv.- ben.*
- *Az értékpapír titok meghatározása az értékpapírok forgalomba hozataláról szóló 1996.CXI.tv.-ben.*
- *a biztosítási titok meghatározása az 1995. évi XCVI. tv.-ben.*
- *3/1994.(PK13) BAF rendelkezés, az egyes bankbiztonsági követelmények meghatározásáról.*
- *98/1995.(VII.24.) Korm. rendelet az egyes értékpapírok előállításának, kezelésének és fizikai megsemmisítésének biztonsági szabályairól.*
- *A Pénzügyi Szervezetek Állami Felügyelete elnökének 10/2001. számú ajánlása a pénzügyi szervezetek működésének biztonsági feltételeiről.*
  (http://www.pszaf.hu/2001/102001.htm)

⇒ *A személy és vagyonvédelemmel foglalkozó 2005. évi CXXXIII.tv.*

⇒ *a tűzvédelemmel foglalkozó jogszabályok:*
- *1996. évi XXXI tv. A tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról.*
- *4/1980. (XI. 25.) BM rendelettel hatályba lépett Országos Tűzvédelmi Szabályzat.*

14.3.9. Keresztösszefüggések

A védelmi intézkedések, a követelmények, és a veszélyforrások keresztösszefüggését a következő táblázatban kell szerepeltetni:

VÉDELMI INTÉZKEDÉS		*VÉSZÉLYFORRÁS*		*KÖVETELMÉNY*	
Jele	*Megnevezése*	*Jele*	*Megnevezése*	*Jele*	*Megnevezése*

14.3.10. A Megbízó szerepe

A Megbízó szerepe a Biztonsági Politika készítésénél a következő:

⇒ *a Biztonsági Politika Vezérigazgatói utasítás formájában kerül kiadásra, tehát a végső változatnak utasítás, és nem ajánlás jellegűnek kell lennie,*
⇒ *a Megbízónak a Biztonságpolitikai koncepciót el kell fogadnia, amely a követelmények és a védelmi intézkedések specifikációjának az alapja,*
⇒ *a védelmi intézkedések végső változata nem tartalmazhat alternatívákat, a Biztonsági Politika készítése során a Megbízónak döntenie kell.*

14.3.11. A kritikus pontok

A Biztonsági Politika készítésének kritikus pontjai az alábbiak.

⇒ *„A biztonság a tudatosan felvállalt kockázatokon keresztül valósul meg" elvet érvényesíteni kell. Ez annyit jelent, hogy kerülhet a szakértők által javasoltnál gyengébb védelmi intézkedés meghatározásra, azonban ezt a tényt külön írásban rögzíteni kell. A Biztonsági Politika a Megbízó szándékait, tudatos kockázat vállalásait kell, hogy tartalmazza, azonban a későbbi esetleges számonkérés lehetősége miatt rögzítendő a szakértő eltérő véleménye.*
⇒ *A védelmi intézkedéseket úgy kell specifikálni, hogy az egyes védelmi technikák annak alapján megrendelhetők legyenek.*

14.3.12. Akcióterv

E pontban az egyes védelmi intézkedések végrehajtásával kapcsolatos feladatokat, határidőket és felelősöket (a munkaköröket, nem a személyek nevét) kell megadni.