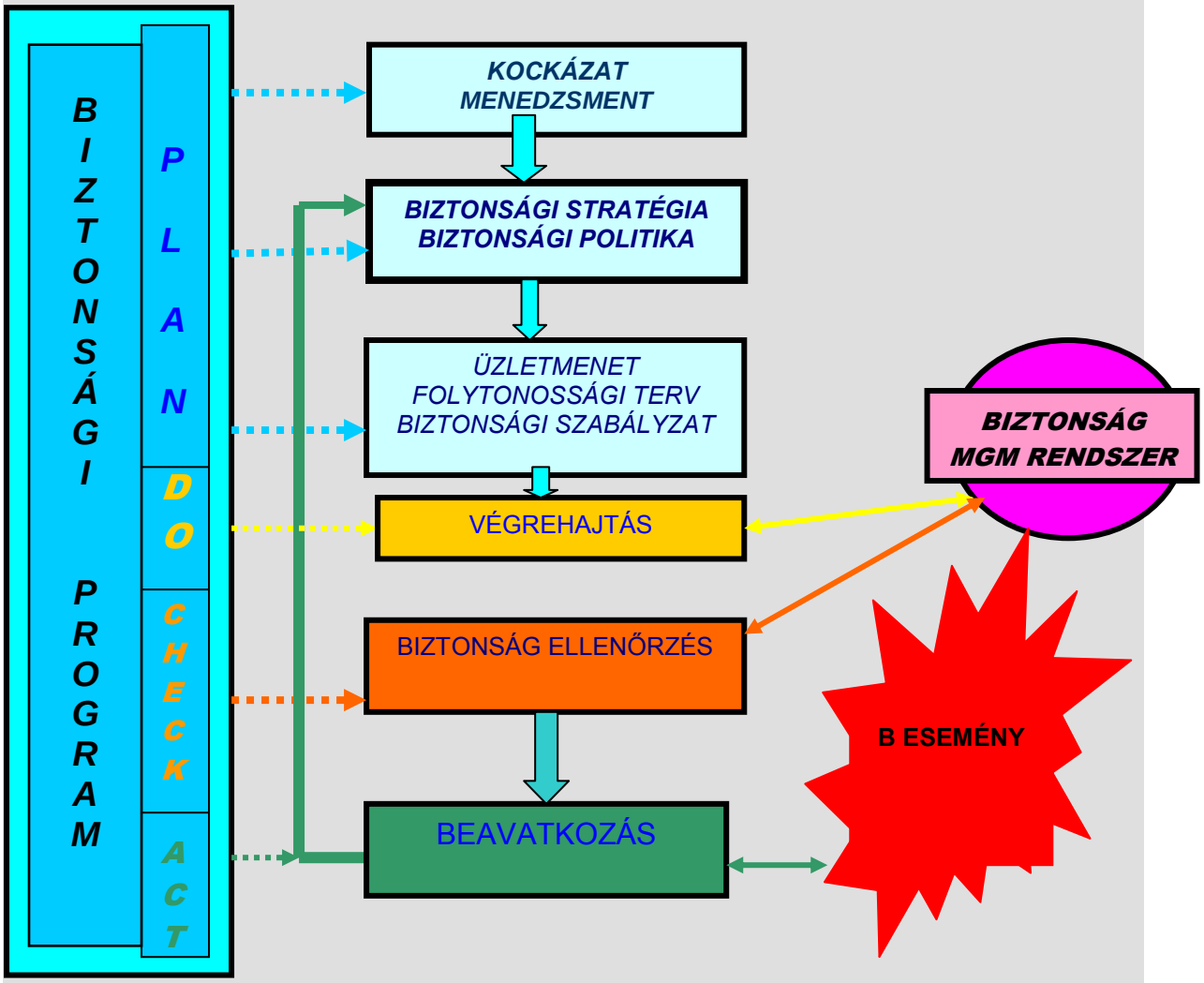
VASVÁRI GYÖRGY CISM

BIZTONSÁGSZERVEZÉSI MÓDSZERTAN

INFORMATION SECURITY MANAGEMENT SYTEM *ORGANISATION METHODOLOGY*

ISMS *II. kötet*



2011

Szakmai lektor:
Erdősi Péter Máté CISA, elektronikus aláírás szolgáltatás szakértő

Tartalom

1. A BIZTONSÁGI POLITIKA FELÉPÍTÉSE

1.1. A VÉDELMI INTÉZKEDÉSEK SPECIFIKÁLÁSA AZ ÜZLETI REDNSZERBEN

Az üzleti rendszer sajátosságai szerint, figyelembe véve az átfedéseket kell specifikálni. Ez azt jelenti, hogy alapvetően a szervezési, és a fizikai védelmi intézkedések a teljes biztonsági rendszerre érvényesek, míg a logikai védelmi intézkedések az üzleti rendszer sajátosságai szerint alakítandók.

1.2. VÉDELMI INTÉZKEDÉSEK SPECIFIKÁLÁSA AZ INFORMÁCIÓS RENDSZERBEN

1.2.1. Szervezési védelmi intézkedések

1.2.1.1. Szervezet és működés

1.2.1.1.1. Szervezet

1.2.1.1.2. Biztonsági szervezet

1.2.1.1.3. Tűzvédelem

1.2.1.1.4. Polgári védelem

1.2.1.2. Titokvédelem

1.2.1.2.1. Személyes adatok védelme

1.2.1.2.2. Adatok, alkalmazások, értékek védelmi osztályozása

1.2.1.2.3. Eszközök védelmi osztályozása

1.2.1.2.4. Helyiségek védelmi osztályozása

1.2.1.3. Iratkezelés

1.2.1.3.1. Papíralapú iratok

1.2.1.3.2. Elektronikus íratok

1.2.1.4. Humánpolitika

1.2.1.4.1. Munkaviszony létesítés, és megszüntetés

1.2.1.4.2. Feladat meghatározás, szétválasztás, csere

1.2.1.4.3. Szabadság kiadási politika

1.2.1.4.4. Karrier menedzsment

1.2.1.4.5. Teljesítménykövetés

1.2.1.4.6. Biztonsági kultúra, és tudatosság, humán tűzfal

1.2.1.4.7. Oktatás

1.2.1.5. Szerződések

1.2.1.5.1. Kockázat áthárítás

1.2.1.5.2. Szerződés harmadikféllel (outsourcing, SLA, SLM)

1.2.1.5.3. Szolgáltatási szint megállapodás

1.2.2. Technikai védelmi intézkedések

1.2.2.1. Fizikai védelmi intézkedések

1.2.2.1.1. Fizikai hfv

Aktív támadás elleni védelem

- *Épület automatika*
- *Belépés és mozgás ellenőrzés*
- *Behatolás-védelem*
- *Felügyeleti központ*
- *Értéktárolás védelem*
- *Értékszállítás védelem*
- *Üres íróasztal politika*

Passzív támadás elleni védelem

- *Elektromágneses kisugárzás elleni védelem*
- *Akusztikus kisugárzás elleni védelem*
- *Hulladékmegsemmisítés*

1.2.2.1.2. Fizikai rendelkezésre állás védelme

Energia ellátás
Tűzvédelem
Beszéd kommunikáció
Klimatizálás
Megbízhatóság
Dokumentáció

Karbantartást ellátók

1.2.2.2. Logikai védelmi intézkedések

1.2.2.2.1. Logikai hozzáférés-védelem

Aktív támadás elleni hozzáférés-védelem
Passzív támadás elleni hozzáférés-védelem

1.2.2.2.2. Logikai rendelkezésre állás védelme

Vírus védelem
Mentés/újraindítás
Logikai rombolás
Dokumentáció
Rendszerkövetés

1.2.2.3. Hálózatok védelme

1.2.2.3.1. LAN

1.2.2.3.2. WAN

1.2.2.3.3. Nem bizalmas hálózati kapcsolatok

Internet kapcsolat
Szerviz kapcsolat
Felhasználói kapcsolat
Banki kapcsolat

1.2.2.3.4. Beszédhálózat

1.2.2.4. Védelem az IR életciklus során

1.2.2.4.1. Fejlesztés

1.2.2.4.2. Átadás/átvétel

1.2.2.4.3. Üzemeltetés

1.2.2.4.4. Selejtezés

1.3. A SZÁMON KÉRHETŐSÉG

1.3.1. Információk védelmének számon kérhetősége

1.3.2. Eszközök számon kérhetősége

1.4. A BIZTONSÁGI POLITIKA VÉGREHAJTÁSA

1.4.1. Akcióterv

1.4.2. A Biztonsági Politika karbantartása

1.4.3. A Biztonsági Politika oktatása

1.5. KERESZTÖSSZEFÜGGÉSEK

1.6. A BIZTONSÁGI POLITIKA HATÁLYBA LÉPÉSE

2. VÁLASZ MENEDZSMENT (BIZTONSÁGI ESEMÉNYEK KEZELÉSE)

2.1. A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉNEK CÉLJA

Felkészülés a biztonsági esemény bekövetkezésére, és a gyors, hatékony válasz feltételeinek biztosítása.

- A biztonsági esemény minden olyan negatív következményekkel járó esemény, amely a biztonságra nézve fenyegetést jelent, vagy jelenthet, azaz egy olyan esemény, amely negatív hatást fejt ki. Ez az esemény kockázatot képez.
- Ugyanakkor az esemény hatása lehet pozitív is, amikor hozzájárul a szervezet, vállalat célkitűzéseinek teljesüléséhez, ez természetesen nem biztonsági esemény.

2.2. A BIZTONSÁGI ESEMÉNY VÁLTOZATAI

a) amikor a biztonsági esemény a rendszerre részleges fenyegetést jelent, vagy jelenthet.
b) Amikor a biztonsági esemény a teljes rendszer leállásához vezet, vagy vezethet

Az a) esetben a kárkövetkezmények csökkentésére a „Biztonsági Események Kezelésének Programja szolgál.(lásd 3. fejezet). A b) esetben a kárkövetkezmények csökkentésére az ÜFT szolgál.(lásd 4., és 5. fejezet). Célszerű a Biztonsági Események Kezelésének rendjét az ÜFT-vel összekapcsolni, mivel a b)esetben az ÜFT gondoskodik a kárkövetkezmények elhárításáról, de a a számon kérhetőséget ekkor is biztosítani kell.

2.3. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

A biztonsági események kezelésére egy Biztonsági Eseménykezelő Programot kell készíteni, amely az alábbi fázisokból áll:

- A felkészülési fázis
  Amelyben a
  - A Biztonsági Események kezelése eljárás rendje elkészül
  - A tesztelések megtörténnek
  - A karbantartást terv szerint végrehajtják
  - Az oktatást rendszeresen megtartják
  - A tartalék eljárásokat, erőforrásokat (tartalék eszközök, mentett adatok, programok, rendszer beállítások) biztosítják

- Az észlelési fázis
  Amelyben az eseményt észlelik, azonosítják, és az arra jogosult, és kötelezett személy jelenti a koordinátornak (aki általában az ÜFT-ben meghatározott Katasztrófa menedzser).
- Az értékelési fázis
  Amelyben a koordinátor azonosítja az eseményt, meghatározza a hatás szintjét, és dönt a megteendő intézkedésekről. Ezek lehetnek az Eljárási Rend alapján a visszaállítás, vagy az ÜFT indítása. A biztonsági események (részleges kárkövetkezmény) a visszaállítás az eredeti állapot helyreállítását igénylik, a tartalék erőforrások felhasználásával. A felhasználói igényeket a help desk kezeli figyelemmel az SLA követelményekre, és ezeket a visszaállítási team használja fel.
- A visszaállítási fázis
  Amelyben a koordinátor intézkedései nyomán a Visszaállítási team (ugyan az mint az ÜFT-ben) visszaállítja az eredeti állapotot.
- Az intézkedési fázis
  Amelyben az
  Értékelés alapján a koordinátor dönt arról, hogy szükséges-e a visszaállításon kívül egyéb intézkedést tenni (pl. a védelmi intézkedést korszerűsíteni, lecserélni).
- Számonkérési fázis
  Amelyben a koordinátor
  - Gondoskodik a bizonyítékok összegyűjtéséről, és megőrzéséről
  - Meghatározza az esetleges felelősöket
  - Dönt belső ellenőrzési vizsgálat, vagy belső, illetve külső jogi eljárás kezdeményezéséről.

2.4. A KOORDINÁTOR SZEREPE

A koordinátor (általában az ÜFT katasztrófa menedzser) felelős a biztonsági események kezelésének menedzseléséért, és e tevékenységét a Vezérigazgató képviseletében látja el.

2.5. PROBLÉMAKEZELÉS

A probléma gyakorlatilag az események egyik változata, nem biztonsági esemény, de a kezelését a biztonsági eseményekhez hasonlóan kell megoldani. Az irányítója a help desk, amely igénybe veszi a megfelelő szakértőket (HW, SW, NW, Szervezés).

A problémákat osztályozni kell (üzleti hatás, sürgősség alapján), és biztosítani kell a nyomkövetést.

A probléma, változás, és konfiguráció menedzsmentet össze kell hangolni.

3. A BIZTONSÁGI ESEMÉNYEK, ÉS PROBLÉMÁK KEZELÉSÉNEK PROGRAMJA

3.1. A PROGRAM CÉLJA

3.2. A BIZTONSÁGI ESEMÉNY, ÉS A PROBLÉMA FOGALMA

3.3. TEENDŐK A PROGRAM EGYES FÁZISAIBAN

- FELKÉSZÜLÉSI FÁZIS
- ÉSZLELÉSI FÁZIS
- ÉRTÉKELÉSI FÁZIS
- VISSZAÁLLÍTÁSI FÁZIS
- INTÉZKEDÉSI FÁZIS
- SZÁMONKÉRÉSI FÁZIS

3.4. A KOORDINÁTOR

- MUNKA, FELADAT KÖRE
- ELÉRHETŐSÉGE (MUNKAHELYEN, OTTHON, MÁSUTT)

4. A MŰKÖDÉSFOLYTONOSSÁG MENEDZSMENT

4.1. A MŰKÖDÉSFOLYTONOSSÁG TERVEZÉS CÉLJA

A működésfolytonosság tervezés célja, a vállalati (szervezeti) színtű folyamatos és rendeltetésszerű üzleti tevékenység biztosítási feltételeinek kidolgozása, felkészülés a katasztrófa bekövetkezése esetén a kárkövetkezmények csökkentésre, gyors elhárítására. Az ÜFT elkészítése elemi fontosságú a vállalat számára (nem beszélve arról, hogy a szabványok is előírják), mert soha nem lehet tudni, hogy ÉS HA MÉGIS A KATASZTRÓFA (működésfolytonosság megszakadása) BEKÖVETKEZIK. Ezt a feladatot, ma már vállalati biztonság szintjén kell megoldani. Ami annyit jelent, hogy az ÜFT készítése a következő részekből áll:

1. Üzleti rendszer működésfolytonosság tervezése
   Az Üzletmenet Folytonossági Tervben (BCP, ÜFT) az üzleti rendszer katasztrófaterv készítése rendszer, és ezen belül folyamat orientált megközelítést igényel. A működés folytonosság megszakadását úgy értelmezzük, hogy azok az üzleti erőforrások sérülnek, amelyek az üzleti folyamatok működésének „környezeti, infrastrukturális" feltételeit biztosítják, azaz a folyamatok a működésének előfeltételei.
2. Az üzleti, és támogató folyamatok működésfolytonosságának a tervezése (az üzleti folyamatok, és a támogató folyamatok az üzleti rendszerben mennek végbe).
   Az üzleti, és támogató folyamatok folytonossági tervezése folyamat orientált megközelítésű, és ez azt jelenti, hogy arra ad választ, hogy mit kell tenni, ha egy üzleti folyamat kiesik. Tehát egyenként kell foglalkozni az üzleti folyamatokkal, legalább a küldetés kritikus folyamatokkal.
   Az üzleti folyamatok: a vállalat alaptevékenységet valósítják meg.
   - A folyamat tevékenységek összefüggő sorozata.

   A támogató folyamatok: a vállalatirányítás, menedzsment, fejlesztés, marketing, pénzügy, számvitel, kontrolling, humán erőforrás menedzsment, jogi, minőségbiztosítási, logisztikai, ellenőrzési folyamatok, amelyek támogatásával tudnak az üzleti folyamatok végbe menni.
3. Az információs rendszer működésfolytonosságának biztosítása rendszer, és azon belül folyamat (alkalmazás) orientált megközelítést igényel. Azaz a működés folytonosság zavarait, megszakadását, úgy értelmezzük, hogy erőforrások sérülnek, amelyek folyamatok (alkalmazások) működés folytonosságában idéznek, elő zavarokat vagy szakítják meg. Az informatikai működésfolytonosság tervezése.
   Az információs rendszer működésfolytonosságának biztosításánál abból kell kiindulni, hogy az üzleti folyamatok jelentős részét, az informatikai alkalmazások kiszolgálják, azaz az üzleti folyamatban működési zavarok léphetnek fel, amennyiben az információs rendszer részben vagy egészben működés képtelen.
4. A 3.-ból következik, hogy *a Tervben meg kell határozni, küldetés kritikus folyamatonként azokat a 2. és 3. szerint tervezett eljárásokat, eszközöket (erőforrásokat), amelyek az egyes üzleti folyamatok (támogató folyamatok) működésfolytonosságának biztosításához fel lehet, kell használni a folyamatok*

(alkalmazások) működés folytonossági problémáinak áthidalásához (visszaállítás), illetve, végleges megoldásához (helyreállításához.).

4.2. A TERVEZÉS KIINDULÓ FELTÉTELEI

⇒ *Amennyiben a Megbízó nem rendelkezik Biztonsági politikával ezt az anyagban fel kell tüntetni, és rá kell mutatni a keresztösszefüggésre.*

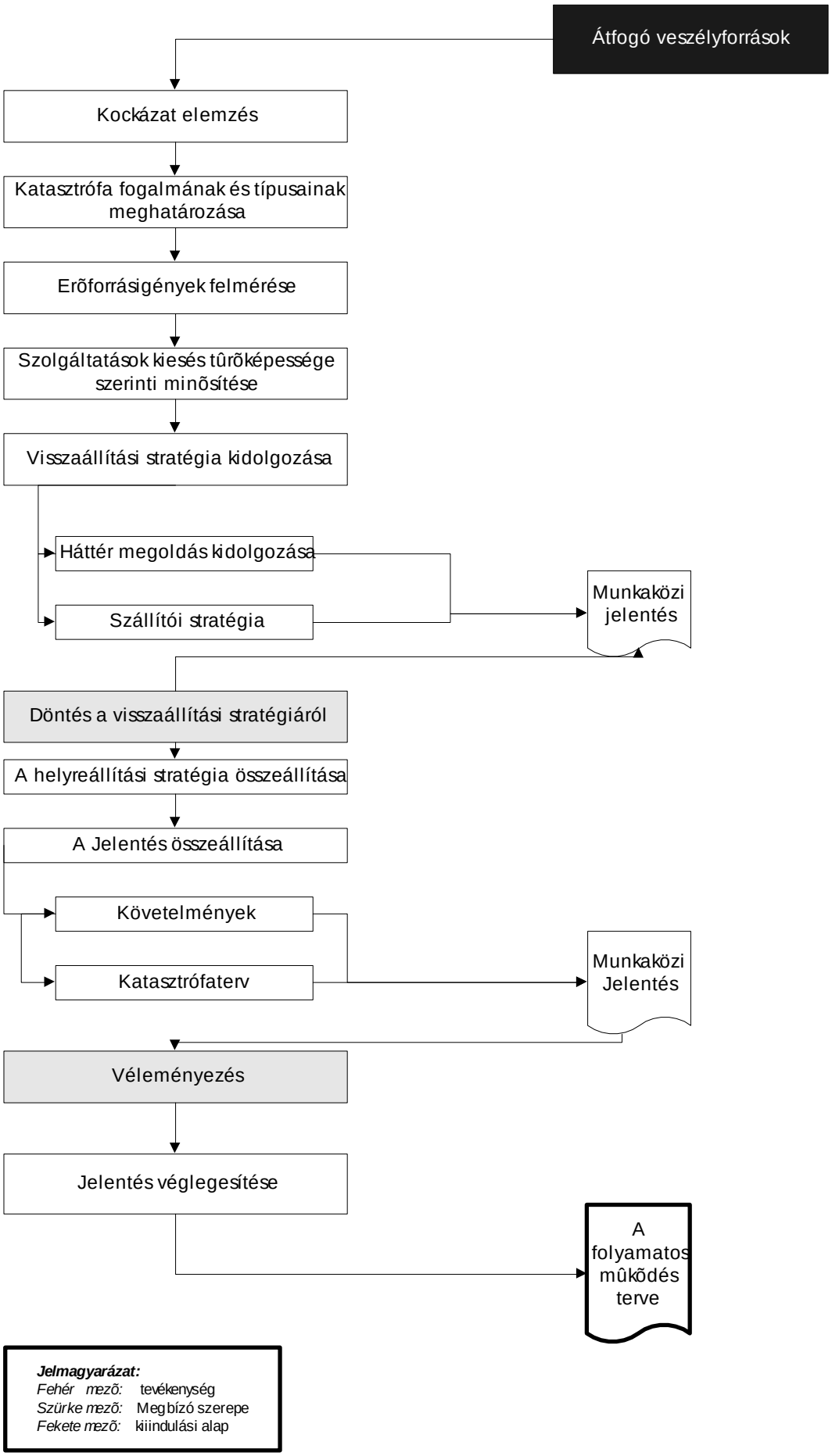
⇒ *A valóságban a vészhelyzet az üzleti tevékenység (üzleti rendszer = ÜR), és az információs rendszer (IR) között szoros kölcsön hatásban van.*

4.3. A TERVEZÉS ALAPJA

A tervezés alapja a veszélyforrás elemzés során a teljes rendszer működését fenyegető, (feltárt), ***átfogó technikai veszélyforrások****.*

4.4. AZ ANYAG KIDOLGOZÁSA

A tervezés folyamatábrája a következő oldalon található.


Átfogó veszélyforrások
Kockázat elemzés
Katasztrófa fogalmának és típusainak meghatározása
Erõforrásigények felmérése
Szolgáltatások kiesés tûrõképessége szerinti minõsítése
Visszaállítási stratégia kidolgozása
Háttér megoldás kidolgozása
Szállítói stratégia
Munkaközi jelentés
Döntés a visszaállítási stratégiáról
A helyreállítási stratégia összeállítása
A Jelentés összeállítása
Követelmények
Katasztrófaterv
Munkaközi Jelentés
Véleményezés
Jelentés véglegesítése
A folyamatos mûködés terve
Jelmagyarázat:
Fehér mezõ: tevékenység
Szürke mezõ: Megbízó szerepe
Fekete mezõ: kiindulási alap

4.5. AZ ÜZLETI HATÁS I. KOCKÁZAT ELEMZÉS

Először a veszélyforrásokat kell elemezni, majd a veszélyforrások kockázat elemzését kell elkészíteni. Az átfogó, a folyamatos működést, és az elérhetőséget, azaz a rendelkezésre állást fenyegető veszélyforrások általában a következők:

4.5.1. Szervezési veszélyforrások

4.5.1.1. Szervezeti

+ Az egységes, központilag irányított biztonsági szervezet hiánya.

4.5.1.2. Humán

+ A biztonsági tudatosság hiánya, nem megfelelő humán tűzfal.
+ A tömegdemonstráció következményei elleni védelem gyengeségei.
+ A sztrájk következményeire történő felkészülés hiánya.
+ A bombariadó megelőzése, és következményei elleni védelem hiánya.

4.5.1.3. Szabályozások hiányosságai

+ Adat-, és titokvédelmi utasítás hiánya, vagy gyengeségei
+ Az üzleti, és támogató folyamatok szabályozásának hiánya vagy gyengeségei

4.5.1.4. Szerződések

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

4.5.2. Fizikai veszélyforrások

4.5.2.1. Fizikai hozzáférés-védelmi

+ A fizikai vandalizmus elleni védekezés gyengeségei.

4.5.2.2. Fizikai rendelkezésre állási

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

4.5.3. Logikai veszélyforrások

4.5.3.1. Logikai hozzáférés-védelmi

+ A számítógépes vandalizmus elleni védelem hiánya vagy gyengesége.

4.5.3.2. Logikai rendelkezésre állási

+ Rendszerszoftver rendelkezésre állásának gyengeségei.
+ Alkalmazói szoftver rendelkezésre állásának gyengeségei.
+ Vírusfertőzés.
+ Elektromágneses rombolás.

4.5.4. Életciklus kockázat

A erőforrások életciklusának nem megfelelő követése átfogó kockázat. Amikor például a küldetés kritikus alkalmazásokat, működőképességük határát figyelembe nem véve pénzügyi, vagy bármely okokra hivatkozva, azokat tovább üzemeltetik.

4.5.5. A visszaállítási kockázat

Külön rá kell mutatnunk a visszaállításnál fellépő kockázatokra. E kockázatok meghatározásánál abból kell kiindulni, hogy a fenyegetés az, ha a meghatározott sebezhetőségi ablakon belül a visszaállítás nem történik meg.

4.5.6. A főbb üzleti kockázatok

+ Pénzügyi kockázat,
+ Piaci
+ Hírnév kockázat,
+ Működési kockázat
+ Jogi kockázat
+ Rendszeres kockázat, amelyet egy partner hibája (kötelezettségeinek nem teljesítése, okozhat, pl. bank rendszerben, a pénzforgalmat bonyolítóknál, és más pénzpiaci résztvevőknél).

4.5.7. A kockázat elemzés végrehajtása

A kockázatelemzést a pont szerint, veszélyforrásonként kell elvégezni, célszerűen annak a szakértőnek, aki a veszélyforrást megállapította.

Egy veszélyforrás kockázat elemzése következőket tartalmazza:

⇒ Veszélyforrás kódja és neve:
⇒ Fenyegetettség: minősítés (C, I , A)
⇒ A bekövetkezési valószínűség: minősítés (VS,S,M,L)
⇒ A sebezhetőség: minősítés (G,R esetünkben G)
⇒ A kockázat: minősítés (VS,S,M,L,XL)

4.6. AZ ÜZLETI HATÁS II. A KATASZTRÓFA FOGALMA

A katasztrófa fogalma általában a működésfolytonosság megszakadása.

4.6.1. Az IT folytonosság megszakadás osztályozása

Az IT erőforrások rendelkezésre állásának megszakadását az alábbiak szerint osztályozhatjuk:

⇒ *I. Kategória. Az erőforrások általánosan nem állnak rendelkezésre, az üzleti tevékenység megszakad. (pl. tűz, bombariadó, vírusfertőzés, túszejtés következtében).*

⇒ *II. Kategória. Egyes erőforrások nem állnak rendelkezésre, az üzleti tevékenység megszakad (pl. az energiaellátás teljes kiesése).*

⇒ III. Kategória. Egy erőforrás elem kiesik, a működésfolytonosság nem szakad meg.

Az I. és a II. kategóriák képezik a katasztrófák osztályait, ide tartoznak az átfogó kárkövetkezménnyel járó biztonsági események. Míg a III. kategória részleges kárkövetkezménnyel járó biztonsági események, amelyek részleges védelmi intézkedéseket igényelnek, ezért azzal a Biztonsági politika fogalakozik.

4.6.2. Üzleti rendszer működésfolytonossága megszakadásának osztályozása (ÜR)

⇒ I. Kategória. A küldetéskritikus üzleti folyamatok végrehajtását kiszolgáló objektum teljes kiesése (pl. tűz).
⇒ II. Kategória. A küldetéskritikus üzleti folyamatok végrehajtását szolgáló infrastruktúra kiesése egyes erőforrások kiesése következtében (pl. energia ellátás vagy bombariadó).

4.6.3. Üzleti, és támogató folyamatok megszakadásának osztályozása

Az üzleti, és támogató folyamat szintű katasztrófa, amikor az informatikai alkalmazás (szolgáltatás), vagy az üzleti rendszer egyéb erőforrásainak kiesése miatt az üzleti folyamat, az üzleti tevékenység megszakad. Az üzleti folyamatok az Üzleti rendszerben mennek végbe, és azokat kiszolgálhatják az IR-ben megvalósuló informatikai alkalmazások (folyamatok is).
Az üzleti, és támogató folyamat katasztrófa helyzete akkor következhet be, ha
❶ az információ, és/vagy üzleti rendszer visszaállítási ideje hosszabb, mint az üzleti folyamat sebezhetőségi ablaka, és
❷az információ, és/vagy üzleti rendszer katasztrófája miatt az üzleti folyamat kiesik, így az üzleti tevékenység megszakad és a visszaállítási stratégia (az informatikai

és/vagy üzleti rendszer katasztrófatervében) olyan háttért választ, hogy egy felhasználó vagy felhasználói csoport nem viseli el az ebben az esetben a visszaállításig tartó üzleti folyamat kiesést.

Természetesen, például amennyiben az informatikai katasztrófaterv háttérként egy távoli aktív redundans, katasztrófatűrő rendszert határoz meg, az üzleti folyamatok katasztrófatervének készítésénél figyelembe kell venni, hogy az informatika kiesése nem valószínű.

4.6.4. A küldetéskritikus folyamatok

A küldetéskritikus folyamatok azok, amelyek kiesése következtében a folyamatos üzleti tevékenysége megszakad. A küldetéskritikus folyamatokat meg kell határozni, az alábbiak között

- az ÜR: üzleti folyamatok, és
- IR: informatikai alkalmazások, amelyek kiszolgálják a küldetés kritikus folyamatokat.

A küldetéskritikus folyamatok a sebezhetőségi ablakok segítségével állapíthatók meg.

A többszintű rendszereknél vizsgálni kell az egyes szintek alkalmazásainak egymástól való függőségét, mivel nem zárható ki egy csak a központra vagy csak egy közép szintre vagy csak egy alsó szintre vonatkozó katasztrófa helyzet bekövetkezése. Ilyenkor az egyéb szintek alkalmazásai is kieshetnek, így a katasztrófa kiterjedhet. Például egy erősen a központi rendszerre épített információ-rendszerben a központ kiesése ellehetetlenítheti az alsóbb szinteket is.

4.6.5. Az erőforrás igények meghatározása

A katasztrófatervezés célja szerint az üzleti tevékenység folyamatosságának biztosítása a feladat (az erőforrás igények meghatározása az üzlet kritikusság szerint), amelyhez először az erőforrás igényeket kell felmérni, mivel ezek ismerete nélkül nem lehet tudni, mit kell visszaállítani, illetve helyreállítani.

4.6.5.1. Az üzleti rendszer (ÜR) erőforrás igényei

Az üzleti rendszer hátterének, az üzleti folyamatok, és az azokat támogató folyamatok folyamatos végrehajtásának feltételeit kell biztosítania. A katasztrófa lehet például a központi épület megsemmisülése, vagy közép, illetve alsó szintű szervezeti egységek (pl. igazgatóság) objektumainak megsemmisülése. Az ÜR erőforrásai között az objektumon kívül, az adatok, dokumentációk, bizonylatok, a logisztikai eszközök, és berendezések, az ügyvitel technikai eszközök, és berendezések, valamint az intelligens épület (épületautomatika, épület biztonsági rendszer stb.), az infrastruktúra is szerepelnek. Az üzleti rendszer erőforrás igényeket (1/ÉR.sz. kérdőív), és a felhasználók szolgáltatás kiesés tűrőképességét (2.sz.kérdőív) kell felmérni.

4.6.5.2. Az üzleti, és támogató folyamatok erőforrás igénye

Az üzleti, és támogató folyamatok erőforrás igényét folyamatonként kell meghatározni.(lásd 1/ÉR kérdőív).

4.6.5.3. Az információ-rendszer (IR) erőforrás igényei

Az információ-rendszerben az alkalmazások folyamatos és rendeltetésszerű működését kell biztosítani. A tervezéshez tehát az alkalmazások erőforrás igényére, valamint a felhasználók nyilatkozatára van szükség az üzleti tevékenységük informatika függőségéről. Ezek elkészítése kérdőívek segítségével történik. A két kérdőív:

- ⇒ az alkalmazások erőforrás igénye (1/IR.sz. kérdőív), amelyet alkalmazásonként kell kitölteni és
- ⇒ a számítástechnikai szolgáltatás kiesés hatásbecslése (2.sz,kérdőív).

1/ÉR.sz.kérdőív

Az Üzleti rendszer folyamatainak erőforrás igénye

1. Az objektum megnevezése:
2. Az objektum címe:
3. Az irodai alapterület:
4. Az objektumban működő küldetéskritikus üzleti, és támogató folyamatok:
5. A folyamatok helyigényei:
6. A folyamatokat ellátó humán erőforrások:
7. Az egyes folyamatok folyamatosságának biztosításhoz szükséges adatok:
8. Az egyes folyamatok eszköz igénye
9. Az egyes folyamatok számítástechnikai szolgáltatás igénye
10. Az egyes folyamatok ügyvitel technikai eszköz igénye (távbeszélő kpt, készülék, fax, sokszorosító gép)
11. Az egyes folyamatok logisztikai igényei (pl. szgk, teher gk, raktár):
12. Az objektumban alkalmazott épület automatika (pl. klíma, felvonó, épület biztonsági rendszer) :
13. Az egyes folyamatok folyamatosságának fenntartásához szükséges dokumentum igények (folyamat leírások, szabályzatok, bizonylatok, nyomtatványok, szerződések stb.):

Dátum

Kiállító aláírása

1/ IR.sz. kérdőív

Az informatikai alkalmazások erőforrás igénye

1. Informatikai alrendszer neve:

2. Az alrendszer feladata, milyen folyamatot(okat) szolgál ki:

3. A futás idő:

4. Az alkalmazás csúcs ideje:

5. A futtatás munkaerőigénye a kpt.-i rendszerben:
   A hw igény:
   Core system:
   A hálózat típusa:
   Hálózati elemek:

6. Felhasználói terminálok típusa: mennyisége:

7. Rendszer sw igény:

8. Alkalmazói sw igény:

9. Input adatok:

10. Sw.-ek háttértárolási igénye:

11. Input adatok háttér tárolási igénye:

12. Nyomtatvány igény:
    A nyomtatvány neve:
    Formátuma:

13. Szállítók adatai:

14. Az alkalmazás irodatechnika igénye:

15. Dokumentációk:

Dátum

Kiállító aláírása

2.sz.kérdőív

Az ÜR folyamatok, IR alkalmazások kiesésének hatásbecslése (folyamatonként készítendő)

1. A felhasználó szervezeti egység neve:

2. A felhasználó szervezeti egység címe:

3. A felhasznált szolgáltatás megnevezése:

4. A felhasználó által elviselhető kiesési idő:

   A 0-1 órás kiesés:

   - ☐ nem hidalható át
   - ☐ nagy költséggel hidalható át
   - ☐ nem jelentős

   A 1-8 órás kiesés:

   - ☐ nem hidalható át
   - ☐ nagy költséggel hidalható át
   - ☐ nem jelentős

   A8-24 órás kiesés:

   - ☐ nem hidalható át
   - ☐ nagy költséggel hidalható át
   - ☐ nem jelentős

5. Van-e olyan időszak, amikor a folyamat, alkalmazás kiesése különösen káros:

   - ☐ Igen, mikor:
   - ☐ nem (a felhasználás nem naptár érzékeny)

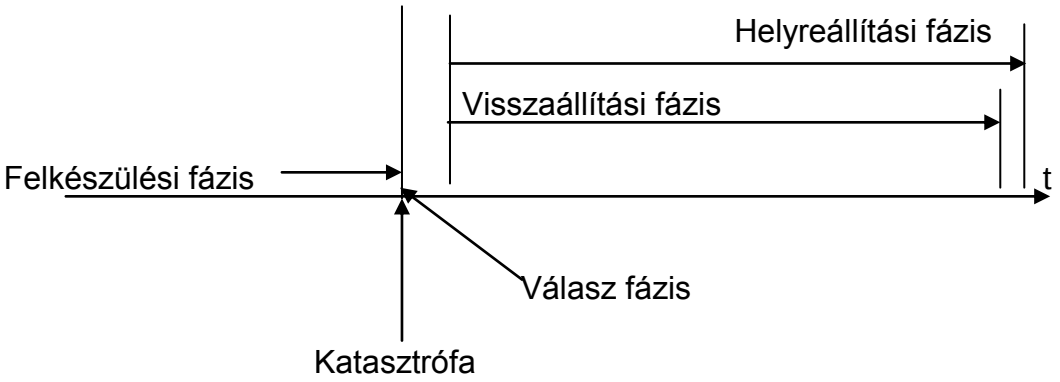
Dátum

aláírás

4.7. A MEGSZAKADÁS ELHÁRÍTÁS FOLYAMATA

Az elhárítás folyamata a következő fázisokból áll:

⇒ ***Felkészülési fázis***, amelyben a működésfolytonosság megszakadásának bekövetkezése előtti feladatokat kell megoldani (a terv oktatása, és karbantartása, a rendszerszervezés, a tesztelés).
⇒ ***Válasz fázis***, amelyben a megszakadás bekövetkezését követő legrövidebb időn belül meg kell kezdeni a katasztrófa kihirdetését, a kárkövetkezmények csökkentését, és a visszaállítás megkezdését.
⇒ ***Visszaállítási fázis***, amelyben a szolgáltatásokat a háttér felhasználásával ideiglenesen újra kell indítani.
⇒ ***Helyreállítási fázis***, amelyben a szolgáltatásokat az eredeti helyen kell újraindítani, és a hátteret le kell állítani.



4.7.1. A Katasztrófa Kezelő Központ

A Katasztrófa Kezelő Központ (KKK) célja a munkahely, a munkafeltételek biztosítása a katasztrófa menedzsment számára,
⇒ A katasztrófa tervezéshez, és
⇒ A katasztrófaterv végrehajtásához.
A KKK szervezete megegyezik a katasztrófa team szervezetével. A katasztrófa menedzser (team vezető) fő állásban végzi a feladatot, és egy adminisztratív alkalmazott segíti a munkáját. A vezető a Vezérigazgató alárendeltségébe tartozik közvetlenül. A visszaállítási, és a helyreállítási teamek eligazítás, oktatás célzattal megjelenhetnek a helyiségekben.
A munkafeltételek:
⇒ A team tagok számának megfelelő munkahelyek száma.
⇒ Egy 15-30 fős tárgyaló, illetve oktató terem.
⇒ Az egyes munkahelyeken alternatív távközlési lehetőségek
⇒ A munkahelyeken a vállalat IR-re kapcsolt munkahelyek, mobil pc-k.
⇒ Irodagépek adatok rögzítésére, másolására, és továbbítására.
⇒ Oktatási segédeszközök
⇒ Tűzbiztos lemezszekrények a Katasztrófaterv, és mellékletei számára.
Pénzügyi keret a költségek fedezésre.

A KKK elhelyezése a vállalat központi szervei épületében kell történjen.

4.7.2. A teamek szervezése

4.7.2.1. A teamek szervezete, és működése

⇒ *Funkció*. A teamek feladatai:
- Felkészülési team, amelynek feladata a katasztrófa bekövetkezése előtt a szükséges, tervezett védelmi intézkedések tervezése, karbantartása, oktatása.
- Katasztrófa team, amelynek feladata a katasztrófa elhárítás egyes fázisaiban a teamek irányítása. A válasz fázisban a katasztrófa kihirdetése, a kárkövetkezmények csökkentése, a visszaállítási team, majd a helyreállítási team munkába állítása, és irányítása
- Visszaállítási team, amelynek feladata a katasztrófa helyzet kihirdetése után az háttér eljárások, központok eszközök felhasználásával az üzleti tevékenység újraindítása.
- Helyreállítási team, amelynek feladata eredeti üzleti tevékenységnek az eredeti helyen történő helyreállítása.

⇒ *Szervezet.* A teamnek egy vezetője, tagjai, és egy adminisztrátor a szervezete. A tagok feladatukat a normál munkakörük mellett látják el. A Felkészülési fázisban a team vezető megítélése szerinti munkarendben dolgoznak, katasztrófa esetén a team munka képezi főfeladatukat (A Katasztrófaterv Vezérigazgatói utasítás kell legyen!!!).

⇒ *Kapcsolatok.* A gazdasági szervezet Katasztrófa teamje a Vezérigazgató alárendeltségében dolgozik, egyedül jogosult a menedzsment, és a külső kapcsolatok (pl. Minisztérium, sajtó) tájékoztatást adni. A szakmai katasztrófa teamek, felhasználva az irányításuk alatt működő szakmai Visszaállítási, és Helyreállítási teameket, a gazdasági szervezet Katasztrófa teamjének vannak alárendelve.

⇒ *Erőforrás igények.* A felkészülési fázisban meg kell tervezni a team munkájához szükséges eszközöket. Ez azt is jelenti, hogy a visszaállításhoz szükséges háttér költségeit először becsült, majd árajánlat alapján konkrét értékkel kell szerepeltetni. A Helyreállításnál mivel a kárkövetkezményeket nem lehet előre megmondani, becsült értéket kell szerepeltetni.

4.7.2.2. A teamek tagjai

A gazdasági szervezet Katasztrófa teamjének tagjai a következők:

⇒ A Katasztrófa menedzsmentért felelős vezető, a team vezetője
⇒ A szakterületek (ÉR, IR) menedzsmentjének képviselője
⇒ A gazdasági szervezet biztonsági vezetője
⇒ Humánpolitikai vezetés képviselője
⇒ A pénzügyi menedzsment képviselője

A szakterületi teamek tagjai a következők:

⇒ A teamek vezetésére célszerű egy katasztrófa menedzsert beállítani, a Biztonsági vezető alárendeltségében.

⇒ A felkészülési team azokat a munkatársakat tartalmazza, akikkel a tervben meghatározott felkészülési feladatokat végre kívánjuk hajtani. Ezt, a vállalatok különbözősége miatt mindig az adott feladatok függvényében kell meghatározni.

⇒ Válasz teamet nem szervezünk, az üzletmenet folytonossági tervnek azonban meg kell határozni, hogy ki a felelős, és jogosult a katasztrófa helyzet megállapításáért, és ennek a személynek kell a további teameket riasztani.

⇒ Katasztrófa team:
- A szakterület vezetésének képviselője, a team vezetője
- Biztonsági vezető,
- Szakmai munkatársak
- Gazdasági vezető
- Adminisztratív vezető
- Humánpolitikai vezető

⇒ Visszaállítási teamek:
- **Informatikai.**
  - Üzemeltetési vezető, a team vezetője
  - IT biztonsági felelős
  - Hw szakértő
  - Rendszerszoftver szakértő
  - Alkalmazói rendszerek szakértő
  - Hálózati szakértő
  - Kiegészítő berendezések szakértő
  - Az informatikai eszközök anyagellátásért felelős vezető
- **Üzleti**
  - Egy adminisztratív (az infrastruktúráért felelős) vezető, a team vezetője
  - Vagyonbiztonsági felelős
  - Szakértők

⇒ Helyreállítási teamek
- **Üzleti**
  - Az ingatlan beruházás, fejlesztés képviselője, a team vezetője
  - Épület gondnokság, karbantartás vezetője
  - Biztonsági vezetés egy képviselője
  - Adminisztratív vezetés egy képviselője
  - Pénzügyi vezetés egy képviselője
- **Informatikai**
  - Az informatikai fejlesztés egy vezetője, a team vezetője
  - Hw szakértő
  - Rsw szakértő
  - Alkalmazási rendszer szakértő
  - IT biztonsági felelős
  - Pénzügy képviselője

4.8. A VISSZAÁLLÍTÁSI STRATÉGIA

4.8.1. A visszaállítási stratégia célja

A visszaállítási stratégia célja az ÜR esetében: olyan háttér objektumok (infrastruktúrális megoldások), illetve eljárások (üzleti folyamatok), és az IR esetében: háttér rendszerek (az informatika részére történő) kiválasztása, amelyek lehetővé teszik, akár kompromisszumok árán is (pl. csak a küldetés kritikus folyamatok számára) a működésfolytonosság ideiglenes újraindítását, a helyreállítás befejezéséig. Az erre vonatkozó tervet nevezik Disaster Recovery Plan-nek (DRP), Katasztrófa Visszaállítási Terv is, amely az ÜFT keretein belül készül.

4.8.2. Az üzleti hatás III. A sebezhetőségi ablak

Az üzleti, és támogató folyamat szintű sebezhetőségi ablak az az időtartam, amelyet az üzleti folyamat a szolgáltatások, erőforrások kiesése esetén még elvisel, azaz a minimális szolgáltatás indításához maximálisan rendelkezésre álló időtartam (kiesés tűrő képesség).

+ A sebezhetőségi ablak azt határozza meg, hogy az adott üzleti tevékenység a technikai feltételek hiánya esetén mennyi ideig tartható fenn, folytatható. Ez az az időtartam, ami alatt a visszaállítást, azaz az üzleti tevékenységet a háttér felhasználásával újra kell indítani. Azaz a KÍVÁNT IDŐTARTAM:

A sebezhetőségi ablakok alapján pl. az informatikai alkalmazások minősítése a következő.

- I. kategória. Küldetés kritikus alkalmazások (sebezhetőségi ablak 0-1 óra).
- II. kategória. Lényeges alkalmazások (sebezhetőségi ablak 1-8 óra).
- III. kategória. Szükséges alkalmazások (sebezhetőségi ablak 8-24 óra).
- IV. kategória. Kívánatos alkalmazások (sebezhetőségi ablak > 24 óra).

4.8.3. Az Üzleti rendszer hátterének kiválasztása

Az üzleti rendszer háttere alapvetően egy háttér objektumot, illetve háttér infrastruktúrát jelent, amely lehet:

⇒ Hideg háttér, azaz egy infrastruktúrával ellátott, de be nem rendezett alapterülettel bíró háttér objektum a katasztrófa esetére.

⇒ Meleg háttér, amely az eredeti objektum egyes küldetéskritikus tevékenységeinek elhelyezésére van kialakítva, és berendezve.

⇒ Forró háttér, amely alkalmas az eredeti objektumban folytatott küldetéskritikus tevékenységek folytatására.

4.8.4. Az üzleti folyamatok háttér eljárásának kiválasztása

Az üzleti, és támogató folyamat szintű visszaállítási stratégia annak a biztosítása, hogy a szolgáltatások kiesése esetén, az informatikai és/vagy üzleti rendszer szolgáltatás vissza, illetve helyreállításáig az üzleti tevékenységét folytatni lehessen. Ez a gyakorlatban azt jelenti, hogy

- A sebezhetőségi ablaknak megfelelően kell meghatározni a háttér eljárást, majd
- A visszaállítás módszerét.

A háttér eljárás lehet
- Manuális eljárás
- Fél automatikus eljárás, mint manuális megoldás + számítástechnikai, ügyvitel technikai eszköz (pl. kézi számológép) alkalmazása.
- Számítástechnikai eszköz (off line), és/vagy ügyvitel technikai eszköz alkalmazása.

A visszaállítás módszere lehet
- Gyors intézkedés
- Részleges visszaállítás
- Teljes visszaállítás.

A fenti háttér eljárások alkalmazása esetén, a kiinduló adatok az utolsó mentés adatai (mentés alatt az üzleti rendszerben a papíralapú adathordozók háttér tárolását értjük), ami azt jelenti, hogy a mentés időpontja, és a minimális szolgáltatás indulása közötti időben lehet adatvesztés. Ugyan akkor az informatikai, és/vagy Üzleti rendszer visszaállítás, illetve a helyreállítás megtörténtekor a minimális szolgáltatás adatait be kell táplálni az eredeti informatikai alkalmazásba.
A minimálisan elfogadható szolgáltatáson azt a szolgáltatást értjük, amellyel az üzleti tevékenység (üzleti, és támogató folyamat) az eredeti informatikai, illetve üzleti rendszerszolgáltatások vissza, illetve helyreállításig az üzleti folyamat szintjén folytatható.

4.8.5. Az informatika hátterének kiválasztása

A rendelkezésre állás *növelésére szolgáló háttér megoldások két alapvető változata ismert, éspedig*

⇒ *az adatok rendelkezésre állását biztosító, részleges védelmi intézkedés, és*

⇒ *a rendszerrendelkezésre állást biztosító átfogó védelmi intézkedés.*

Az adatok rendelkezésre állásának biztosításához a diszk tükrözés elvét alkalmazzák. Ennek egyik igen elterjedt változata a RAID (redundant array of independent disks, független diszkek redundáns sorozata) technológia. A rendszer lényege, hogy a diszkeket többszörözik, és ugyanazt az adatot szimultán írják/olvassák több diszkre/diszkről. Így egy diszk kiesése esetén nincs adatvesztés, és a rendszer tovább képes folytatni a feldolgozást. Valójában ez a megoldás az adott konfigurációban a diszkek rendelkezésére állását növeli meg. A RAID technológiának több változata létezik ezek RAID 0., 1., 3., 5., 7., 10., 53 változatok. A

diszk tükrözés alkalmazása a rendelkezésre állás részleges sérülése ellen nyújt védelmet.
Emellett a RAID rendszerek alkalmazzák az adatok védelmére az adatok párhuzamos kódolt tárolását. Hiba esetén a meghibásodott adatokat az adatvédelmi meghajtón kódolt formában tárolt adatokból állítja elő a rendszer.
Az átfogó veszélyforrások elleni védelemre a hátterek két változata szolgál :

- ⇒ *a passzív redundans rendszerek, és*
- ⇒ *az aktív redundans rendszerek.*

A passzív redundans rendszereknél a háttér rendszer nem vesz részt az eredeti rendszeren folyamatban lévő feladatban. Az eredeti rendszerben fellépő hiba esetén a passzív hátteret aktiválni kell vagy a hiányzó elemek betöltésével kell módosítani. A háttér rendszerre az átálláshoz szükséges idő figyelemre méltó, így a megszakadás jelentős. A passzív redundans rendszerek változatai:

- ⇒ *off line, és*
- ⇒ *visszaállítás bázisú rendszerek.*

Az Off line változatnál az adatok manuális átvitele, a betáplálás és indítás képez időigényt. A visszaállítás bázisú rendszerek periodikusan átmásolják a fileokat, hiba esetén indítják a hátteret. Ez is időigényes, és az utolsó mentés és a háttér indítása közötti időszak adatai elvesznek. Az alkalmazások, és a felhasználók érzékelik a kiesést. A passzív redundans rendszerek magas rendelkezésre állást biztosítanak.
Az aktív redundans rendszerek minimálisan egy háttér processzort alkalmaznak, amelyen ugyanazon adatokon, ugyan abban az időpontban, ugyanazt a műveletet hajtják végre, mint az eredeti rendszer. Az aktív redundans rendszer lehet

- ⇒ *hibatűrő vagy*
- ⇒ *túlélő hibatűrő rendszer.*

A hibatűrő rendszerek processzor párokon alapulnak. A folyamatos működést automatikusan állítják vissza, a hibát tehát nem áthidalják. Így nincs szükség az alkalmazás(-ok) újraindítására vagy az adatbázis visszaállítására. Továbbá folyamatos integritás ellenőrzést végeznek a mikroprocesszoroknál, a belső buszoknál, és a meghajtóknál. Hiba észlelése esetén a hiba okát elszigetelik, mielőtt a folyamatos működésben kárt okozna. A hibatűrő rendszereknél átállási idő (a másodperc törtrésze) nem érzékelhető, a túlélő hibatűrő rendszereknél az átállási idő minimális (másodperc). Ebből következik azonban, hogy a túlélő hibatűrő rendszerek „csak gyakorlatilag" biztosítják, hogy a hiba fellépés ne legyen érzékelhető. A túlélő hibatűrő rendszerekben a folyamatos működést egy speciális szoftver irányítja, szemben a hibatűrő rendszerekkel, ahol a hw, és a rendszer szoftver is speciális. A túlélő hibatűrő rendszer a speciális szoftveren kívül szokványos, kereskedelemben elérhető hw, és rendszer szoftver elemekből áll, ezért az ára is kedvezőbb. Az aktív redundans rendszerek folyamatos rendelkezésre állást biztosítanak.
Mind a két változat kiépíthető a háttér lokális vagy távoli elhelyezésével. A meleg, illetve forró háttérnek a passzív, és a lokális aktív rendszerek, míg a katasztrófatűrőnek a távoli aktív rendszerek felelnek meg. A lokális aktív rendszerek, az eredeti rendszerrel azonos biztonsági környezet miatt, nem elégítik ki a katasztrófatűrő hátterekkel szembeni biztonsági követelményeket. Például tűz esetén

az eredeti és a háttér konfiguráció egyaránt sérülhet, de az objektum környezetéből adódó kockázatok is azonosak. A lokális aktív redundans hátterek ezért csak részleges védelmet, és nem folyamatos, hanem csak magasabb rendelkezésére állást biztosítanak.
A hiba menedzsment tevékenységeket a passzív, és az aktív háttereknél az alábbi táblázatban mutatjuk be:

Hiba menedzsment	*Passzív háttér tevékenysége*	*Aktív háttér Tevékenysége*
1. A hiba felismerése	*Hibajelenség jelzése*	*Hibajelzés mielőtt bármely adat sérülne*
2. A hiba elszigetelése	*Hiba jelenség elszigetelése*	*A hiba jelenség mellett a rendszer a háttéren folyamatosan fut*
3. A hiba javítása	*A hibajavítás alatt a háttéren a rendszer fut*	*A hibajavítás alatt a háttéren a rendszer fut*
4. Az eredeti funkcionalitás helyreállítása	*A javítás befejezése után, az eredeti funkcionalitás visszaállításához, a rendszert újra kell indítani*	*A rendszer, a hibajavítás befejeztével, fogadja a konfigurációba visszatérő eredeti rendszert, és visszaállítja az eredeti funkcionalitást*

A hátterek típusai:

- ⇒ Hideg háttér, több hetes sebezhetőségi ablak megvalósításához. Ez egy infrastruktúrával ellátott üres gépterem. A szállítókkal kötött szerződésekben kell a soron kívüli szállító készséget biztosítani.
- ⇒ Meleg háttér, a küldetés kritikus alkalmazások hátthereként, a kivitelétől függően egy – néhány órás sebezhetőségi ablak megvalósításához, amely nem automatikusan induló, hanem újraindítást igénylő rendszerrel építhető ki (ez lehet az eredeti konfigurációval megegyező konfiguráció, lokális vagy távoli passzív redundans rendszer, illetve lokális aktív redundans rendszer).
- ⇒ Forró háttér, az összes alkalmazások hátthereként, egy – néhány órás sebezhetőségi ablak megvalósításához, amely nem automatikusan induló, hanem újraindítást igénylő rendszerrel építhető ki (ez lehet az eredeti konfigurációval megegyező konfiguráció, lokális vagy távoli passzív redundans rendszer, illetve lokális aktív redundans rendszer).
- ⇒ Katasztrófatűrő háttér, az eredeti rendszer tűkörképeként, folyamatos működés megvalósításához, amely távoli aktív redundans rendszerrel építhető ki.

Összefoglalva az információs rendszernek a rendelkezésre állása biztosítására a következő, a felsorolás sorrendjében növekvő erősségű, redundans megoldások alkalmazhatók:

⇒ *Nagy megbízhatóságú (MTBF értékű) hw eszközök alkalmazása, és hideg tartalék berendezések biztosítása (ezzel a fizikai rendelkezésére állásnál foglalkozunk),*

⇒ *Magas rendelkezésre állást biztosító rendszer alkalmazása (lokális passzív, illetve lokális aktív redundans rendszer),*

⇒ *Folyamatos rendelkezésre állást biztosító katasztrófa tűrő rendszer alkalmazása (távoli aktív redundans rendszer).*

4.8.6. Az adatvesztés csökkentése

Az adatvesztés csökkentése igen jelentős feladat. Amennyiben az információs rendszerünk hibatűrő, katasztrófatűrő ez a probléma megoldott, illetve a hibatűrő esetben a mentések rendszere adhat megoldást arra az esetre, ha a teljes hibatűrő rendszer kiesik. Amennyiben a háttér küldetéskritikus alkalmazásokra vonatkozik, két feladat jelentkezik:

- A rendszeres adatmentésnél, az utolsó mentés adatainak, és a háttér indításáig nem fogadott adatok bevitelének biztosítása. bevitele a háttérbe,
- A háttéren nem futó alkalmazásoknál, pedig a katasztrófától a helyreállításig a manuális adatbiztosítás, vagy az adatszolgáltatóktól az adatok újra lekérésének biztosítása.

4.9. HELYREÁLLÍTÁSI STRATÉGIA

A helyreállítási stratégia célja, hogy megoldásra kerüljön a katasztrófa kárkövetkezményeinek felszámolása, és az üzletmenet az eredeti helyen, eszközökkel, és módon folytatódjon. Ez természetesen azt is jelenti, hogy a háttér eljárásokat, központot le kell állítani, és az eredeti helyen, a folyamatokat, informatikai alkalmazásokat újra kell indítani. Előfordulhat az, hogy az eredeti erőforrások olyan mértékben sérülnek, hogy nem helyreállíthatók, ekkor az eredeti, az eredetivel megegyező erőforrásokat jelenti. A helyreállítást bármilyen fejlesztéssel nem célszerű összekapcsolni. Tehát a visszaállítás fázis addig tart amíg a helyreállítás be nem fejeződik, az újraindítás az eredeti erőforrásokkal nem történt meg.

Az újraindítást, ha a háttér katasztrófatűrő, a háttér elvégzi, amennyiben a háttér nem katasztrófatűrő el kell végezni. Igen kritikus kérdés az adatvesztés elkerülése. Amennyiben a háttér a küldetéskritikus alkalmazásoknak a visszaállítását biztosítja csak, akkor az alábbiakat nem lehet a háttérről bevinni, hanem a felkészülési fázisban kell kidolgozni, miként lehet egyéb módon (pl. manuális gyűjtéssel) megoldani.

A helyreállítás során biztosítani kell

√ Az adatvesztés elkerülésére a háttérről
- a visszaállításkor a háttérre bevitt rendszeresen mentett adatokat, és
- az utolsó mentés, és a háttér indítása között nem fogadott adatokat, valamint
- a katasztrófát követően a háttéren keletkezett adatok bevitelét.

√ Az információs rendszer, illetve az alkalmazások, az azokat szállító cég Eljárás Rendje szerinti újraindítását, a felkészülési fázisban a küldetéskritikusságuk alapján eldöntött priorítási sorrendben.

- √ Az újraindítás után a rendszert, a felkészülési fázisban előkészített teszt eljárásokkal, teszt adatokkal tesztelni kell. Kiemelten ide tartozik az eredeti rendszerben alkalmazott védelmi intézkedések (hozzáférés) tesztelése.
- √ A helyreállításról jelentés készítését, amely magába foglalja a a helyreállítási stratégiával kapcsolatos felmerült problémákat, javaslatokat a teendő intézkedésekre.
- √ Szükséges víruskatasztrófa (amikor vírus fertőzés következtében megszakad a teljes információs rendszer működése) esetére kidolgozni egy helyreállítási akció tervet.

4.10. SZÁLLÍTÁSI STRATÉGIA

A szállítói stratégiában meg kell határozni, hogy az eredeti berendezés, rendszer szállítójától egy katasztrófa bekövetkezésekor mit várunk el. A szállítói szerződéseknek nem csak azt kell tartalmaznia, hogy miként látja el a szállító a garanciális, illetve szavatossági kötelezettségét, alkatrész szállítási kötelezettségét, hanem egy katasztrófa esetén melyek a kötelezettségei. Ezek a következők lehetnek:

- ⇒ Részvétel szakértővel a visszaállításban, illetve a helyreállításban
- ⇒ Alkatrész, berendezés soron kívüli szállítása
- ⇒ Informatika esetében háttér központ biztosítása

A katasztrófa elhárítása során a szállítói stratégia csak akkor hajtható végre, ha az eredeti helyen tárolt szállítói szerződések egy másod példánya a KKK-ban is tárolva van.

4.11. A TERV OKTATÁSA

A Tervet a munkatársaknak tájékoztatás céljából, a team tagoknak feladataik megismertetése céljából oktatni kell. A felkészülési fázisban meg kell határozni, hogy mely szervezeti szervezi, és mely oktatja a tervet.

4.12. A TERV KARBANTARTÁSA

A gazdasági szervezet Katasztrófa teamje felelős a Katasztrófatervek karbantartásáért. A felkészülési fázisban a tesztek tapasztalatait, valamint az üzleti tevékenység változásait kell követni. Katasztrófa esetén a tapasztalatokat kell feldolgozni, és átvezetni a Katasztrófaterven.

4.13. AZ AKCIÓTERVEK

Az akciótervekben a következőket kell megadni:

- ⇒ Feladat
- ⇒ Felelős
- ⇒ Időpont
- ⇒ Eszköz igény

4.14. KRITIKUS PONTOK

A tervezés kritikus pontjai az alábbiak.

- ⇒ A terv készítésénél a költséghatékonyság nem szakmai engedményeket igényel, hanem kifinomult megoldási módszereket.
- ⇒ Amennyiben a vállalat nem rendelkezik Biztonsági politikával a háttérre vonatkozó vagyon-, és az IT biztonsági intézkedéseknél ezt fel kell tüntetni. Ilyen esetben a meglévő védelmi intézkedéseket kell követelményként a hátterekre megadni.
- ⇒ A Működésfolytonossági Tervet (MFT, BCP) Vezérigazgatói utasításként kell kiadni. Ez különösen az informatikai folytonossági tervnél fontos, mivel a teamek tagjai nemcsak az informatikai szervezetből kerülnek ki.
- ⇒ A Terv tesztelésének a megtervezése alapvető kérdés. A legjobb terv is a környezet változásai miatt működésképtelenné válhat.
- ⇒ A teamek tagjainál nem szabad neveket megadni, csak munkaköröket.
- ⇒ Az 1.sz kérdőívet a szakmai szervezeteknek kell kitöltenie, vagy az egyetértéséről írásban kell nyilatkoznia.
- ⇒ A 2.sz kérdőívet csak a felhasználó szervezeti egység töltheti ki, és a vezetője írhatja alá.

4.15. A MEGBÍZÓ SZEREPE

A Megbízó joga „a kockázat tudatos felvállalásának elve" alapján a háttér megoldást kiválasztani. Ugyanakkor, amennyiben a szakértők véleménye ettől eltér, ezt külön írásban rögzíteni kell. A háttér központ erőforrás igényei nem jelentik annak megtervezését, de követelmény szinten elegendőeknek kell lenniük a tervezéshez.

4.16. A VÉDELMI INTÉZKEDÉSEK ÖSSZEFOGLALÁSA

A katasztrófa, a működésfolytonosság megszakadása kárkövetkezményeinek elhárításra, illetve a felkészülésre teendő védelmi intézkedéseket, a követelmények alapján, össze kell foglalni a következő táblázat szerint:

Azonosító	*Megnevezés*

A védelmi intézkedések a következők lehetnek:

- ⇒ SZERVEZÉSI:
  - ➢ Teamek szervezése,
  - ➢ A Folyamatos működés tervének karbantartása,
  - ➢ A Folyamatos működés tervének oktatása
  - ➢ Szerződések visszaállításra,

- Szerződések helyreállításra,
- Szerződések biztosításra,
- Akciótervek

⇒ TECHNIKAI:

- Hátterek (eljárások, központok, módszerek)
- Újraindítási eljárások
- Szállítási eljárások
- A háttér eszközök karbantartása
- Katasztrófa Kezelő Központ

5. AZ ÜZLETMENET FOLYTONOSSÁGI TERV

5.1. KÖVETELMÉNYEK

5.1.1. A folyamatos működés fenyegetettsége

(mind a három területen, üzleti rendszer, üzleti, és támogató folyamatok, információs rendszer)

5.1.1.1. A veszélyforrások

5.1.1.2. A kockázat elemzés

5.1.1.3. A kockázatok

5.1.1.4. Az üzleti hatások elemzése

5.1.2. A katasztrófa (működésfolytonosság megszakadásnak) a meghatározása

(mind a három területen)

5.1.2.1. A katasztrófa értelmezése

5.1.2.2. A katasztrófa fogalma

5.1.2.3. A katasztrófák osztályozása

5.1.3. Kiinduló feltételek

5.1.3.1. Lokalizált vészhelyzet

5.1.3.2. Kapcsolat a vállalati ÜFT-vel

5.1.3.3. A változó üzleti és informatikai környezet hatásai

5.1.3.4. A biztonsági követelmények biztosítása

5.1.4. Erőforrás igények

5.1.4.1. Az Üzleti rendszer erőforrás igénye

5.1.4.1.1. Adatok

5.1.4.1.2. Elhelyezés

5.1.4.1.3. Logisztikai berendezések

5.1.4.1.4. Ügyvitel technikai eszközök

5.1.4.1.5. Dokumentációk, bizonylatok

5.1.4.1.6. Intelligens épület, infrastruktúra

5.1.4.2. AZ üzleti folyamatok erőforrás igénye

5.1.4.2.1. A háttér eljárás rendszerterve

5.1.4.2.2. Adatok

5.1.4.2.3. Számítástechnikai eszközök, támogató szolgáltatások

5.1.4.2.4. Ügyvitel technikai eszközök

5.1.4.2.5. Dokumentumok

5.1.4.2.6. Munkaerő

5.1.4.2.7. Helyiség, berendezés

5.1.4.2.8. Energia

5.1.4.3. Az informatikai alkalmazások erőforrás igénye

5.1.4.3.1. Humán

5.1.4.3.2. IR technológia (HW, RSW, NW)

5.1.4.3.3. ASW

5.1.4.3.4. Adat

5.1.4.3.5. Dokumentáció

5.1.4.3.6. Energia ellátás

5.1.4.3.7. Kisegítő berendezések

5.1.4.3.8. Nyomtatványok

5.1.4.3.9. Beszéd kommunikáció

5.1.4.3.10. Adatok, és szoftverek háttértárolási igénye

5.1.5. Visszaállítási stratégia

5.1.5.1. Az üzleti rendszer elhelyezése

5.1.5.2. Az üzleti folyamatok osztályozása (a sebezhetőségi ablakok alapján)

5.1.5.2.1. Üzleti folyamatok

5.1.5.2.2. Támogató folyamatok

5.1.5.3. Az informatikai alkalmazások osztályozása

5.1.5.3.1. Alrendszerek sebezhetőségi ablakai

5.1.5.3.2. A minősítések

5.1.5.4. Háttér stratégia (ÜR, IR)

(a várhatóan nagyszámú folyamat ellenére folyamatonként!)

5.1.5.4.1. A lehetséges ÜR háttér alternatívák, a visszaállítás módszere, és erőforrás igénye, teendők a felkészülési fázisban

5.1.5.4.2. Az üzleti, és támogató folyamatok minimális szolgáltatási igénye, a háttér eljárás, a háttér eljárás módszere, és erőforrás igénye, teendők a felkészülési fázisban,

5.1.5.4.3. IR háttér alternatíva, és a visszaállítás módszere, teendők a felkészülési fázisban.

5.1.6. Helyreállítási stratégia

5.1.6.1. A károk felmérése

5.1.6.2. A pénzügyi feltételek biztosítása a helyreállításhoz

5.1.6.3. A helyreállítási munkálatok menedzselése

5.1.6.4. Az eredeti erőforrások újraindítása

5.1.6.5. A visszaállítás alatt keletkezett adatok bevitele az eredeti rendszerekbe

5.1.6.6. A helyreállított rendszer tesztelése

5.1.6.7. A háttér rendszerek, eljárások leállítása

5.1.6.8. Helyreállítási jelentés készítése

5.1.7. Szállítói stratégia

5.1.7.1. IR

5.1.7.1.1. Core system

5.1.7.1.2. Hálózat

5.1.7.2. ÜR

5.1.7.2.1. Elhelyezés

5.1.7.2.2. Logisztika

5.1.7.2.3. Üzleti folyamatok eszközeinek igénye alapján

5.1.7.2.4. Épület automatika

5.2. A KÖVETELMÉNYEK MELLÉKLETEI

5.2.1. Interjú alanyok listája

5.2.2. Felhasznált dokumentumok listája

5.2.3. Kérdőívek

5.3. A MEGSZAKADÁS ELHÁRATÁSI INTÉZKEDÉSEK

5.3.1. Felkészülési fázis akció terve

5.3.1.1. Teamek létrehozása

⇒ Felkészülési team
- Funkció
- Szervezet
- Kapcsolatok
- Erőforrás igény

⇒ A válaszra jogosult, és a válaszért felelős személy (munkakör)

⇒ Katasztrófa team
- Funkció
- Szervezet
- Kapcsolatok
- Erőforrás igény

⇒ Visszaállítási team
- Funkció
- Szervezet
- Kapcsolatok
- Erőforrás igény

⇒ Helyreállítási team
- Funkció
- Szervezet
- Kapcsolatok
- Erőforrás igény

5.3.1.2. Dokumentumok biztosítása

⇒ IR leltárak [hw, rsw, asw, nw (beszéd, és adattávközlési vonalak), kisegítő berendezések]
⇒ ÉR leltárak (elhelyezés, logisztikai eszközök, épületautomatika, ügyviteltechnika, üzleti, és támogató folyamatok)
⇒ Értesítési listák (felső vezetés, team tagok, hatóságok)
⇒ Szállítók listája (hw, sw, nw, kellékek)
⇒ Munkatársak listája, címe, elérhetősége
⇒ Szerződések (szállítási, biztosítási), és a képviselők elérhetősége

5.3.1.3. Kockázat áthárítás (biztosítások)

5.3.1.4. Szállítói kapcsolatok

5.3.1.5. A Katasztrófakezelő Központ kialakítása

- Helyiségek,
- Berendezések,
- Számítástechnikai eszközök (hw, sw, nw, dokumentációk)
- Beszéd távközlési eszközök vonalak,
- Háttér adathordozók tárolása

5.3.1.6. Humán erőforrás igény biztosítása

- Katasztrófakezelő központ,
- Team tagok
- Visszaállítás,
- Üzemeltetés

5.3.1.7. IR technológia biztosítása

- Háttérközpont
- HW
- NW
- RSW
- Hw, rsw dokumentációk
- Felhasználói háttér
- Kisegítő berendezések, eszközök,
- Nyomtatványok, kellékek

5.3.1.8. IR alkalmazások biztosítása

- Alkalmazói sw biztosítása
- Adatok biztosítása
- Alkalmazói rendszerek dokumentációi biztosítása
- Az alkalmazás újra indításának eljárás rendje biztosítása

5.3.1.9. ÜR technológia biztosítása

- Elhelyezés (épület, berendezések, infrastruktúra),
- Dokumentációk
- Logisztikai eszközök, és dokumentációk
- Épület automatikai eszközök, és dokumentációk
- Üzleti folyamatok, és támogató folyamatok minimális szolgáltatásai eljárásainak

rendszerszervezése, és erőforrás igényei biztosítása

5.3.1.10. A hátterekre a vagyon-, és IT biztonsági védelmi intézkedések (a Biztonsági Politikának megfelelően)

5.3.1.11. Életvédelmi intézkedések

5.3.1.11.1. Életvédelmi eszközök és elhelyezésük

5.3.1.11.2. Elsősegélynyújtás

5.3.1.11.3. Kiürítési terv (tűz, bombariadó, egyéb katasztrófa)

5.3.1.12. Pénzügyi feltételek biztosítása az egyes fázisokhoz

5.3.1.13. A Terv tesztelése

5.3.1.13.1. Szóbeli

- A teszt rövid leírása
- A teszt végrehajtói
- A tesztelés gyakorisága

5.3.1.13.2. Helyzet szimulációs

- A teszt rövid leírása
- A teszt végrehajtói
- A tesztelés gyakorisága

í

5.3.1.14. A Terv oktatása

5.3.1.14.1. Menedzsmentnek

5.3.1.14.2. Team tagoknak

5.3.1.14.3. Munkatársaknak

5.3.1.15. A Terv karbantartása

5.3.1.15.1. Katasztrófa előtt

5.3.1.15.2. Katasztrófa után

5.4. VÁLASZ FÁZIS

5.4.1. Akcióterv

5.4.1.1. A vészhelyzet megállapítása, kihirdetése

5.4.1.2. A teamek riasztása

5.4.1.3. Kárkövetkezmények csökkentése

5.4.1.4. Emberi életek mentése

5.4.1.5. Kiürítés

5.4.1.6. Eszközök mentése

5.4.1.7. A teamek munkájának megkezdése

5.4.1.8. Tájékoztatás a katasztrófáról

5.4.1.9. Hatóságok

5.4.1.10. Sajtó

5.5. VISSZAÁLLÍTÁSI FÁZIS

5.5.1. Akcióterv

5.5.1.1. IR újra indítás

5.5.1.2. Az alkalmazói rendszerek prioritásai

5.5.1.3. Az alkalmazói rendszerek újraindítása

5.5.1.4. Az alkalmazói rendszerek üzemeltetése

5.5.1.5. ÜR újra indítás

5.5.1.6. Üzleti folyamatok újraindítása

5.6. HELYREÁLLÍTÁSI FÁZIS

5.6.1. Akcióterv

5.6.1.1. Kárfelmérés

5.6.1.2. Helyreállítás tervezése

5.6.1.3. Fizikai katasztrófa akcióterve

5.6.1.4. Logikai katasztrófa akcióterve

5.6.1.5. Kárkövetkezmények elhárítása

5.6.1.6. Eredeti állapot helyreállítása

5.6.1.7. Vírus katasztrófa elhárítási terve

5.7. A TERV MELLÉKLETEI

5.7.1.1. A 3,3,1.2.-ben szereplő dokumentumok

5.7.1.2. A 3.3.1.9.-ban szereplő dokumentációk

5.7.1.3. A védelmi intézkedések összefoglalása

6. A BIZTONSÁGI SZABÁLYZAT KIDOLGOZÁSA

6.1. A BIZTONSÁGI SZABÁLYZAT CÉLJA

A Biztonsági Szabályzat (BSZ) célja, hogy a védelmi intézkedések üzemeltetési feladatait, és az ezekkel kapcsolatos felelősségeket úgy szabályozza, hogy az üzemeltetés ne gyengítse a védelmi intézkedést, illetve a védelmi intézkedés kényszerítse ki a védelmi követelményeket.

6.2. A BIZTONSÁGI SZABÁLYZAT ALAPJA

A BSZ készítésének alapja

- ⇒ a Biztonsági Politika, és
- ⇒ a Katasztrófaterv, amelyek a védelmi intézkedések alkalmazására vonatkozó utasítások.

Vigyázat! A szabályzat magatartást, cselekvést meghatározó szabályok összessége, míg az utasítás valaminek a végrehajtására vonatkozó rendelkezés.

6.3. A BIZTONSÁGI SZABÁLYZAT FELÉPÍTÉSE

A BSZ felépítése, és tartalma a következő fejezetben található meg.

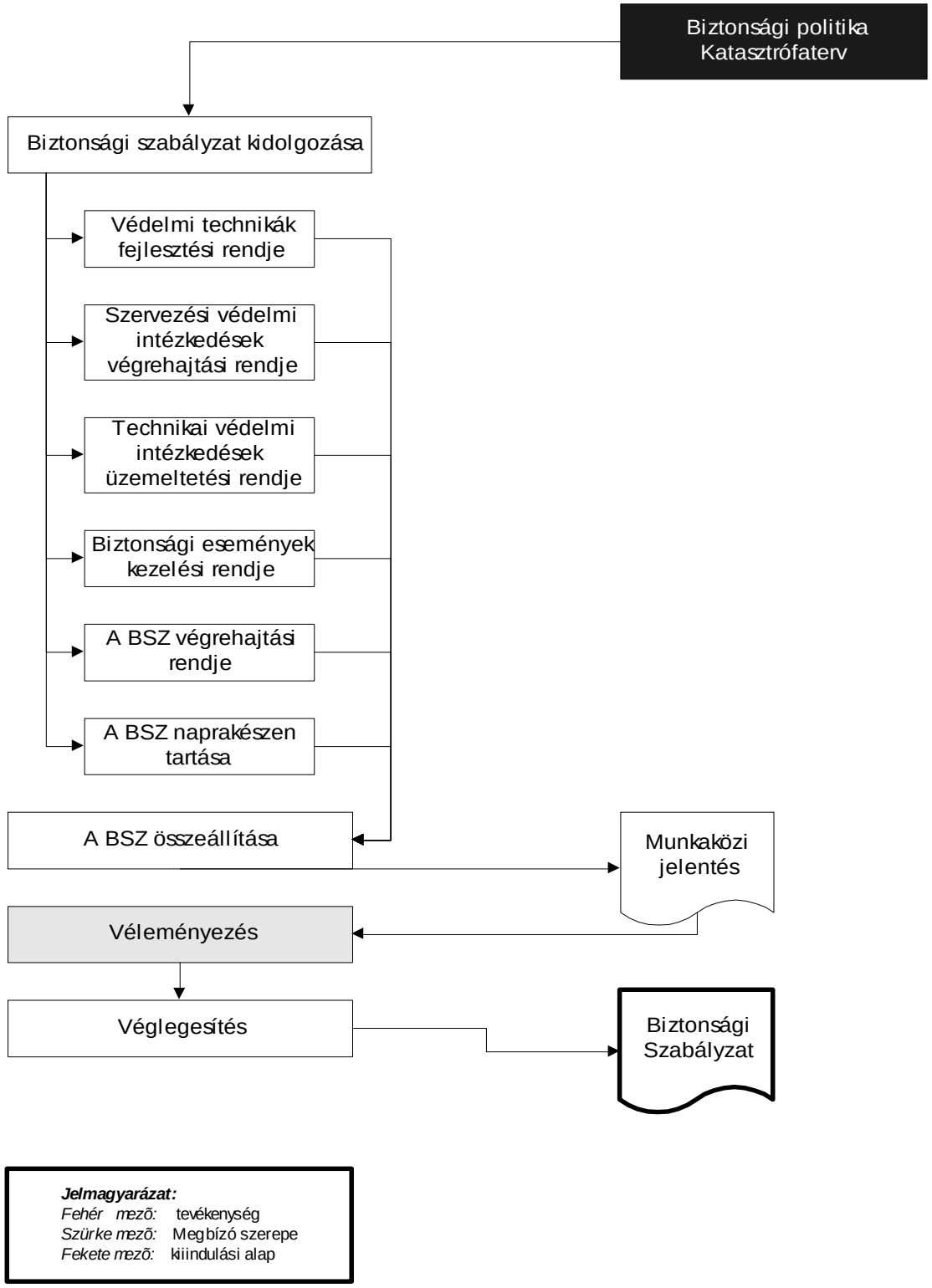
6.4. A KIDOLGOZÁS

A Biztonsági Szabályzat készítésének folyamatábrája a következő oldalon található.

6.4.1. Kiinduló feltételek

- ⇒ *A BSZ a teljes vállalat területén szabályozza a vagyon-, és az informatikai biztonság üzemeltetésével kapcsolatos feladatokat, és felelősségeket. Amennyiben a Megbízó csak egy részterületre (pl. informatika) igényli a szabályozást a BSZ bevezetőjében utalni kell a vállalati BSZ-re (ha ilyen nincs, annak hiányára).*
- ⇒ *Amennyiben a BSZ-t úgy kell elkészíteni, hogy az egyéb biztonsági dokumentumok nem állnak rendelkezésre, akkor csak a meglévő védelmi intézkedések kerülhetnek szabályozásra. Ehhez szükség van a működő védelmi intézkedések feltárására, amelynek során a biztonságszervező előtt ismertté válhatnak védelmi gyengeségek is. Nem szabad (mert nem lehet) a BSZ készítése címén a hiányzó dokumentumokat elkészíteni. Ellenben a BSZ–el együtt át kell a Megrendelőnek adni az ismertté vált gyengeségekről egy figyelem felhívó kísérő anyagot. Ez az anyag azonban nem lehet veszélyforrás elemzés, még kevésbé védelmi intézkedések specifikálása.*

A BIZTONSÁGI SZABÁLYZAT KÉSZÍTÉSÉNEK FOLYAMATÁBRÁJA



Kapcsolódó szabályzatok
A BSZ-t a következő szabályzatokkal összhangban kell elkészíteni:

⇒ Szervezeti és működési szabályzat,
⇒ Titokvédelmi utasítás,
⇒ Iratkezelési szabályzat,
⇒ Tűzvédelmi szabályzat,
⇒ Munka és balesetvédelmi szabályzat, és
⇒ Jogi, és szerződéses kötelezettségek dokumentumai
⇒ Polgári védelmi szabályzat.

Ebből következik, hogy a kidolgozási folyamatban biztosítani kell a fenti szabályzatok felelőseinek aktív közreműködését.

6.4.2. A védelmi intézkedések üzemeltetése

A védelmi intézkedések üzemeltetése alatt a védelmi intézkedés

⇒ *működtetését vagy végrehajtását,*
⇒ *felhasználását, és*
⇒ *karbantartását értjük.*

Értelemszerűen az egyes védelmi intézkedések üzemeltetésének szabályozásánál mind a hárommal foglalkozni kell. A szervezési védelmi intézkedéseknél, mivel azok utasítás formájában realizálódnak végrehajtásról, míg a technikai védelmi intézkedéseknél működtetésről lehet szó. A technikai védelmi intézkedések egy része azonban nem igényel működtetést, de karbantartást viszont igen (például Faraday háló vagy egy helyiség speciális falazata).

A védelmi intézkedéseket csak a BSZ-ben szabályozott módon lehet életbe léptetni, működtetését felfüggeszteni, illetve megszüntetni. A hatályos védelmi intézkedésekről a BSZ melléklete szerinti nyilvántartást kell vezetni.

A nyilvántartás felépítése:

Sor sz.	Azonosító	Megnevezés	Eredet (szállító)	Regisztráció időpontja	Megszüntetés Időpontja

Az azonosító a részleges védelmi intézkedéseknél a Biztonsági politikában, és a Katasztrófatervben alkalmazott azonosító. A megnevezés a védelmi intézkedésnek a Biztonsági politikában, és a Katasztrófatervben alkalmazott elnevezése. Az eredet a szervezési védelmi intézkedéseknél belső szabályzatra való hivatkozás, a technikai védelmi intézkedésnél a készítő/szállító megnevezése.

6.4.3. A biztonsági szervezet típusai

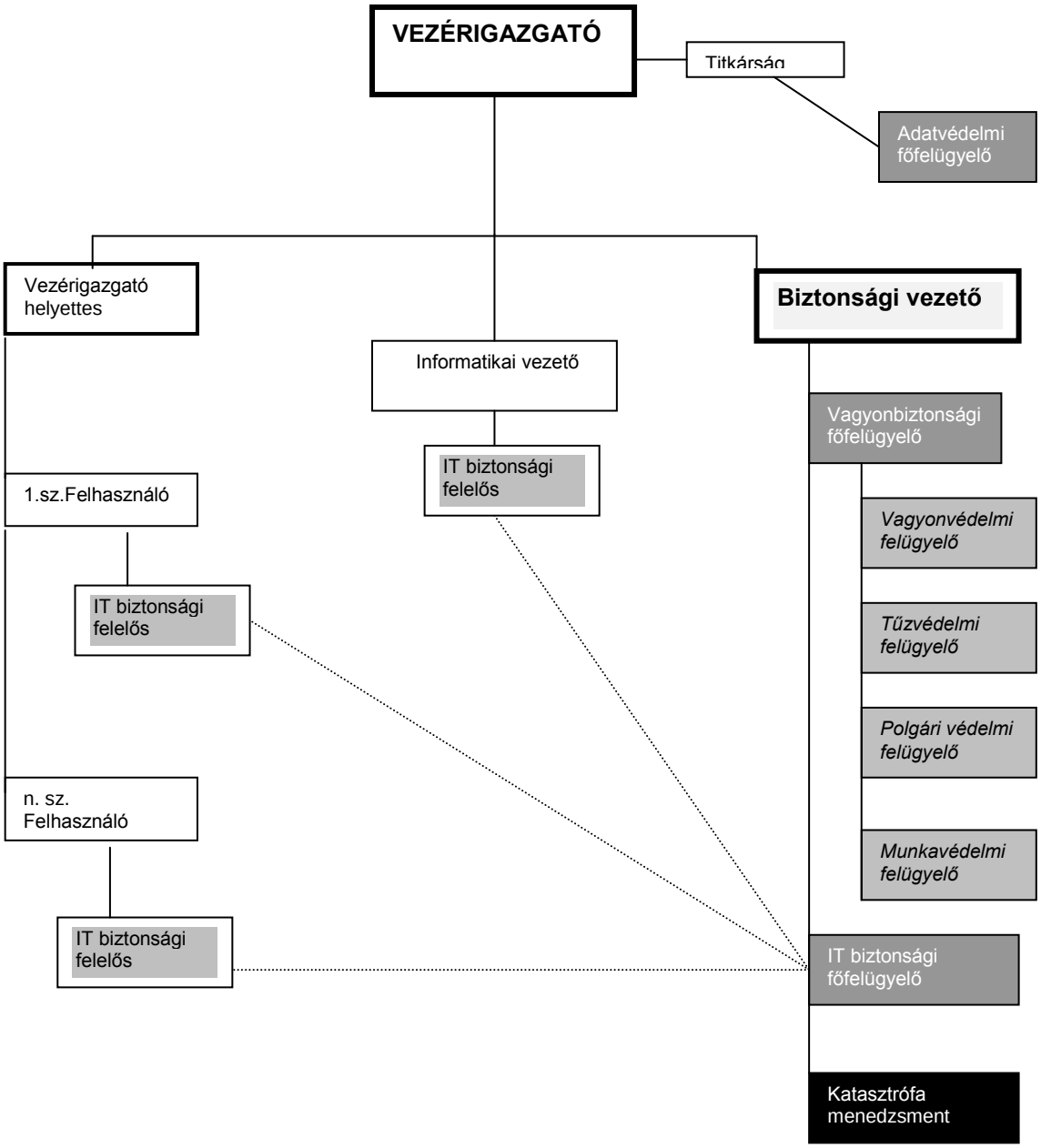
A biztonsági szervezetnek az egyenszilárdság elve alapján központosítottnak, és integrált kell lennie. Ez azt jelenti, hogy a gazdasági szervezet első számú vezetője – aki a biztonságért egy személyben felelős — közvetlen alárendeltségében kell az adat, és vagyonbiztonságot egyaránt irányító biztonsági szervezetet kialakítani. Az egyes szervezeti egységeknél létesített biztonsági felelősi munkakörök (vagyon, és IT biztonsági) az adott szervezet vezetőjének alárendeltségébe tartoznak, de a szakmai irányításukat a központi biztonsági szervezetnek kell ellátni.

Az alábbiakban megadunk három alternatívát a gazdasági szervezetekben kialakítható informatikai biztonsági szakmai biztonság menedzsmentre, valamint az ábrák egyúttal a biztonsági szervezet felépítését is bemutatják.

Az alternatívák:

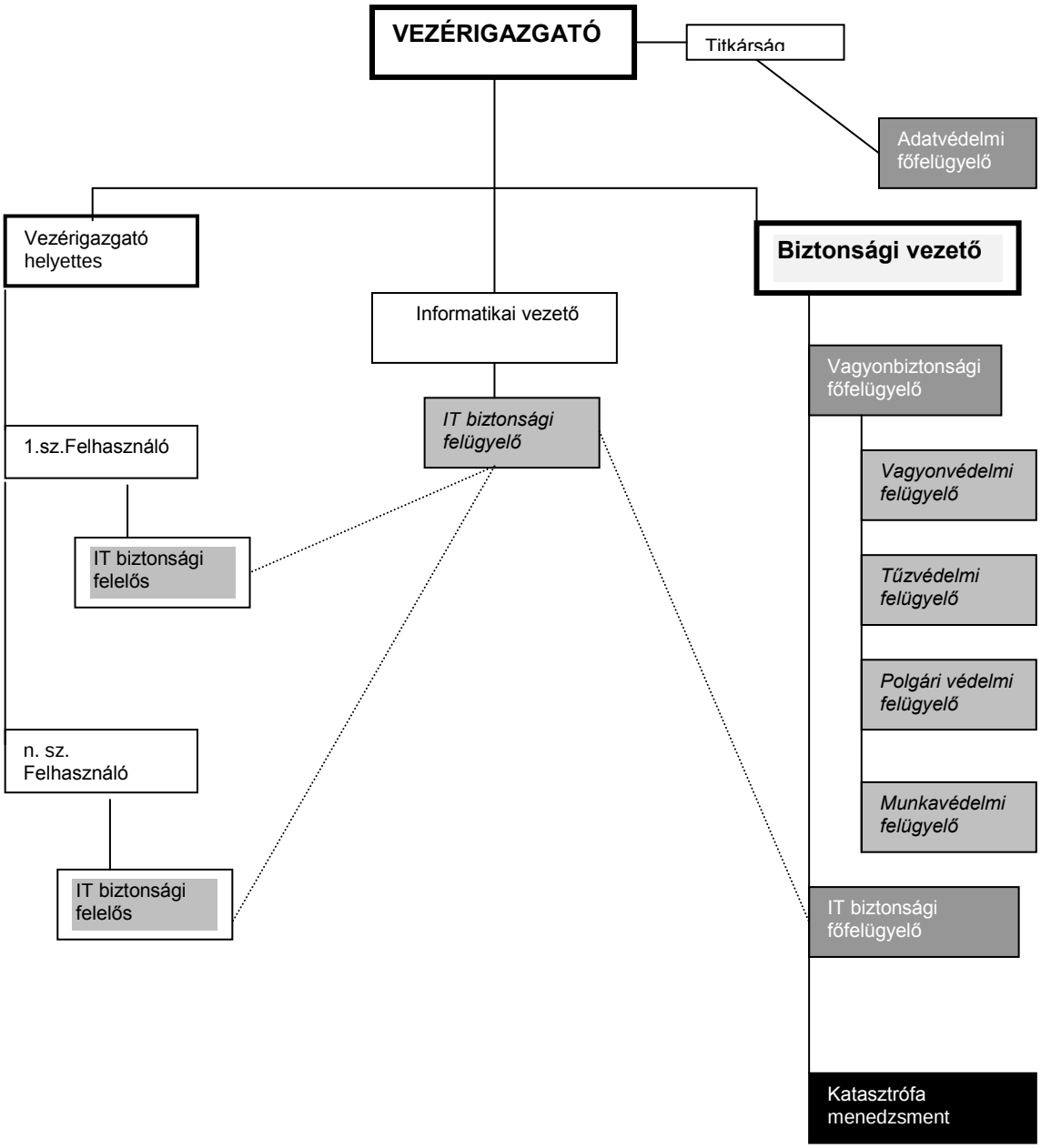
- ⇒ ***Elosztott.*** Az IT biztonság szakmai irányítását az IT biztonsági főfelügyelő látja el, akihez közvetlenül tartoznak az informatikai szervezet IT biztonsági felelőse, és a felhasználói szervezetek IT biztonsági felelősei.
- ⇒ ***Centralizált.*** Az IT biztonság szakmai irányítását az IT biztonsági főfelügyelő látja el, akihez közvetlenül az informatikai szervezet IT biztonsági felügyelője tartozik. A felhasználói szervezetek IT biztonsági felelőseinek szakmai irányítását az informatikai szervezet IT biztonsági felügyelője látja el.
- ⇒ ***Erősen centralizált.*** Az IT biztonság szakmai irányítását az IT biztonsági főfelügyelő látja el, akihez közvetlenül az informatikai szervezet IT biztonsági felügyelője tartozik., aki ellátja felhasználói szervezetek IT biztonság menedzsmentjét is.

6.4.3.1. Elosztott



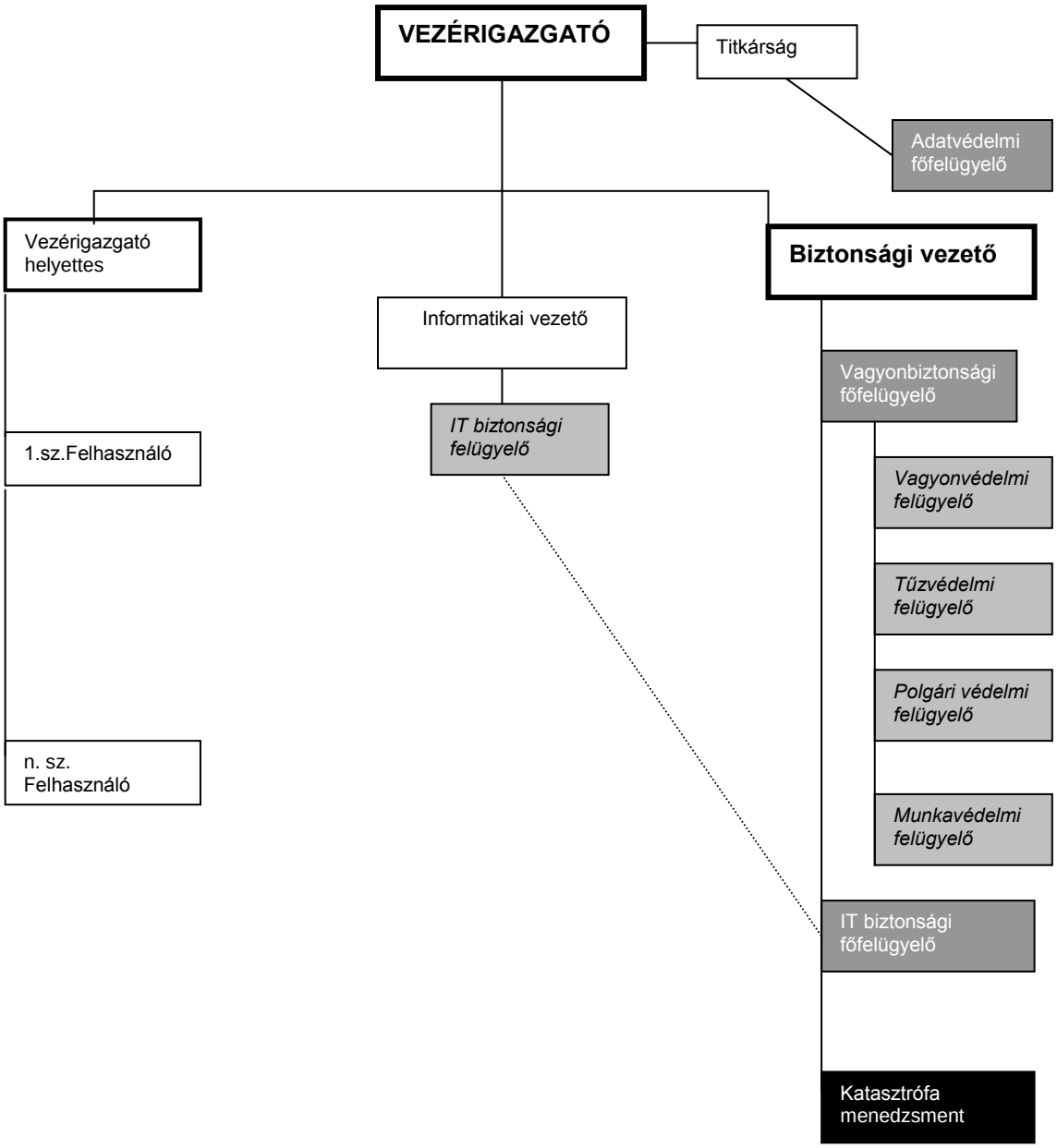
.

6.4.3.2. Centralizált



.

6.4.3.3. Erősen centralizált



.

6.4.4. A BSZ kibocsátása

A vállalat biztonságáért a Vezérigazgató felelős, tehát a BSZ-t a Vezérigazgató írja alá, adja ki.

6.4.5. A kritikus pontok

⇒ A BSZ-ben nem neveknek, hanem munkaköröknek kell szerepelni.

⇒ A BSZ nem a megismétlése a Biztonsági politikának, illetve a Katasztrófatervnek. A Biztonsági politikában, és a Katasztrófatervben az akciótervek a védelmi intézkedések kidolgozására, fejlesztésére nem az üzemeltetésükkel kapcsolatos feladatokra, és felelősségekre vonatkoznak.

⇒ Előfordulhat az, hogy a Biztonsági Politikában egy védelmi intézkedés egy részére szerepel (hibásan) intézkedés. A védelmi intézkedések teljes körűségét, azaz azt, hogy minden védelmi intézkedés és azok minden üzemeltetési feladatának szerepelnie kell. Például a Biztonsági Politikában csak az szerepel, hogy a logikai hfv.-ben a szükséges tudás elvét kell alkalmazni. A Biztonsági Szabályzatban azonban a teljes jelszó, és a teljes jogosultság menedzsmenttel kapcsolatos üzemeletetési feladatokat, a felelősségeket szabályozni kell.

⇒ A BSZ-ben a titokvédelem, és az iratkezelés nem szerepel. Ezek a Titokvédelmi Utasításban, és az Iratkezelési Szabályzatban kerülnek szabályozásra.

⇒ A BSZ nem ajánlás, hanem végső formájában egy utasítás, tehát a stílusa felszólító jellegű.

⇒ A BSZ megismertetése, és elfogadtatása a biztonsági tudatosság része, ezért a szabályozásnak biztosítani kell, hogy az erre irányuló tevékenység ne legyen formális.

⇒ A BSZ-ben meg kell határozni a BSZ megsértésének következményeit, kifejezve a vállalatvezetésnek elszántságát a felelősségek érvényesítésére

⇒ A védelmi intézkedések életciklusára az IR életciklusra vonatkozó védelmi követelményeket kell érvényesíteni.

⇒ Az Informatikai Biztonsági Szabályzatnál ügyelni kell arra, hogy a fizikai hozzáférés-védelmi intézkedések szoros kapcsolatban vannak a vagyonbiztonság keretében megtett fizikai hozzáférés-védelmi intézkedésekkel. Ez különösen akkor kritikus pont, ha a vagyonbiztonság nem tárgya, illetve nincs rá Biztonsági Szabályzat.

6.4.6. A Megbízó szerepe

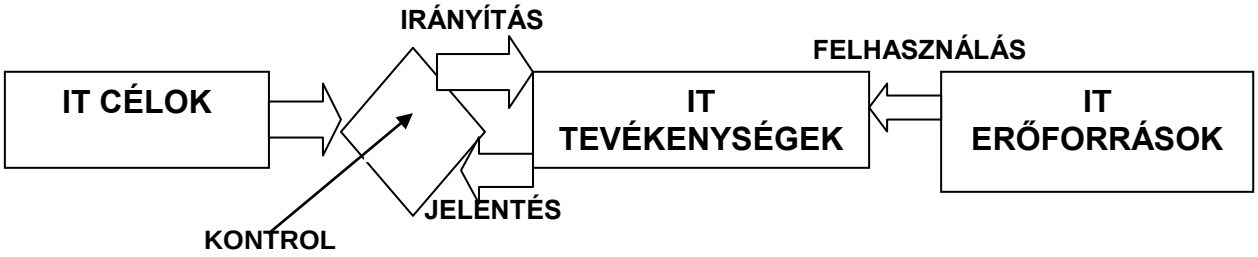
A Megbízó teljes egyetértése szükséges a BSZ kiadásához, ezért a módosítási igényeit át kell vezetni. Javasolt ezeknek az igényeknek a kidolgozás során a folyamatos dokumentálás.

6.5. AZ IT BIZTONSÁGIRÁNYÍTÁS

Az IT biztonságirányítás: rendszer készítése, és karbantartása, gondoskodás a garanciákról, hogy a Biztonsági Stratégia megfeleljen az üzleti céloknak, és legyen konzisztens a törvényekkel, és szabályokkal.

Az IT biztonságirányítás célja: összpontosítani arra a szükségletre, hogy stabil irányítási program álljon rendelkezésre, így a Biztonsági Stratégia, és folyamat tervezhető, implementálható, és karbantartható legyen.

Az IT Biztonságirányítás funkcionális modellje:



Az IT célok:
- Az üzlet lehetővé tétele, és maximalizálása
- Az IT erőforrások felelősséggel való használata
- Az IT kockázatok megfelelő menedzselése

Az IT tevékenységek:
- Kockázat menedzsment (biztonság, gondoskodás az információkról, megfelelősség),
- Haszon realizálása az automatizálás hatékonyságával, és a költségek csökkentése az eredményesség elősegítésére.

Az IT erőforrások a korábbiakban szerepelnek.

Az „Information Security Governance: Guidance for Board of Directors and Executive Management" a vezetési tevékenységeket, a fentiek figyelembe vételével, a következők szerint határozza meg:

*Az **Informatikai Biztonság Menedzsment struktúrája** egyrészt felépül az alábbi biztonsági tevékenységeknek a vezetési szintekhez rendeléséből, másrészt magából az informatikai biztonsági szervezetből (lásd 6.3 pontban) (az MSZ ISO/IEC 17799-ben informatika biztonsági infrastruktúraként szerepel)..*

A felső vezetési szint (igazgatóság) IT biztonságirányítási tevékenységei:
- ⇒ Folyamatosan informált a biztonságról.
- ⇒ Megszabja az irányítást, vagyis politikát, és stratégiát működtet, és meghatározza a globális kockázati profilt.
- ⇒ Erőforrásokat biztosít az IT biztonság eredményességéhez.
- ⇒ Kijelöli a menedzsment felelősségeit.
- ⇒ Meghatározza a prioritásokat.
- ⇒ Támogatja a változásokat.
- ⇒ Meghatározza a kulturális értékeket a biztonsági tudatosság vonatkozásában.
- ⇒ Garanciákat szerez be a belső, és külső ellenőrzéstől.
- ⇒ Ragaszkodik ahhoz, hogy a menedzsment a biztonsági beruházásokat, és a fejlesztéseket mérhetően végezze, valamint kövesse figyelemmel azok hatékonyságát.

A menedzser szint (IT VEZ. IG. H. és/vagy ÜGYVEZETŐ IG) tevékenységei:

- ⇒ Biztonsági politikát ír, üzleti inputokkal.
- ⇒ Gondoskodik arról, hogy az egyéni szerepek, felelősségek, és jogosultságok világosan legyenek kommunikálva, és mindenki értse meg.
- ⇒ Azonosítja a fenyegetéseket, elemzi a sebezhetőségeket, és figyelembe veszi az általános gyakorlatot.
- ⇒ Létrehozza a biztonsági infrastruktúrát.
- ⇒ Fejleszt egy biztonsági, és ellenőrzési rendszert, amely szabványokat, mértékeket, gyakorlatot, és folyamatokat tartalmaz, és a szervezet irányító testülete egy politika alapján hagyja jóvá a szerepeket, és felelősségeket, és eszerint jelöli ki azokat.
- ⇒ Biztosítja a biztonsági célok (bizalmasság, sértetlenség, rendelkezésre állás, számon kérhetőség, garanciák) megvalósulását.
- ⇒ Megtervezi a végrehajtási folyamatokat.
- ⇒ Biztosítja, hogy a biztonság az IT életciklusának integrált része legyen.
- ⇒ Biztosítja a képzést, a biztonsági tudatosságot.
- ⇒ Dönt, hogy milyen erőforrások álljanak rendelkezésre, meghatározza a lehetséges védelmi intézkedések fontossági sorrendjét, és implementálja a magas priorítású védelmi intézkedések közül azokat, amelyeket a vállalat tud biztosítani.
- ⇒ Monitorozza a biztonsági eseményeket, és biztosítja azok kezelését.
- ⇒ Periodikus vizsgálatokat, és teszteket végez.
- ⇒ Biztosítja a biztonsági tudatosságot, oktatást, tréningeket.
- ⇒ Felhasználja az érettségi szint (maturity level) értékelési módszert (lásd melléklet) az önértékelésre.

Az IT biztonsági vezető feladatai:

- ➢ A vállalat biztonsági rendszerén belül, az üzleti rendszerrel összhangban lévő IT biztonsági alrendszer szervezése.
- ➢ A biztonsági stratégiát megvalósító biztonsági program kidolgozása, és megvalósítása.
- ➢ A humán, fizikai, és logikai védelmi intézkedések
  - Beszerzése, fejlesztése,
  - Üzemeltetése,
  - Rendeltetésszerű alkalmazásának felügyelete, és
  - A megszüntetése,

  olyan módon, hogy ezek kikényszerítsék a vállalat üzleti céljának megfelelő biztonsági követelményeket a kockázatok folyamatos figyelembevételével, követésével.
- ➢ Az IT szervezetbe tartozó informatikai biztonsági felelősök szakmai irányítása.
- ➢ A biztonsági tudatosság erősítése.
- ➢ Gondoskodás az IT biztonsági események kezeléséről.
- ➢ Rendszeresen, évente legalább két alkalommal jelentést készít a menedzsment részére, az IT biztonság helyzetéről a belső ellenőrzési jelentések, mérések, biztonsági események, és problémák felhasználásával.

Az MSZ ISO/IEC 17799 szerint szükséges létrehozni egy Informatikai Biztonság Menedzsment Fórumot. Ez a fórum része a szervezet vezető testületének. Fő feladatai:

- felülvizsgálja és jóváhagyja az informatikai biztonsági szabályzatot és az átfogó felelősségeket (összehangolja azokat),
- figyelemmel kíséri azokat a változásokat, amelyek az információvagyonnak a fenyegetettsége, miatt lépnek fel,
- felülvizsgálja, és figyelemmel kíséri a véletlen biztonsági eseményeket,
- az informatikai biztonságot, fokozó újításokat jóváhagyja.

Ezenkívül ellát informatikai biztonsági koordinációs tevékenységet, mint

- sajátos informatikai biztonsági szerepeket és felelősségeket állapít meg az egész szervezetre kiterjedően,
- sajátos módszereket és folyamatokat állapít meg az informatikai biztonsági kockázatbecslésre, a biztonsági osztályozási rendszerre,
- az egész szervezetre kiterjedően állapít meg és támogat informatikai biztonsági kezdeményezéseket/újításokat, például biztonsági népszerűsítő programokat,
- gondoskodik arról, hogy a biztonságtechnika része legyen az informatikai tervezés folyamatának,
- felméri az új rendszerek és szolgáltatások számára kiválasztott sajátos informatikai biztonsági intézkedések alkalmasságát, és összehangolja megvalósításukat,
- áttekinti a véletlen biztonsági eseményeket,
- népszerűsíti az egész szervezetben az informatikai biztonság üzleti támogatottságának átláthatóságát.

6.6. AZ IT BIZTONSÁG HATÉKONYSÁGÁNAK MÉRÉSE

6.6.1. Az IT biztonság sikerességének meghatározása

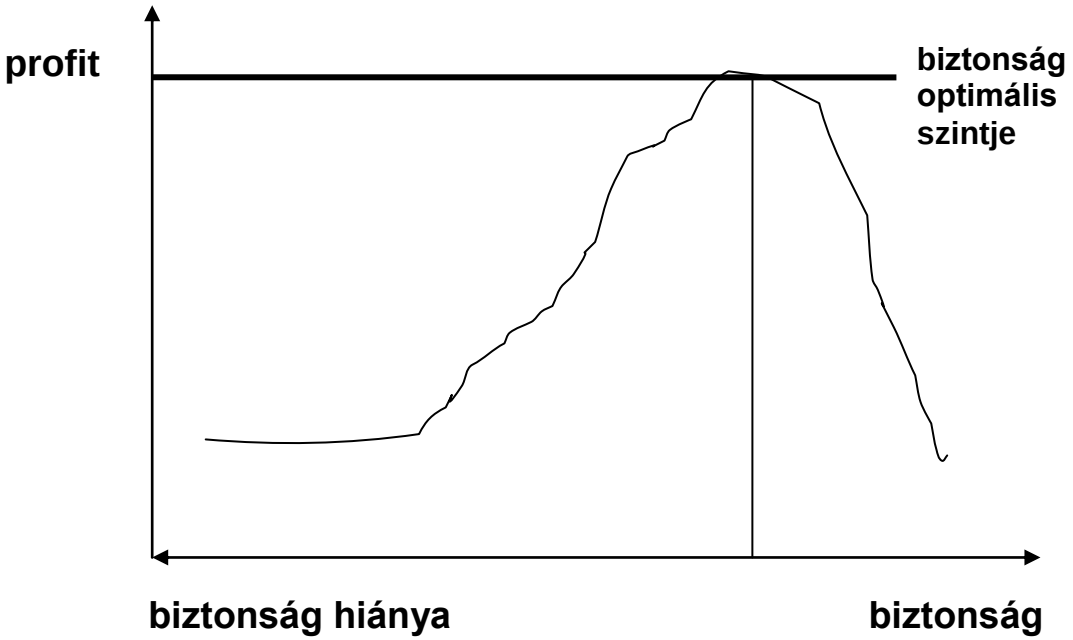
- Semmilyen esemény nem okozott nyilvános zavart.
- Az új implementációk kis száma késett biztonsági zavar miatt.
- A küldetés kritikus üzleti folyamatokat kiszolgáló IT rendelkezik ÜFT-vel.
- A kritikus infrastruktúra elemeinek rendelkezésre állása automatikusan felügyelve van.
- Az alkalmazottak tudatossága mérhető fejlődést mutat (rendszer biztonsági elvek, és a feladatok teljesítménye etikai, és biztonsági oldalról).

6.6.2. Az IT biztonságirányítás sikerességének meghatározása

- Teljes megfelelés vagy megegyezéses, és rögzített eltérés a minimális biztonsági követelményektől.
- A fejlesztett, és dokumentált IT tervek, és politikák meghatározott százaléka megfelel az IT biztonsági küldetésnek, elgondolásnak, céloknak, értékeknek, és a vezetés szabályainak.
- Az IT biztonsági tervek, és politikák meghatározott százaléka ismertetve van a részvényesekkel.

6.6.3. A biztonság költséghatékonyságának meghatározása

A vállalatok üzleti érdeke a biztonság, de ez egyúttal annyit is jelent, hogy a biztonságnak nem lehet csak a védelem költségeinek, és a sikeres támadások, okozta költségek, üzleti szempontból elviselhető arányát, képezni. Az üzleti érdek tehát módosíthatja ezt az arányt. Björck a [60]-ben írja Martinra (1992) hivatkozva, hogy a biztonság optimális szintje egy szervezetben, pénzügyi szempontból ott van, ahol a védelmi költségek a támadások által okozható költségek csökkentésével azonosak. Egyúttal a következő görbével ábrázolja a biztonság menedzsment balanszírozási lehetőségének alakulását, a biztonság optimális szintjének (azaz itt csak a pénzügyi szempontok szerepelnek).



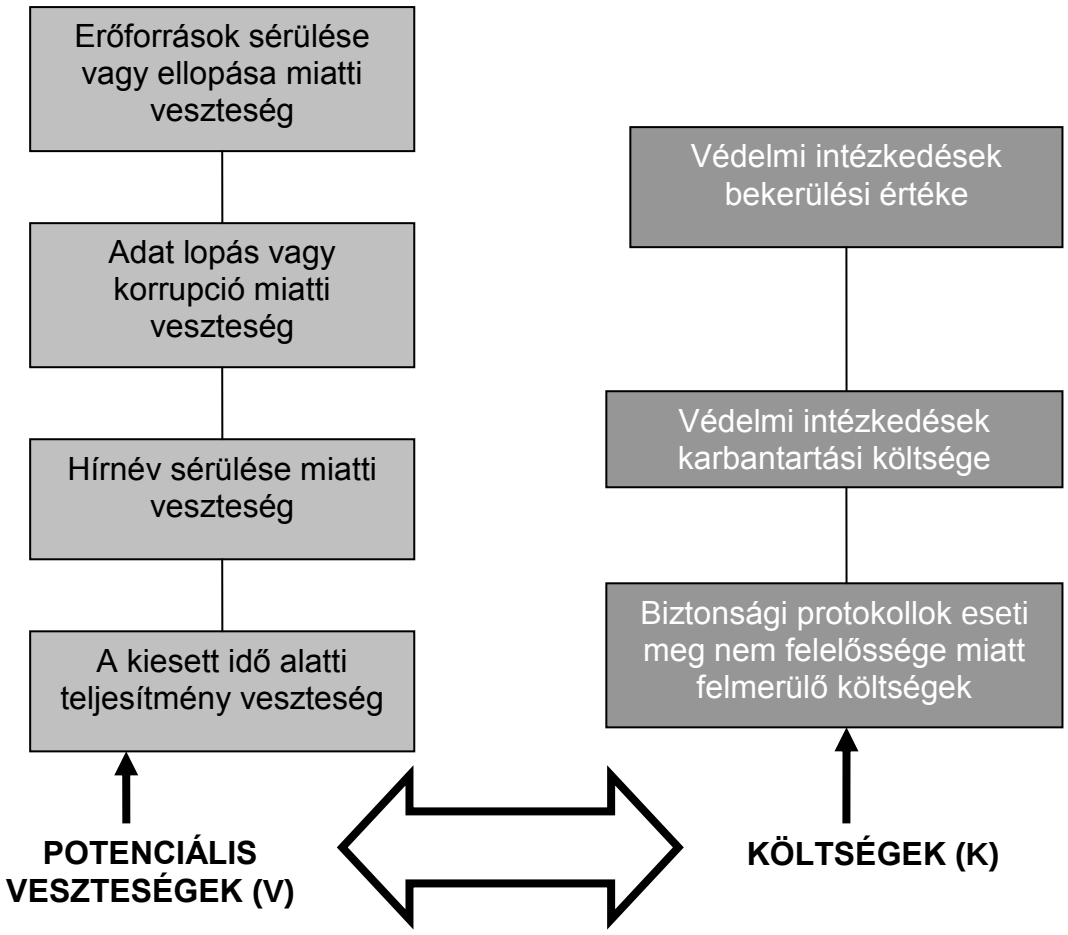
Az ábrából következik, hogy a kis biztonsági szint, a sikeres támadási arány nagyobb valószínűsége miatt, a profit csökkenését eredményezheti, míg a túl sok biztonság esetén a védelem nagyobb költségei csökkentik a profitot. Általában az adott időben alkalmazott védelem költségei, és az adott időben elkövetett támadások költségei nem ismertek. Így az optimum elérésére csak, azt folyamatosan szem előtt tartva, törekedni lehet.

A biztonsági beruházások megtérülési szintjét, egyébként a Return of Security Investment (ROSI) mutató fejezi ki. A biztonsági költségek megtérülnek, ha a hatásukra a kockázatok elfogadható szintre (a ROSI elfogadható) csökkennek. A számszerű meghatározás nehézsége ott van, hogy egy támadás esetében a kár elsősorban a vagyontárgyakban (tárgyi, és szellemi) keletkezik, és a tárgyiakban határozható meg csak

számszerű módszerekkel, nem beszélve a vagyontárgyakon kívül az erőforrásokhoz tartozó humán erőforrásokról. Így a kárnak lesz egy becsült összetevője is. Általában azt tartják, hogy a biztonságra nem szabad többet költeni, mint amit egy biztonsági eseménynél veszíthetünk (a tárgyi, és szellemi vagyontárgyak, egyéb erőforrások sérülésével).

Az informatikai biztonságra vonatkozóan A. Mizzi [61]-ben, az előző bekezdésben írtakat felvetve, bemutat egy eljárást, összefüggéseket ad meg, az informatikai biztonsági beruházás megtérülési mutatójának (ROISI, Return on Information Security Investment) számítására. A károknál azonban csak a hw, és sw károkat, tárgyi, és szellemi (nem tárgyiasult) veszi figyelembe. Ismert, hogy az informatikai erőforrások ezen kívül, humán, valamint egyéb (pl. létesítmények) elemeket is tartalmaznak, amelyek szintén sérülhetnek.

S. Niels [26]-ban egy jó megközelítést add meg a védelmi intézkedések költségei, és a potenciális, lehetséges, becsült veszteségek közötti egyensúlyozásra. E módszert, alkalmazva a könyvben meghatározott fogalmakat, az alábbiakban mutatjuk be:



A potenciális veszteségek, mint az előbbiekben erről szó volt, összességében, tehát csak becsülhetők, míg a költségek számíthatóak. Ezekből következtetve, *a biztonsági beruházás megvalósítható, ha*

$$K<V$$

tehát a költségek kisebbek, a becsült veszteségeknél.

Végül fel kell hívni a figyelmet arra, hogy a fentiek általában a profit orientált szervezetekre vonatkoznak. Ugyanakkor rá kell mutatni arra, hogy mennél biztonság érzékenyebb egy szervezet tevékenysége, annál inkább a döntő, a megtérüléssel szemben a biztonsághoz fűződő érdek.

7. BIZTONSÁGI SZABÁLYZAT

7.1. AZ IT BIZTONSÁG IRÁNYÍTÁSA

7.1.1. AZ Informatikai Biztonság menedzsment struktúrája

7.1.1.1. Igazgatóság biztonsági feladatai

7.1.1.2. Felső vezetés biztonsági feladatai

7.1.1.3. IT Biztonsági Forum

7.1.1.4. IT Biztonsági vezető feladatai

7.1.1.5. IT biztonsági szervezet

7.1.2. Az IT biztonság hatékonyságának mérése

7.1.2.1. IT biztonság sikeressége, és költség hatékonysága

7.1.2.2. IT biztonságirányítás sikeressége

7.2. BIZTONSÁGI POLITIKA KÉSZÍTÉSE

A célszerűségi okokból a Stratégiák után tárgyalt, az I. kötet. 14. Biztonsági Politika készítése fejezete.

7.3. RÉSZLEGES VÉDELMI INTÉZKEDÉSEK

7.3.1. Általános rész

7.3.1.1. A Biztonsági Szabályzat célja

7.3.1.2. Értelmezések

⇒ A védelmi intézkedés a veszélyforrás bekövetkezési valószínűsége, illetve a bekövetkezésekor keletkező kár csökkentésére szervezési vagy technikai eszközökkel tett intézkedés.
⇒ A részleges védelmi intézkedés egy erőforrás védelmére tett intézkedés.
⇒ Az átfogó védelmi intézkedés a teljes rendszer kiesése esetén a kárkövetkezmények csökkentésére tett intézkedés.
⇒ A felhasználó egy entitás (humán vagy gépi) a hozzáférés védelmi rendszeren kívül, amely a hfv.-i rendszerrel együtt tud működni, és nincs speciális jogosultsága a Biztonsági Politika kikényszerítésére.

Az alábbiakban az egyes pontoknál megadott feladatok az előfordulási gyakoriság alapján lettek kiválasztva, a teljesség igényét nem elégítik ki.

7.3.2. A védelmi technikák fejlesztése

Ebben a fejezetben az egyes védelmi intézkedésekből következő feladatot, illetve feladatokat a következő sablon szerint kell megadni:

⇒ A védelmi intézkedés megnevezése:
⇒ A feladat meghatározása:
⇒ A működtetésért felelős:
⇒ A karbantartásért felelős:
⇒ A Felhasználó(-k), amennyiben értelmezhetők. :
⇒ A felhasználás szabályai:

7.3.2.1. A fejlesztés/beszerzés

⇒ A fejlesztés, beszerzés eldöntése
⇒ A fejlesztés, beszerzés megrendelése (A Biztonsági Politikában, illetve a Katasztrófatervben specifikált védelmi intézkedések alapján).
⇒ A fejlesztés, beszerzés során a biztonsági követelmények érvényesítése, ellenőrzése.

7.3.2.2. Az átadás/átvétel

7.3.2.2.1. Átadás / átvételi folyamat

⇒ A biztonsági követelmények érvényesítésének ellenőrzése az átvétel folyamán.
⇒ A szállító biztonsági nyilatkozatainak (pl. biztonsági követelmények betartása a fejlesztés során, vagy fenyegetés mentességi nyilatkozat)átvétele, megőrzése.

7.3.2.2.2. Bevezetés, regisztráció

⇒ Az átvett védelmi intézkedés regisztrációja.

7.3.2.2.3. Védelmi intézkedés megszüntetési rendje

7.3.3. A védelmi intézkedések üzemeltetése

7.3.3.1. Szervezési védelmi intézkedések

Ebben a fejezetben az egyes védelmi intézkedésekkel kapcsolatos feladatot, illetve feladatokat a következő sablon szerint kell megadni:

⇒ A védelmi intézkedés megnevezése:
⇒ A feladat meghatározása:
⇒ A végrehajtásért felelős:
⇒ A karbantartásért felelős:

7.3.3.2. Biztonsági szervezet

⇒ A biztonsági szervezet helye a vállalati SZMSZ-ben.
⇒ A biztonsági szervezet felépítése, és működése.
⇒ A humán erőforrások szerepének, és felelősségének meghatározása (felső vezetés, vezetők, alkalmazottak (felhasználók, tulajdonosok).

7.3.3.2.1. Humánpolitikai védelem

⇒ A humán politika (felvétel, alkalmazás, munkaviszony megszüntetés) kidolgozása, végrehajtása.
⇒ A jogi, és szerződéses kötelezettségek érvényesítésével kapcsolatos felelősségek érvényesítése.

7.3.3.2.2. Védelem a harmadikfelekkel kötött szerződésekben

⇒ A harmadik felekkel kötött szerződésekben a biztonsági követelmények érvényesítése.
⇒ A harmadik felekkel kötött szerződések végrehajtása során a biztonsági követelmények érvényesítésének ellenőrzése

7.3.3.2.3. Kockázat áthárítás

⇒ Vagyoni kárra biztosítások kötése.
⇒ Nem vagyoni kárra biztosítások kötése.

7.3.3.2.4. Biztonsági dokumentumok kezelése

⇒ A biztonsági dokumentumok (Biztonsági Átvilágítás, Biztonsági Politika, Katasztrófaterv) egy példányának őrzése, karbantartása.
⇒ A védelmi intézkedések dokumentációja egy naprakész példányának őrzése.

7.3.3.3. Technikai védelmi intézkedések

Ebben a fejezetben az egyes védelmi intézkedésekből következő feladatot, illetve feladatokat a következő sablon szerint kell megadni:

⇒ A védelmi intézkedés megnevezése:
⇒ A feladat meghatározása:
⇒ A működtetésért felelős:
⇒ A karbantartásért felelős:
⇒ A Felhasználó(-k), amennyiben értelmezhetők:
⇒ A felhasználás szabályai:

7.3.3.3.1. Védelmi intézkedések az üzleti rendszerben

Azok a védelmi intézkedések, amelyek nem szerepelnek az alábbiakban.

7.3.3.3.2. Fizikai hozzáférés-védelem

⇒ A nyers belépő kártyák megrendelése, őrzése.
⇒ Üres íróasztal politika.
⇒ A belépő kártyák megszemélyesítése, és nyilvántartása
⇒ A belépési, mozgási jogosultságok meghatározása.

⇒ A zárt láncú tv. rendszer felvételeinek archiválása, őrzése.
⇒ A belépő kártyák, illetve a jogosultságok módosítása, törlése.
⇒ A visszavont belépő kártyák megsemmisítése.

7.3.3.3.3. Fizikai rendelkezésre állás védelme

⇒ Gondoskodás az eszköz, berendezés redundanciáról.
⇒ Az akusztikus, és elektromágneses kisugárzás védelem időszakos ellenőrzése.

7.3.3.3.4. Logikai hozzáférés-védelem

⇒ A jelszó menedzsment biztosítása (felhasználó azonosító kiadása, és regisztrálása, első jelszó kiadása, és regisztrálása, jelszavak visszavonása).
⇒ A jogosultság menedzsment (a jogosultságok kiadása, és visszavonása, nyilvántartása).
⇒ A jogosultságok jelszavakhoz rendelése.
⇒ A bejelentkezés megszakítás (time out) eljárás érvényesítése.
⇒ A jelszavakkal kapcsolatos felhasználói kötelezettségek érvényesítése, ellenőrzése)
⇒ A védelmi intézkedések meghatározása, érvényesítése tűzfalaknál.
⇒ A rejtjelező eszközök elhelyezésének, kezelésének, védelmének meghatározása.
⇒ A bizalmas számítástechnikai bázis (a jelszavas hozzáférés védelmi szoftver védelmének érvényesítése.
⇒ Digitális aláírás (tartalomhitelesítés).

7.3.3.3.5. Logikai rendelkezésre állás védelem

⇒ A mentési rendszer kidolgozása.
⇒ A mentési rendszer rendeltetésszerű üzemeltetése.
⇒ A mentési másodpéldányok elkülönített helyen történő őrzésének a biztosítása.
⇒ Vírus védelem

7.3.3.3.6. Védelem az információs rendszer életciklusában

⇒ A biztonsági követelmények meghatározása az erőforrások fejlesztés/beszerzése során.
⇒ Az átadás/átvétel lefolytatása, a biztonsági követelmények érvényesítésének ellenőrzése.
⇒ Az átvétel megtörténte után a fejlesztői jogosultságok visszavonása.
⇒ A programok, általában erőforrások módosításának, cseréjének jogosultsága
⇒ A papír és elektronikus hulladékok megsemmisítésével, eszközök selejtezésével kapcsolatos eljárás.

7.3.3.3.7. Védelem a hálózatokban

⇒ A bizalmas hálózatban (intranet) alkalmazandó védelmi intézkedések üzemeltetése.
⇒ A nem bizalmas (extranet, Internet) hálózatokban alkalmazandó védelmi intézkedések üzemeltetése.

7.3.3.3.8. A számon kérhetőség biztosítása

⇒ Elrettentés

⇒ Audit trail
⇒ Audit log
⇒ Behatolás védelem logja
⇒ Információk leltára
⇒ Informatikai eszközök leltára
⇒ Üzleti rendszer eszközeinek leltára
⇒ A fegyelmezés folyamata

7.3.3.4. Működtetést nem igénylő technikai védelmi intézkedések

⇒ A működtetést nem igénylő védelmi intézkedések karbantartása.(fizikai pl. biztonsági falak, üvegek, logikai pl. védelem logikai rombolás ellen.).

7.4. ÁTFOGÓ VÉDELMI INTÉZKEDÉSEK

7.4.1. Szervezési védelmi intézkedések

Ebben a fejezetben az egyes védelmi intézkedésekkel kapcsolatos feladatot, illetve feladatokat a következő sablon szerint kell megadni:

⇒ A védelmi intézkedés megnevezése:
⇒ A feladat meghatározása:
⇒ A végrehajtásért felelős:
⇒ A karbantartásért felelős:

7.4.1.1. Humán erőforrások biztosítása

7.4.1.2. A teamek szervezése, készenlétük biztosítása

7.4.1.3. A Katasztrófaterv időszakonkénti tesztelése

7.4.1.4. Szállítói kapcsolatok

7.4.1.5. Kockázat áthárítási szerződések

7.4.1.6. A Katasztrófaterv karbantartása

7.4.1.7. Pénzügyi feltételek biztosítása

7.4.2. Technikai védelmi intézkedések

Ebben a fejezetben az egyes védelmi intézkedésekből következő feladatot, illetve feladatokat a következő sablon szerint kell megadni:

⇒ A védelmi intézkedés megnevezése:
⇒ A feladat meghatározása:

⇒ A működtetésért felelős:
⇒ A karbantartásért felelős:
⇒ A Felhasználó(-k), amennyiben értelmezhetők:
⇒ A felhasználás szabályai:

7.4.2.1. A háttér eljárások, háttér központok

⇒ működtetése vagy készenlétben tartása
⇒ technológia, alkalmazások, mentések biztosítása

7.4.2.2. A Katasztrófa Kezelő Központ működtetése.

⇒ A katasztrófa menedzser felelős a KKK folyamatos naprakész működtetéséért.

7.4.2.3. Életvédelmi intézkedések.

⇒ Itt kell megadni a kiürítési tervet (-ket), a bombariadó esetén teendőket.

- ellenőrizték a bizonyítékot), valamint hogy a rendszer tárolta (*megőrizte*) és feldolgozta-e a visszanyerni való bizonyítékokat.

7.5. A VÉDELMI INTÉZKEDÉSEK MEGSZÜNTETÉSE

⇒ A védelmi intézkedéseket, csak a biztonsági szervezet szüntetheti meg, és egyúttal a nyilvántartásból azokat törölni kell, a felhasználók értesítése mellett.

7.6. ZÁRÓ RENDELKEZÉSEK

7.6.1. A BSZ végrehajtásával kapcsolatos felelősségek

⇒ Meg kell határoznia biztonsági szervezetben mely munkakört betöltő személy felelős a BSZ végrehajtásáért.

7.6.2. Az ellenőrzés

⇒ A BSZ végrehajtását a biztonsági szervezetnek követni kell, valamint a belső ellenőrzésnek be kell vennie az éves ellenőrzési tervbe.

7.6.3. A BSZ naprakészen tartása

⇒ A BSZ végrehajtásáért felelős egyúttal köteles biztosítani a napra készen tartását.

7.7. A BSZ HATÁLYBALÉPÉSE

7.8. A BSZ MELLÉKLETE

⇒ A BSZ melléklete a védelmi intézkedések nyilvántartása, amelyet a biztonsági szervezet vezet, és tárol.

8. A BIZTONSÁG BELSŐ ELLENŐRZÉSI MÓDSZERTAN KIDOLGOZÁSA

8.1. A MÓDSZERTAN CÉLJA

A Biztonság belső ellenőrzési módszertanának kidolgozása a biztonságszervezés utolsó fázisa. A Módszertan a Megrendelő számára a biztonság belső ellenőrzése kialakításának, tervezésének, és végrehajtásának segédeszköze. A fejezet további része, és az ezt követő fejezet, módszertani útmutatást ad a Módszertan elkészítéséhez.

8.2. A MÓDSZERTAN KIDOLGOZÁSA

A Módszertan kidolgozásának folyamatábrája a következő oldalon található.

8.2.1. Kiinduló feltételek

A Módszertan kidolgozásához rendelkezésre kell állni a Megrendelő Biztonsági politikájának, a Katasztrófatervnek, a Biztonsági Szabályzatnak, amely egyaránt vonatkozik az ÜR-ben az üzleti folyamatokra, és az IR-ben az informatikai folyamatokra. Ezek részbeni, vagy teljes hiánya esetén a Módszertan csak a megtett védelmi intézkedések, és a működő szabályzatok alapján készíthető el, és ezt a tényt az anyagban fel kell tüntetni.

8.2.2. A felépítés

A Módszertan felépítését, és tartalmát a következő fejezetben tárgyaljuk.

8.2.3. A Megbízó szerepe

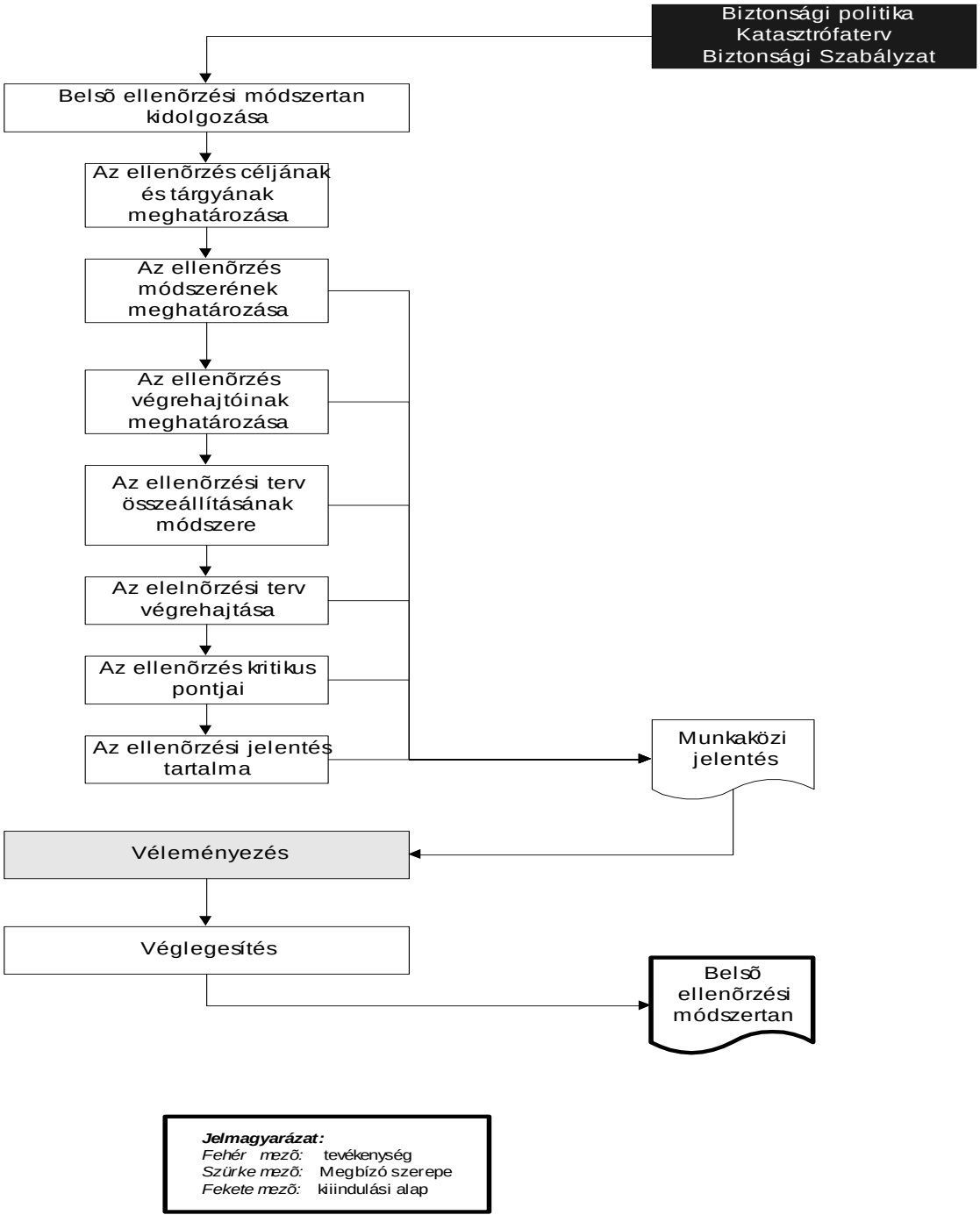
A Megbízó szerepe elsősorban abban áll, hogy közre kell működnie a Módszertannak a vállalat belső ellenőrzési rendszerébe, és gyakorlatába történő beillesztésében. Problémát okozhat a biztonság ellenőrzés személyi feltételeinek biztosítása. E tekintetben azonban nem lehet engedményeket tenni, fel kell ajánlani a külső ellenőrzés lehetősségét addig, ameddig a belső feltételek nem teremtődnek meg.

8.2.4. A kritikus pontok

⇒ A Módszertant az adott szervezet biztonsági dokumentumai alapján kell, illetve lehet elkészíteni, amely azt jelenti, hogy

- a biztonsági dokumentumok hiányában vagy a biztonságszervezés korábbi fázisait is el kell végezni, vagy ami van, annak az ellenőrzésére kell a Módszertant elkészíteni,

A BELSŐ ELLENŐRZÉSI MÓDSZERTAN KÉSZÍTÉSÉNEK FOLYAMATÁBRÁJA



- A Módszertan egy adott ellenőrzéshez segédeszközül szolgál, nem lehet minden lehetséges ellenőrzésre előre konkrétan alkalmas Irányelveket készíteni.

⇒ Figyelembe kell venni, hogy az adott szervezetnél a belső ellenőrzés fel van-e készülve az ilyen ellenőrzési feladatok végrehajtására. Amennyiben nincs, akkor kiegészítésképen javaslatot kell készíteni a belső ellenőrzési szervezet kiegészítésére, illetve az ott dolgozók szakmai követelményeire.

⇒ A biztonsági belső ellenőröknek, a következőknek kell eleget tenniük:

- A vagyonbiztonsági ellenőrnek vagyonbiztonsági képesítéssel kell rendelkeznie,
- Az informatikai biztonsági ellenőrnek informatikai képzettséggel, és informatikai biztonsági ismeretekkel kell rendelkeznie, valamint előnyös, ha van okleveles információ-rendszer ellenőr vizsgája (CISA), illetve 2003-tól mód van Okleveles Informatikai Biztonsági Menedzser oklevelet megszerezni (CISM, CERTIFIED INFORMATION SECURITY MANAGER).

⇒ Figyelembe kell venni az ISO/IEC 17799 szabvány előírásait az IR auditálásnál. Éspedig:

- Az auditálási követelményekről meg kell egyezni a menedzsmenttel
- Az ellenőrzés tárgyáról meg kell állapodni, és azt ellenőrizni kell.
- Az ellenőrzésnek korlátozva kell lennie a szoftver és az adatok vonatkozásában csak az olvasásra.
- Hozzáférés nem csak olvasásra, csak a rendszer fileok elszigetelt másolására megengedett, és a másolatokat az audit után törölni kell.
- Azokat az IT erőforrásokat, amelyek szükségesek az ellenőrzéshez azonosítani kell, és rendelkezésre kell bocsátani.
- A speciális követelményekről meg kell állapodni, és azonosítani kell azokat.
- Minden hozzáférést nyomon kell követni, és naplózni kell.
- Minden folyamatot, követelményt és felelősséget dokumentálni kell.

⇒ A jogszabályi megfelelősséget vizsgálni kell

- Az üzleti és az IT mgm felügyelete, és
- A belső ellenőrzések alapján is.

9. A MÓDSZERTAN FELÉPÍTÉSE ÉS TARTALMA

9.1. AZ ELLENŐRZÉS CÉLJA

A biztonság belső ellenőrzése annak az ellenőrzése, hogy a Biztonsági Politika, a Katasztrófaterv, és a Biztonsági Szabályzat, illetve a gyakorlat elfogadható biztosítékot nyújtanak-e az üzleti cél megvalósítására, az üzleti, és informatikai folyamatokban a nem kívánt események megelőzésére, jelzésére, és kijavítására, a kockázatok csökkentésére (mind az ÜR, mind IR-ben).

9.2. AZ ELLENŐRZÉS MÓDSZERE

Az ellenőrzést a következők szerint kell végrehajtani:

9.2.1. A megfelelősség vizsgálata

A megfelelősség vizsgálata azt jelenti, hogy

1. *a védelmi intézkedéseknek meg kell felelniük*
   - ⇒ a legjobb gyakorlatot képviselő COBIT 4.1, és MSZ-ISO/IEC 17799. szabványnak.
   - ⇒ az adott időpontban hatályos jogszabályoknak. Az **alapvető** jogszabályok:
     - **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 199. Évi LXVI. tv.*
       - *az üzleti titok a Büntető törvénykönyvről szóló 1978. évi IV. tv.-ben*
       - *a szellemi tulajdonjogok védelméről szóló jogszabályoknak*
     - **A pénzintézetekkel kapcsolatos jogszabályok:**
       - a banktitok meghatározása a hitelintézetekről és pénzintézeti vállalkozásokról szóló 1996. CXII. tv.- ben, illetve a 2000. évi módosításnak.
       - 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 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.
- **A humán biztonság** egyes kérdéseivel foglalkozó 2005. évi CXXXIII. tv.
- **Fizikai biztonság** egyes kérdéseivel foglalkozó
  - A MABISZ által kiadott biztosítási feltételek.
  - A személy, és vagyonvédelemről szóló 2005. évi CXXXIII. Tv.
- **Logikai biztonság** *egyes kérdéseivel foglalkozó biztonság értékelési kritériumoknak (mint ISOIEC 15408-1, 2, 3,).*

⇒ a belső szabályzatoknak, éspedig (itt a belső szabályzatokat, illetve utasításokat kell felsorolni):

⇒ a biztonsági szabványoknak.

2. A menedzsment, és az alkalmazottak magatartás módjának, meg kell felelniük az etikai értékeknek, amelyeket az adott szakma állít eléjük.
   D. Bell (2006) azt írja: a megfelelősség azt jelenti, hogy munkánkban, és életünkben megtesszük, amit jogilag tenni kell, míg az etikai értékek azokat a teendőket jelentik, amelyeket erkölcsileg kötelező tenni.

Megjelent magyar szabványok (amelyeket figyelembe vettünk)::

- MSZ ISO/IEC 9594-8-2004 Informatika. Nyílt rendszerek összekapcsolása.
- MSZ ISO/IEC 15408-1,2,3 Az informatikai biztonság értékelésének közös rendszere.
- MSZ ISO/IEC 17700-1 Biztonságtechnika, kulcsgondozás.
- MSZ-ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények
- MSZISO/IEC 17799 Informatikai biztonság menedzselésének eljárás rendje.
- MSZ E- 15100-1 Informatikai szolgáltatás irányítása

Az alábbiakban néhány külföldi, illetve nemzetközi biztonsági szabványt példaképen megadunk:

- 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..
- *ISO/IEC 17799 Code of practice for information Security Management*
- *ISO/IEC 27001: 2005 Information Security Management-Requirements*
- *MSZ-ISO/IEC 17799:2005 Informatikai biztonság Menedzsment*
- *RBAC Protection Profile, Version 0,2 Draft: Dec, 19, 1997: (http://csrc.gov!cc/pp/pplist/htm)*
- *Information Technology Security Evaluation Criteria*
- *Trusted Computer System Evaluation Criteria*
- Common Criteria for Information Security Evaluation Criteria 2.1

- Magyar Szabvány: MSZ 17128: Távközlőhálózatok és távközlési szolgáltatások védettsége
- *ITU -T recommendation X.200: Open System Interconnection – Basic Reference Model: The Basic Model (azonos az ISO/IEC 7498-1 szabvánnyal)*
- *IITU -T (CCITT) Recommendation X.800: Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications: Security Architecture for Open Systems Interconnection for CCITT Applications. Technikailag megegyezik az ISO 7498-2 (Information processing systems – Open systems interconnection – Basic Reference Model – Part 2: Security architecture) szabvánnyal.*
- *Kiegészítés az ITU-T X.800 ajánlásához: Amendement 1: Layer Two Security Service and Mechanism for LANs*
- *FIPS Special Publication 500-157, Smart Card Technology: New Methods for Computer Access Control.*
- *FIPS Special Publication 800-2, Public Key Cryptography.*
- *FIPSPUB46-2 DATA ENCRYPTION STANDARD (DES), 1998*
- *FIPSPUB48 GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTI FICATION, 1977*
- *FIPSPUB73 GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS, 1980*
- *FIPSPUB81 DES MODES OF OPERATION -- 1980*
- *FIPSPUB83 GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL, 1980*
- *FIPSPUB87 GUIDELINES FOR ADP CONTINGENCY PLANNING, 1981*
- *FIPSPUB112 PASSWORD USAGE, 1985*
- *FIPSPUB113 COMPUTER DATA AUTHENTICATION, 1985*
- *FIPSPUB140-2 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 2000*
- *FIPSPUB171 KEY MANAGEMENT USING ANSI X9.17, 1992*
- *FIPSPUB180-1 SECURE HASH STANDARD (SHS), 1995*
- *FIPSPUB181 AUTOMATED PASSWORD GENERATOR (APG), 1993*
- *FIPSPUB185 ESCROWED ENCRYPTION STANDARD (EES), 1994*
- *FIPSPUB186-1 DIGITAL SIGNATURE STANDARD (DSS), 1998*
- *FIPSPUB190 GUIDELINE FOR THE USE OF ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES, 1994*
- *FIPSPUB191GUIDELINE FOR THE ANALYSIS OF LOCAL AREA NETWORK SECURITY, 1994*
- *FIPSPUB 196 ENTITY AUTHENTICATION USING PUBLIC KEY CRYPTOGRAPHY, 1997*

A megfelelősség vizsgálatának nehézségét képezi, hogy lényegében hazai jogszabályok, szabványok, az esetek többségében nem állnak rendelkezésre. Lásd a helyzetet összefoglaló ábrát (Mivel kell védeni?). Természetesen a megfelelősséget a Biztonsági Politikában, a Katasztrófatervben, és a Biztonsági Szabályzatban már

érvényesíteni kellett. A biztonsági dokumentumoknak azonban tartalmazni kell az érvényesített jogszabályokat, utasításokat, szabványokat. Ez azonban a belső ellenőrt nem menti fel az érvényesítendő jogszabályok ismeretétől.

A legújabb ISO biztonsági szabvány család:

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
- ISO/IEC 27001 — Information security management systems — Requirements. The older ISO/IEC 27001:2005 standard relied on the Plan-Do-Check-Act cycle; the newer ISO/IEC 27001:2013 does not, but has been updated in other ways to reflect changes in technologies and in how organisations manage information.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)

9.2.2. A megvalósulás ellenőrzése

A megvalósulás vizsgálata azt jelenti, hogy vizsgálni kell a védelmi intézkedések alkalmazási gyakorlata kikényszeríti-e a biztonsági követelményeket. Az ellenőrzésnek fel kell tárnia minden eltérést a Biztonsági Politikában, Katasztrófatervben, és a Biztonsági Szabályzatban meghatározottaktól.

9.2.3. A belső ellenőrzés értékelése

A belső ellenőrzést rendszeresen értékelni kell, és az értékelésből le kell vonni a megteendő intézkedésekre vonatkozó következtetéseket. A COBIT 4 [55], a 214 kontroll cél helyzetének értékelésére alkalmazza az érettségi modellt. Hasonlóképpen megadja a belső ellenőrzés érettségi modelljét is. (lásd II. kötet. 10.4. pont). A belső ellenőrzés értékelését általában külső független auditorral végeztetik el.

9.2.4. A védelmi gyengeségek feltárása

Az előző két pont szerinti vizsgálatok eredménye a gyengeségek feltárása.

9.2.5. Javaslat a teendőkre

A gyengeségek kiküszöbölésére a belső ellenőrzésnek intézkedéseket kell javasolni.

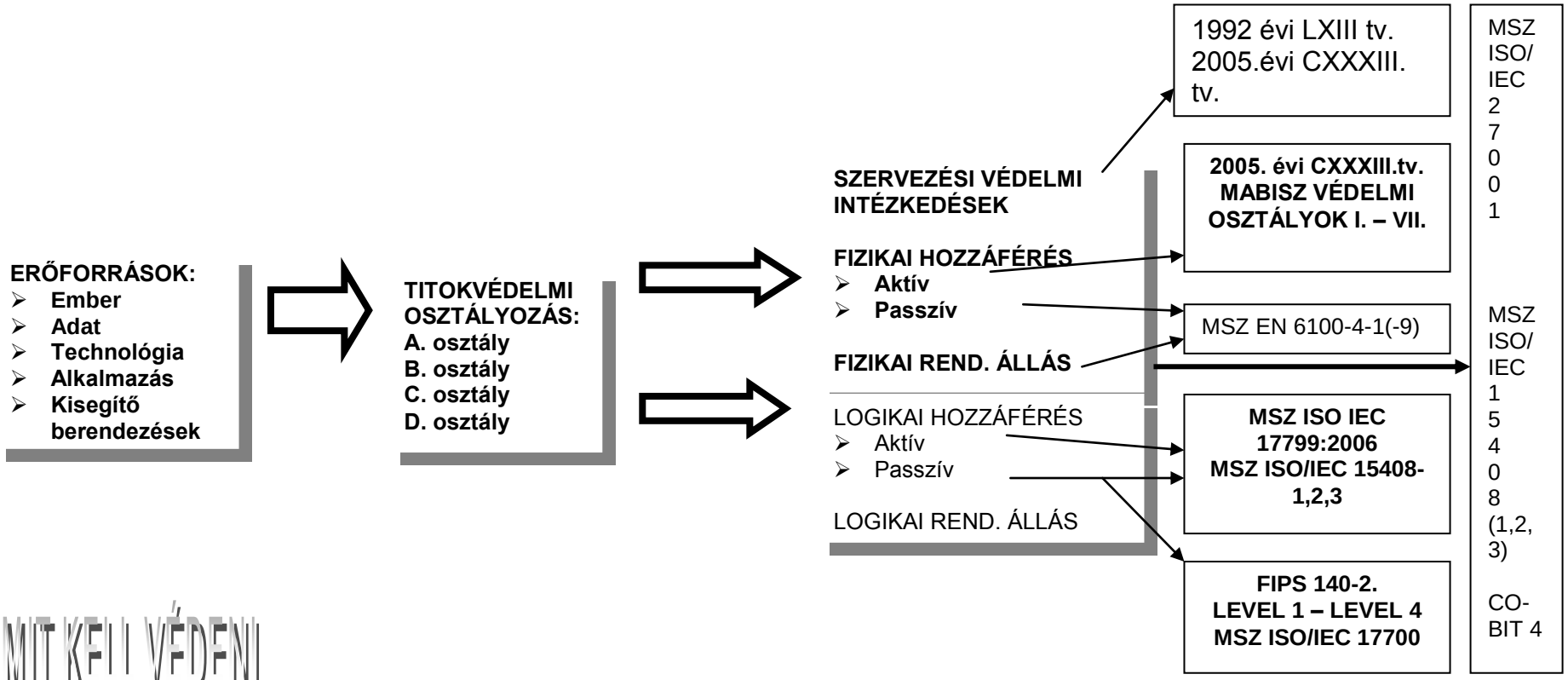
9.3. AZ ELLENŐRZÉS TÁRGYA

Ebben a pontban esetenként a belső ellenőrzés tárgyát kell megadni, amelyet a belső ellenőrzési vizsgálat elrendelésére jogosult határozhat meg. A biztonsági belső ellenőrzés a vállalat teljes területére, az érték, és/vagy az információ-rendszerre terjedhet ki, azaz lehet

- ⇒ *a teljes biztonsági rendszer,*
- ⇒ *egy alrendszer része, például*
  - *a szervezési biztonság,*
  - *a fizikai hozzáférés-védelem,*
  - *a logikai hozzáférés-védelem,*
  - *a fizikai rendelkezésre állás,*
  - *a logikai rendelkezésre állás,*
  - *a Katasztrófatervben specifikált védelmi intézkedések (például a felkészülési fázis),*
  - *a biztonsági dokumentumokban (Biztonsági Politika, Katasztrófaterv, Biztonsági Szabályzat) foglaltak végrehajtása,*
  - *a biztonsági dokumentumok karbantartása,*
  - *a biztonsági dokumentumok oktatása vagy*
- ⇒ *egy üzleti folyamat biztonsági problémái*
- ⇒ *egy védelmi intézkedésre irányuló célvizsgálat.*

A belső ellenőrzést alapvetően befolyásolja a következő öt téma:

- A menedzsment viszonya a belső ellenőrzéshez,
- A kockázatok felismerése, és értékelése,
- Az ellenőrzési tevékenységek, és feladatok szétválasztása a belső ellenőrzés területén,
- A belső tájékoztatási rendszer, és a gyengeségek kijavítása,
- A belső ellenőrzés rendszeres értékelése.


ERŐFORRÁSOK:
Ember
Adat
Technológia
Alkalmazás
Kisegítő berendezések
TITOKVÉDELMI OSZTÁLYOZÁS:
A. osztály
B. osztály
C. osztály
D. osztály
SZERVEZÉSI VÉDELMI INTÉZKEDÉSEK
FIZIKAI HOZZÁFÉRÉS
Aktív
Passzív
FIZIKAI REND. ÁLLÁS
LOGIKAI HOZZÁFÉRÉS
Aktív
Passzív
LOGIKAI REND. ÁLLÁS
1992 évi LXIII tv.
2005.évi CXXXIII. tv.
2005. évi CXXXIII.tv. MABISZ VÉDELMI OSZTÁLYOK I. – VII.
MSZ EN 6100-4-1(-9)
MSZ ISO IEC 17799:2006
MSZ ISO/IEC 15408-1,2,3
FIPS 140-2.
LEVEL 1 – LEVEL 4
MSZ ISO/IEC 17700
MSZ ISO/ IEC 27001
MSZ ISO/ IEC 15408 (1,2, 3)
CO-BIT 4
MIT KELL VÉDENI
MENNYIRE KELL VÉDENI
MIVEL KELL VÉDENI

9.4. AZ ELLENŐRZÉS VÉGREHAJTÓI

9.4.1. A biztonság belső ellenőrzésének helye a vállalati szervezetben

A biztonság belső ellenőrzését a vállalat belső ellenőrzésének szervezetében, és működésében szükséges szervezetileg elhelyezni.

9.4.2. Belső ellenőrzés

A belső ellenőrzést a vállalat saját belső ellenőrzési munkatársai hajtják végre.

9.4.3. Külső ellenőrzés

Mindazokban az esetekben, amikor egy speciális probléma merül fel külső szakértőt célszerű igénybe venni. Ilyen igény merülhet fel, például az elektromágneses kompatibilitás, a rejtjelezés, vagy például a tartalomhitelesítés területén. Továbbá indokolt legalább háromévenként független, külső szakértőkkel a biztonsági rendszert auditáltatni.

9.4.4. A belső ellenőr követelményei

A biztonsági belső ellenőrnek a következő követelményeknek kell eleget tenni-e

- A vizsgált területtől, és a biztonsági termékek forgalmazóitól függetlennek kell lennie.
- Rendelkeznie kell szakmai kompetenciával.
- A feladatának, szerepének, és felelőségének dokumentumban kell rögzítve lennie, általában, és a konkrét vizsgálatra nézve.
- A vizsgálatot költség hatékonyan, határidőre, minőségileg jól, és megfelelően dokumentálva kell elvégeznie.
- Rendelkeznie kell a vizsgálat idejére a szükséges fizikai, és logikai hozzáférési jogosultságokkal.

9.5. AZ ELLENŐRZÉSI TERV

9.5.1. Az ellenőrzési terv összeállítása

Az ellenőrzési tervet évente kell elkészíteni, úgy hogy legalább kétévenként a biztonsági rendszer minden része ellenőrzésre kerüljön. Célszerű háromévente külső, független szervezettel auditáltatni a biztonságot. A biztonsági ellenőrzés lehet

- ⇒ megelőző, amennyiben nincs más ok, csak a rendszeres ellenőrzés szükségességének felismerése
- ⇒ feltáró, amennyiben biztonsági esemény történt, és

⇒ javító célzatú, amennyiben már ismert a védelmi gyengeség, és annak a megszüntetése kívánatos.

9.5.2. Az ellenőrzési feladatok

⇒ Folyamatos ellenőrzési feladat

A folyamatos ellenőrzési feladat a fizikai, és a logikai hozzáférés-védelem által készített naplók értékelése alapján készült havi jelentéseknek, valamint az egyéb vagyon, és informatikai biztonsági események jelentéseinek feldolgozása, amely feltáró *jellegű ellenőrzés.*

⇒ Terv szerinti ellenőrzési feladat

Az éves ellenőrzési terv alapján, amely *megelőző* jellegű ellenőrzés.

⇒ Célvizsgálat

A célvizsgálat (eseti vizsgálat) lehet a biztonság egy területének részletes ellenőrzése, például a vagyonbiztonság, illetve az informatikai biztonságon belül a szervezési vagy a technikai biztonság, amely feltáró *és/vagy* javító *jellegű.*

9.6. AZ ELLENŐRZÉS VÉGREHAJTÁSA

9.6.1. Az ellenőrzés végrehajtásának fázisai

***1.fázis*. a felkészülés,**

⇒ ***Az ellenőrzés tárgyának a meghatározása***

Az ellenőrzés tárgyát a belső ellenőrzés számára vezetői utasítás adja meg.

⇒ ***Az ellenőrzési lista összeállítása***

Az ellenőrzést megelőzően össze kell állítani az ellenőrzés tárgyának megfelelő vizsgálati szempontokat, az ellenőrzési listát. A listát a Biztonsági politikában, és a Katasztrófa Tervben szereplő védelmi intézkedések, illetve a Biztonsági Szabályzat az ellenőrzés tárgyát képező pontjai alapján lehet összeállítani.

Például az ellenőrzés tárgya : *a logikai hozzáférés védelem.*

Az ellenőrzési lista vázlata:

- *Aktív támadás elleni hozzáférés-védelem*
  - *Jelszó rendszer (a Biztonsági Politika e pontjában specifikált védelmi intézkedések, és a Biztonsági Szabályzat vonatkozó pontjai)*
  - *Jogosultsági rendszer (a Biztonsági Politika e pontjában specifikált védelmi intézkedések, és a Biztonsági Szabályzat vonatkozó pontjai),*
  - *Tartalmi hitelesség-védelem (a Biztonsági Politika e pontjában specifikált védelmi intézkedések, és a Biztonsági Szabályzat vonatkozó pontjai),*

- *Time out eljárás (a Biztonsági Politika e pontjában specifikált védelmi intézkedések, és a Biztonsági Szabályzat vonatkozó pontjai),*
- *Passzív támadás elleni hozzáférés-védelem (a Biztonsági Politika e pontjában specifikált védelmi intézkedések, és a Biztonsági Szabályzat vonatkozó pontjai).*

⇒ ***Az ellenőrzés végrehajtóinak listája***

Meg kell adni azokat a belső munkatársakat, és esetleg külső felkért szakértőket, akik az ellenőrzést végrehajtják.

⇒ ***Az interjú alanyok listájának összeállítása***

A listán a védelmi intézkedést üzemeltető érintett terület vezetője, és munkatársai, valamint a felhasználók (minta vétel elve alapján néhány) szerepeljenek.

⇒ ***A tanulmányozandó dokumentumok listájának összeállítása***

A Biztonsági politikában, a Katasztrófatervben, és a Biztonsági Szabályzatban hivatkozott dokumentumok, illetve jogszabályok (esetleg azok módosításai) kell, hogy szerepeljenek e listán.

⇒ ***A szemlék listájának összeállítása***

Szemléket az ellenőrzés tárgyát képező védelmi intézkedések üzemeltetési helyszínein kell tervezni.

⇒ ***A tesztek listájának összeállítása***

Tesztet a védelmi intézkedés tényleges működésének feltárása érdekében célszerű végezni.

2. fázis: ***a valóság feltárása,***

Az ellenőrzés az 1.fázisban megadott ellenőrzési lista alapján történik.

3.fázis. **a követelmények, és a gyakorlat összehasonlítása**

Azt kell vizsgálni, hogy a működő védelmi intézkedés megfelel-e követelményeknek, és a specifikációnak (lásd Biztonsági Politika, Katasztrófaterv), és a gyakorlat, az üzemeltetés kikényszeríti-e a biztonsági követelményeket.
A védelmi intézkedések üzemeltetése alatt a védelmi intézkedés

⇒ *működtetését vagy végrehajtását,*
⇒ *felhasználását, és*
⇒ *karbantartását értjük.*

Értelemszerűen az egyes védelmi intézkedések üzemeltetésének szabályozásánál mind a hárommal foglalkozni kell. A szervezési védelmi intézkedéseknél, mivel azok utasítás formájában realizálódnak végrehajtásról, míg a technikai védelmi intézkedéseknél működtetésről lehet szó. A technikai védelmi intézkedések egy

része azonban nem igényel működtetést, de karbantartást viszont igen (például Faraday háló vagy egy helyiség speciális falazata).

***4.fázis*. a szükséges teendőkre javaslat készítése,**

A szükséges teendők lehetnek új, célzott helyzetfeltárás vagy biztonsági dokumentumok módosítása vagy vezetői intézkedés (pl. fegyelmi eljárás) kezdeményezése.

***5.fázis.* az ellenőrzési jelentés összeállítása**

Az ellenőrzési jelentést, a 7.8. pontban megadottak szerint, és a dokumentált tényekre támaszkodva kell elkészíteni.

9.7. AZ ELLENŐRZÉS KRITIKUS PONTJAI

⇒ Függetlenség

A belső ellenőrzés végrehajtóinak a vizsgált területtől független személyeknek kell lenniük.

⇒ Kompetencia

Az ellenőrzést szakmailag megfelelően felkészült személyeknek kell végeznie.

⇒ Dokumentáltság

Az ellenőrzés teljes folyamatát dokumentálni kell.

9.8. A SARBANES-OXLEY TV. ÉS AZ EU 8.SZ- DIREKTÍVA

A Sarbanes-Oxley USA tv. és az annak alapján megjelent EU 8. sz Direktíva több olyan követelményt tartalmaz, amelynek biztonsági vonatkozásai vannak, ezeket figyelembe kell venni.
Ilyen például:

- ⇒ A belső ellenőrzés megerősítése
- ⇒ A belső ellenőrzés, és az auditorok függetlensége, etikus magatartása.
- ⇒ A számon kérhetőség, és a valódiság (sértetlenség) következetes biztosítása
- ⇒ Az Igazgatóság éves vállalati helyzetértékelési kötelezettsége, amelyben a biztonsági helyzet értékelésének is benne kell lennie.
- ⇒ A pénzügyi rendszerben biztosítani kell a valódiságot, az adatok, alkalmazások sértetlenségét, a biztonság érzékenység alapján meghatározott védelmet.

9.9. A BASEL II.

A Basel Committee on Banking Supervision (BCBS, a BIS mellett működő szervezet) 2003-ban kiadta a BASEL II.-t [56, 57], amely a pénzügyi szervezetekben, és kereskedelmi vállalkozásokban a tőke

megfeleléssel, az ehhez szükséges méréssel, és szabályaival, valamint az ezzel kapcsolatosan jelentkező kockázatok menedzsmentjével foglalkozik [lásd 42-ben]. Az anyag az alábbi fejezetekből áll:

1. Az alkalmazás területei. (A Basel II. alkalmazási kérdéseivel a [44] foglalkozik).
2. A tőke megfelelősség mérésének három pillére

⇒ *Minimális tőke követelmények* (itt foglalkozik például a hitelezési, és ennek kapcsán a működési kockázatokkal). A kockázatok bekövetkezésük esetén kárkövetkezménnyel, veszteséggel, adott esetben a bank működésének megrendülésével járhatnak.

⇒ Felügyeleti vizsgálati, átvilágítási folyamat. (Itt foglalkozik a belső ellenőrzést is érintő ellenőrzési folyamatokkal).

⇒ A piaci fegyelem.(Itt foglalkozik például a piaci követelményekkel, kockázatokkal).

A BASEL II. a banküzleti folyamatokra vonatkozik, és gyakorlatilag minden fejezetben foglalkozik az adott fejezetben tárgyaltak működési kockázataival is. Ugyanakkor a bankbiztonsági kockázatok szintén a működési kockázatokhoz tartoznak, és egy kockázat bekövetkezése esetén veszteség, azaz kárkövetkezmény képződik. Az üzleti folyamatok, és az azokat kiszolgáló informatikai folyamatok, az üzleti cél rendeltetésszerű megvalósítása, pedig kölcsönhatásban van a biztonsági kockázatokkal, követelményekkel.

Az informatikának, amely kiszolgálja a bankok üzleti tevékenységét (ezen belül például a hitelezést), biztosítania kell a hitelezéssel összefüggő adatok valódiságát, sértetlenségét, rendelkezésre állását, valamint az ezekkel végzett műveletek számon kérhetőségét. Ezeknek a nem megfelelő vagy gyenge védelme, biztosítása jelentősen megnövelheti a működési, és konkrétan a hitelezési kockázatokat, amelyek --- mint említettük --- a bank működésének megrendülését okozhatják.

9.10. ELŐZMÉNYEK RENDELKEZÉSRE ÁLLÁSA

A Biztonsági Politikának, a Katasztrófatervnek, és a Biztonsági Szabályzatnak kell rendelkezésre állnia, valamint a biztonsági eseményekkel kapcsolatos, a vizsgált időszakra vonatkozó jelentéseknek. Továbbá amennyiben korábban volt már belső vagy külső ellenőrzés, a vonatkozó jelentésnek is.

9.11. AZ ELLENŐRZÉSI JELENTÉS TARTALMA

9.11.1. Az ellenőrzés tárgya

Az ellenőrzés a jogosult vezető utasítása alapján történhet, amelynek meg kell határoznia az ellenőrzés tárgyát. Ilyen utasítás lehet eseti vagy maga az éves terv.

9.11.2. Az ellenőrzés módszere

A7.2. pont alapján kell megadni.

9.11.3. Az ellenőrzés végrehajtói

A 7.4. pont alapján kell az ellenőrzésben résztvevőket megadni.

9.11.4. Az ellenőrzés megállapításai

9.11.4.1. Feltárt gyengeségek

A feltárt gyengeségeket tárgyilagosan és jól dokumentálva kell megadni, a vizsgálat tárgyából következő tagolásban. Például a logikai hozzáférés-védelem vizsgálata esetében

- ⇒ *Aktív támadás elleni hozzáférés-védelem gyengeségei*
  - *Jelszó rendszer*
  - *Jogosultsági rendszer*
  - *Tartalmi hitelesség-védelem*
  - *Time out eljárás*
- ⇒ *Passzív támadás elleni hozzáférés-védelem gyengeségei*

9.11.4.2. A vizsgált terület minősítése

A vizsgált területet a feltárt gyengeségek alapján minősíteni kell, a COBIT 4.1 a 34 IT folyamathoz megadott érettségi modellt felhasználva. Az értékelés lehet

- ⇒ nincs feltárt gyengeség,
- ⇒ a megfelelősség vonatkozásában van feltárt gyengeség, és/vagy
- ⇒ a megvalósulás vonatkozásában van feltárt gyengeség.

Az ellenőrzési módszereknek az ellenőrzés során felmerült gyengeségeit, és az ellenőrzést akadályozó tényeket a jelentésben szerepeltetni kell.

9.11.5. Javasolt intézkedések

A javasolt intézkedéseknek a védelmi intézkedések erősítésére, a Biztonsági Politika, a Katasztrófaterv, és a Biztonsági Szabályzat módosítására, illetve ha szükséges vezetői fegyelmi intézkedésre kell vonatkozniuk.

9.11.6. A biztonsági átvilágítás alapelvei

Az átvilágítás szempontjait magas szinten, beleértve az informatikai biztonsági átvilágítást is, a COBIT3 tartalmazza. A biztonsági átvilágítás készítőinek célszerű világosan látni, hogy az informatikai biztonsági átvilágítás az információ-rendszer, a vállalat általános átvilágításának részét képezi. Ebből azonban nem következik, hogy nem lehet külön végrehajtani. Az ISACA kiadványa, a CISA REVUE 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 folyamatokba (üzleti, informatikai) implementált kontroll folyamtokkal érendő el.
- ⇒ *A kontroll célja lehet általában:*
  - 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.

9.11.7. Hivatkozások

9.11.7.1. Interjú alanyok listája

9.11.7.2. Tanulmányozott dokumentumok listája

9.11.7.3. Szemlék listája

9.11.7.4. Végrehajtott tesztek listája

9.12. AZ ELLENŐZÉS ERŐFORRÁSAINAK VÉDELME

Az MSZ-ISO/IEC 17799-es szabvány szerint azokat az erőforrásokat, amelyeket az audit, a belső vagy külső ellenőrzés alkalmaz (például: Cumputer Assisted Audit Techniques, CAATs, számítógéppel támogatott audit technika, amely egy ellenőrzéshez alkalmazható sw..) elkülönülten, kell kezelni, és gondoskodni kell a védelmükről. Ezenkívül, biztosítani kell, hogy az ellenőrzés erőforrásai jogosulatlan tevékenységre ne legyenek felhasználhatóak, azaz az információs rendszerünket is védeni kell, az audit során esetleg végrehajtható támadásoktól.
A gyakorlatban ez azt jelenti, hogy

- Az ellenőrök csak olvasásra kaphatnak hozzáférési jogosultságot.
- Az ellenőrök minden tevékenységét naplózni, majd ellenőrizni kell.
- Az audit, az ellenőrzés erőforrásaihoz, csak igen korlátozott számban adható hozzáférési jogosultság.

9.13. MONITORING

A COBIT 4.1 a magas szintű ellenőrzési szempontok között egy külön fejezetet szentel a monitoringnak (monitorizás).
A monitorozás (monitoring) a folyamatok folyamatos felügyelete, amelynek célja az üzleti követelmények, a teljesítmények teljesítésének biztosítása. A biztonsági monitorozás célja védelmi intézkedések nyomon követése, felügyelete, a belső, és külső független ellenőrzések (vizsgálatok) rendeltetésszerű végrehajtásának és hatásának ellenőrzése, illetve szükségességüknek felvetése. Az MSZ ISO/IEC 17799-es szabvány (9.7 pont) azt emeli ki, hogy biztosítani kell elsősorban a hozzáférés védelemmel kapcsolatban a folyamatos megfigyelést a biztonsági események elkerülése érdekében. Ebből a szempontból a naplózás jelent komolyan veendő feladatokat. Természetesen a megfigyelendők között vannak a biztonsági események is, annak érdekében, hogy azok értékeléséhez anyagot szolgáltassunk, és tegyünk újabb bekövetkezésük ellen.

Az ISMS tartalmazza, mindenütt azokat a teendőket, amelyek a biztonság minitorozását szolgálják (habár ez nincs kihangsúlyozva ezeken a helyeken).

10. BIZTONSÁGI PROGRAM (AKCIÓ TERV)

10.1. A PROGRAM CÉLJA ÉS TÁRGYA

Az IT Biztonsági Program (AKCIÓ TERV) célja, hogy a Kockázatmenedzsmentre, Biztonsági Politikában (Szabályzatban), az Üzletmenet Folytonossági Tervben specifikált védelmi intézkedések tervezésére, fejlesztésére/beszerzésre, üzemeltetésére, ellenőrzésére egy megvalósítási, napra készen tartási tervet határozzon meg (COBIT 4 alapján).
A biztonsági program tárgya a biztonsági rendszer (egy ISMS,MSZ ISO/IEC 27001) létrehozását biztosító intézkedések megvalósításnak terve, vagy egy a kockázat menedzsment körében feltárt új kockázat csökkentésének figyelembevételével, új intézkedéseknek a megvalósítási terve.

10.2. A PROGRAM KÉSZÍTÉSE

A program a vagyon, és az IT biztonságra egyaránt vonatkozik, és kiterjed a már működő biztonsági rendszer esetében, egy ellenőrzés, kockázat elemzés, vagy biztonsági esemény miatt, a szabályozások (Biztonsági Politika és/vagy Szabályzat, ÜFT), szükségessé váló módosítási feladataira is.

A program készítésekor meg kell találni az összhangot a biztonság követelmények, és pénzügyi lehetőségek között. Ezért a készítés során a biztonsági menedzsernek (a program készítéséért felelős vezetőnek) egyeztetnie kell a pénzügyekért felelős vezetővel. A program elemei:

- Tervezés (PLAN), a biztonságszervezés lépéseinek dokumentumai,
- Végrehajtás (DO), a biztonságszervezés végrehajtása,
- Ellenőrzés (CHECK),
- Beavatkozás (ACT), a biztonsági esemény vagy az ellenőrzés igényelte intézkedések megtétele.

Természetesen az IT menedzserrel is össze kell hangolni a fejlesztési/beszerzési célokat, feladatokat érintő biztonsági intézkedéseket.

A programnak biztosítani kell a számon kérhetőséget:

- A védelmi intézkedések üzemeltetésért felelősök felelősségét,
- A folyamatok (alkalmazások) tulajdonosainak felelősségét,
- A kockázat menedzsment folyamatosságát,
- A feltárt veszélyforrások figyelembe vételét a Program karbantartásánál,
- Az IT menedzsernek a program megvalósítás biztosításához a szállítók, fejlesztők, üzemeltetők, konzultánsok rendelkezésre állását.

10.3. A PROGRAM SIKER TÉNYEZŐI

Az ISACA kidolgozta a „Biztonsági Program Sikerének Kritikus Elemeit”, [59]. Ezek a következő két csoportra lettek osztva:

10.3.1. AZ ELSŐDLEGES KRITIKUS ELEMEK

- A felső vezetés kötelezettsége a az IT irányelvek meghatározásra.
- Az IT biztonság megértése a menedzsment részéről.
- Az IT biztonság tervezése előbb történjen , mint a az új technológia implementálása
- Az üzleti (vagyon, fizikai), és IT biztonság integrációja
- Az IT biztonság elkötelezettsége a szervezeti célokkal
- A felső vezetés, és a menedzsment tulajdonossága, és számon kérhetősége az IT biztonság implementálására, monitorozásra, ellenőrzésére, jelentésére.

10.3.2. A KIEGÉSZÍTŐ KRITIKUS ELEMEK

- A munkavállalók megfelelő oktatása, és tudatossága az IT erőforrások védelmére
- Az IT Biztonsági Politika, szabványok következetes érvényesítése
- Az IT biztonság helye a szervezeti hierarchiában
- Az IT Biztonsági Stratégia, és taktika költség kerete
- A bord, és a végrehajtók az IT prioritásokra vonatkozó következetes állásfoglalásai
- A rövid távú célokra koncentrálás, a hosszú távú ellenőrzések gyengeségeit eredményezi
- AZ IT biztonság indoklásának képessége
- Az IT biztonság legjobb gyakorlata, és a mérésének általános elfogadottsága.

11. .A BIZTONSÁGI PROGRAM FELÉPÍTÉSE

11.1.1. A program célja

11.1.2. A program tárgya

11.1.3. A program (PLAN, DO, CHECK, ACT)

- Tervezés
  - ⇒ A feladat (Biztonsági Átvilágítás, Biztonsági Politika és/vagy Biztonsági Szabályzat, Üzletmenet Folytonossági Terv, Biztonsági Kultúra Program kidolgozás)
  - ⇒ Végrehajtás
  - ⇒ Felelős (munkakör)
  - ⇒ Határidő
  - Költség igény
- Megvalósítás
  - ⇒ A feladat (Szervezési: intézkedés, Technikai: fejlesztés/beszerzés, átadás/átvétel, üzemeltetés)
  - ⇒ Végrehajtás
  - ⇒ Felelős (munkakör)
  - ⇒ Határidő
  - ⇒ Költség igény
- Ellenőrzés
  - ⇒ A feladat (belső, külső ellenőrzés)
  - ⇒ Végrehajtás
  - ⇒ Felelős (munkakör)
  - ⇒ Határidő
  - ⇒ Költség igény
- Intézkedés (értékelés alapján a szükséges intézkedés)
  - ⇒ A feladat
  - ⇒ Végrehajtás
  - ⇒ Felelős (munkakör)
  - ⇒ Határidő
  - ⇒ Költség igény

11.1.4. A felelősök, végrehajtók jelentési kötelezettségei

11.1.5. Az ellenőrzés

- A program készítés ellenőrzése
- A program végrehajtás ellenőrzése
- A programkarbantartás ellenőrzése

12. MELLÉKLETEK

12.1. A CC, A TCSEC, ÉS AZ ITSEC ÖSSZEHASONLÍTÁSA

Az alábbiakban megadjuk a CC, TCSEC, és ITSEC garanciális szintjeinek, és funkcionális osztályainak összehasonlítását. Megjegyezzük, hogy egzakt azonosságot nem lehet kimutatni közöttük .Időközben megjelent a CC 2.1 Magyar szabvány ként is. MSZ ISO/IEC 15408 1-3 kötet.

A funkcionális osztályok összehasonlítása:

CC	TCSEC, ITSEC
AudIt (FAU)	Audit
Communication (FCO)	Data Exchange
User Data Protection (FCS)	Access Control Accuracy Object Reuse
Privacy (FPR)	
Identification and Authentication (FIA)	Idenfication and Authentication
Protections of Trusted Security Functions (FPT)	
Resource Utilisation (FRU)	Realibility of Service
TOE Access (FTA)	Access Control
Cryptographic Support (FCS)	
Security Management (FMT)	
Trusted Path/Channels (FTP)	Access Control Data Exchange

A garanciális szintek összehasonlítása:

CC	TCSEC	ITSEC
EAL0	**D**	**E0**
EAL1		
EAL2	**C1**	**E1**
EAL3	**C2**	**E2**
EAL4	**B1**	**E3**
EAL5	**B2**	**E4**
EAL6	**B3**	**E5**
EAL7	**A1**	**E6**

12.2. COBIT 4.1

12.2.1. A COBIT 4.1.ÉRETTSÉGI MODELL A BELSŐ ELLENŐRZÉSRE

ÉRETT-SÉGI SZINT	A BELSŐ ELLENŐRZÉSI KÖRNYEZET ÁLLAPOTA	A BELSŐ ELLENŐRZÉSEK MEGÁLLAPÍTÁSAI
0 Nem létező	A belső ellenőrzés szükségessége nem felismert. Az ellenőrzés nem része a szervezeti kultúrának, küldetésnek. Magas kockázata van a belső ellenőrzés hiányosságainak,, és az eseményeknek.	Nincs szándék a belső ellenőrzés szükségességének meghatározására. Az eseményekkel úgy foglalkoznak, amint azok felmerülnek.
1 Kezdeti/ Ad hoc	Néhány vonatkozásban felismert a belső ellenőrzés szükségessége. A kockázati, és ellenőrzési követelmények megközelítése ad hoc, és szervezetlen., kommunikáció, és megfigyelés nélkül. A hiányosságok nem azonosítottak. A munkavállalók nincsenek tudatában felelősségüknek.	Nincs tudatosság az IT ellenőrzések feltételeinek a meghatározása szükségességére. Ha megtörténik, csak ad hoc alapon, magas szinten, és a szignifikáns események reakciójaként. A meghatározás csak az aktuális eseményekre történik meg.
2 Ösztönös	Az ellenőrzések megvannak, de nem dokumentáltak. A működésük az egyének tudásától, és motivációjától függ. A hatékonyság nincs megfelelően értékelve. Sok ellenőrzési gyengeség létezik, de nincs megfelelően feltárva. A hatásuk nagy. A menedzsment tevékenysége az ellenőrzési problémák megoldása nem fontossági sorrend szerint rendezett, és konzisztens. A munkavállalók nincsenek tudatában az ellenőrzési felelősségüknek.	Az ellenőrzés szükségének meghatározása csak akkor történik, ha szükséges, a kiválasztott IT folyamatokra meghatározni az ellenőrzés érettségi szintjét, aktuális szintjét, a cél szintet, amelyet el kell érni, de az ellenőrzési rés létezik. Informális munka értekezletet alkalmaznak,(bevonva az IT menedzsereket, és a programban résztvevő teamet a folyamatba), a megfelelő ellenőrzési folyamat meghatározására, amely motivál egy megállapodásos akció programot.
3 Definiált folyamatok	Az ellenőrzések megvannak, és megfelelően dokumentáltak. A műveletek hatékonyságát rendszeresen értékelik, és a témáknak van egy átlagos száma. Azonban az értékelési folyamat nem dokumentált. Mialatt a menedzsment kiszámíthatóan	Kritikus IT folyamatokat azonosítanak, érték, és kockázat alapon. Részletes elemzést készítenek az ellenőrzési követelményekről, és az ellenőrzési rések okairól, jobb lehetőségek fejlesztésre. Továbbá a munkaértekezletek előmozdítására,

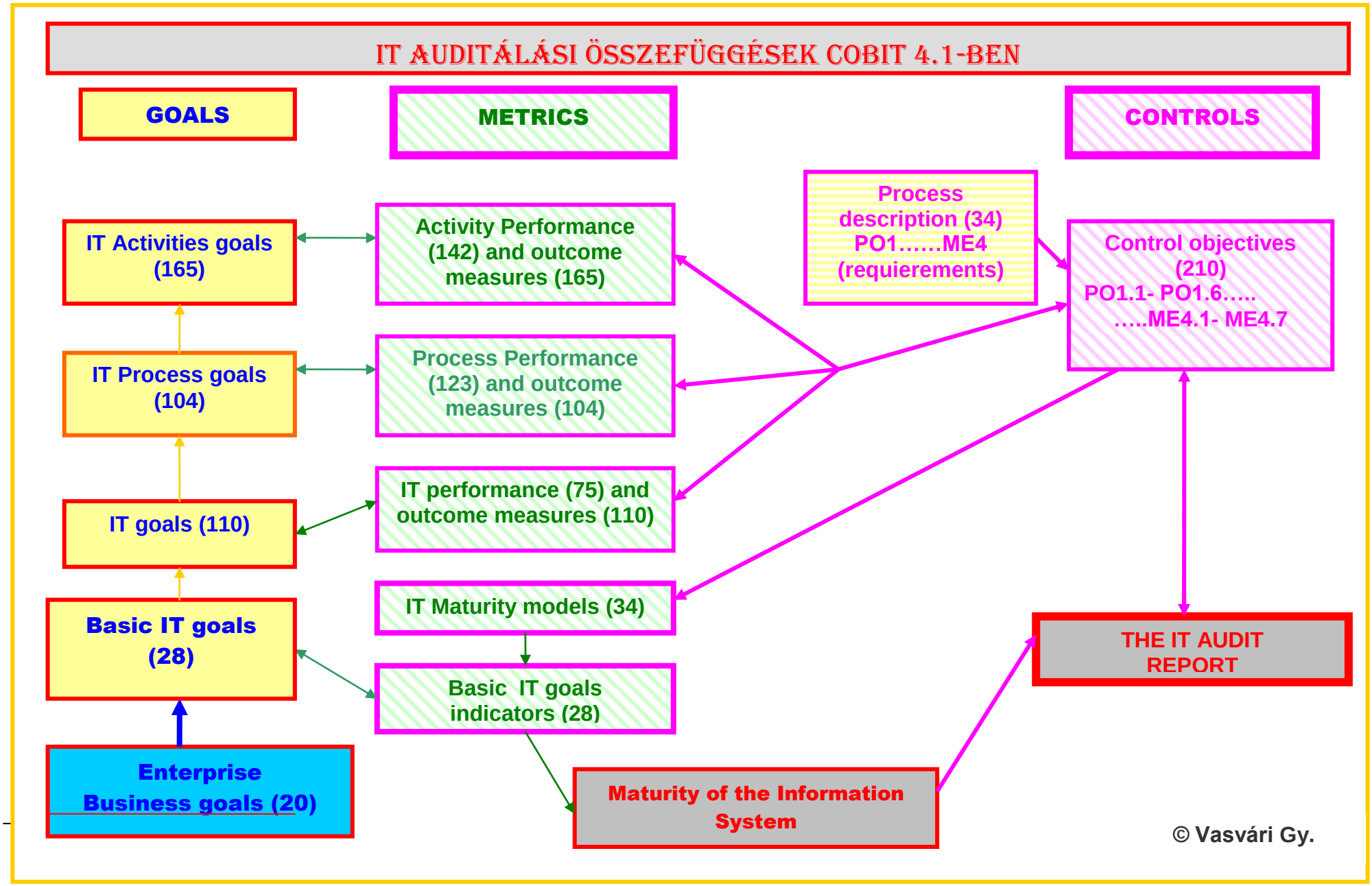
	képes foglalkozni az ellenőrzési témákkal, néhány ellenőrzési gyengeség megmarad, és a hatásuk erős lehet. A munkavállalók tudatában vannak az ellenőrzési felelősségüknek.	az elemzés támogatására eszközöket, és interjúkat használnak, annak érdekében, hogy egy IT folyamat gazda rendelkezzen, és irányítsa a folyamatok meghatározását, és tökéletesítését.
4 Menedzselt, mérhető	Az eredményes belső ellenőrzési, és kockázat kezelési környezet fennáll. A formális, és dokumentált ellenőrzés értékelése rendszeresen megtörténik. Sok ellenőrzés automatikus, és rendszeresen jelentett. A menedzsment a legtöbb ellenőrzést megfelelően kimutatja, de nem minden feladat rutin ellenőrzés tárgya. Konzisztens követése van az azonosított ellenőrzési gyengeségeknek. Az automatikus kontrollokhoz a technológiát taktikailag korlátozottan alkalmazzák.	Az IT folyamatok kritikusságát rendszeresen, a megfelelő üzleti folyamatok tulajdonosai teljes támogatásával, és megállapodással határozták meg. Az ellenőrzési követelmények meghatározása a politikán, és e folyamatoknak az aktuális érettségén alapult, követve egy mélyreható és mérésen alapuló elemzéssel, bevonva a részvényeseket. A számon kérhetősége ezeknek a folyamatoknak tiszta, és kikényszeríthető. A fejlesztési stratégiát támogatják az üzleti események. A teljesítményt, a remélt eredmény elérésére, következetesen megfigyelik. A külső ellenőrzés véletlenszerűen szervezett.
5 Optimalizált	A vállalatot átfogó kockázat, és ellenőrzési program folyamatos, és hatékony ellenőrzési, és kockázati téma megoldást nyújt. A belső ellenőrzés, és a kockázat menedzsment integrálva van a vállalti gyakorlatba, támogatva az automatikus valós idejű megfigyeléssel, teljes számon kérhetőséggel, az ellenőrzés megfigyelésére, a kockázat menedzsmentre, és a megfelelősség kikényszerítésére. Az ellenőrzés értékelése folyamatos, alapozva az önértékelésre, és a gap, és root case analizisre	Az üzleti változásoknál megfontolják az IT folyamatok kritikusságát, és a folyamat ellenőrzés kapacitását ismételten meghatározzák. Az IT folyamatok tulajdonosai rendszeresen végrehajtják önmeghatározását az ellenőrzések az érettségi szintjének, továbbá, hogy találkoznak-e az üzleti szükséglettel, illetve megfontolják az érettség jellemzőit, a hatékonyság, és eredményesség növelése érdekében. A szervezet viszonyít a külső legjobb gyakorlathoz, és keres külső tanácsot a belső ellenőrzés hatékonyságára. A kritikus folyamatok független auditálása elfogadott annak biztosítására, hogy az ellenőrzések a kívánt érettségi szintűek legyenek, és a tervek szerint működjenek.

12.2.2. A COBIT 4.1 ÖSSEFÜGGÉSEK

A következő oldalon a COBIT 4.1 auditálási összefüggések, az audit tervezéséhez nyújthatnak támogatást.

Az ábrán az egyes négyszögekben, a zárójelben szereplő számok, azt mutatják, hogy a szövegben megadottakból hány db van.

Továbbá kiemeljük, hogy a COBIT 4.1 a 4 domainen belül (PO, AI, DS,ME) összesen 34 folyamatot határoz meg (PO1-ME4). A vállalat (rendszer), az azt alkotó folyamatok, és tevékenységek értékeléséhez, pedig, célokat, és mértékeket ad meg, amelyekből megállapítható a folyamat érettsége, minősítése. Mindezek az információs rendszer érettségének a minősítéséhez szolgálnak alapul.


IT AUDITÁLÁSI ÖSSZEFÜGGÉSEK COBIT 4.1-BEN
GOALS
METRICS
CONTROLS
IT Activities goals (165)
Activity Performance (142) and outcome measures (165)
Process description (34) PO1……ME4 (requierements)
Control objectives (210) PO1.1- PO1.6….. …..ME4.1- ME4.7
IT Process goals (104)
Process Performance (123) and outcome measures (104)
IT goals (110)
IT performance (75) and outcome measures (110)
IT Maturity models (34)
Basic IT goals (28)
Basic IT goals indicators (28)
THE IT AUDIT REPORT
Enterprise Business goals (20)
Maturity of the Information System
© Vasvári Gy.

12.3. FIPS PUB 140-2

Ez a szabvány a biztonsági követelményeket határozza meg nem minősített, biztonság érzékeny információk rejtjelezése esetében, (tehát nem állam vagy szolgálati titkot képező információk) számítógépes, illetve távközlési rendszerekben alkalmazott rejtjelező modulok védelmére. A szabvány négy biztonsági szintet határoz meg: Level 1, Level 2, Level 3, Level 4 (növekvő erősségű sorrendben). A biztonsági követelmények kiterjednek a rejtjelező modul bizalmas tervezésére, és implementálására. Többek között:
A rejtjelező modul tervezését, a portokat, és interface-ket; szerepeket, szolgáltatásokat, és a hitelesítést, a fizikai biztonságot, a rejtjelezési kulcs menedzsmentet, a működési környezetet, az elektromágneses interferencia/ elektromágneses kompatibilitás (EMI/EMC) védelmét (47 Code of Federal Regulations Part 15, Subpart B, unintentional Radiators, Digitel Devices, Class A for business use, Class B for home use).

- **Level 1.**

A legalsó szint, amelyre az alapvető biztonsági követelmények vonatkoznak, például egy PC., egy nem értékelt operációs rendszert használva. Az egyéb követelmények, mint fizikai biztonság, hálózati biztonság, és adminisztratív biztonság korlátozottan vagy egyáltalán nincsenek. EMI/EMC üzleti környezetben való alkalmazáshoz.

- **Level 2.**

Itt megjelenik a modul bontás védett kivitele, a modul mozgatható falainak, és ajtójának ellenálló zárása a jogosulatlan behatolás ellen, és minimális szerep bázisú (felhasználó, rejtjelező adminisztrátor, karbantartó), hitelesítést igényel az operátor esetében. A Level 2 megengedi, hogy a software, firmware elemek egy általános célú számítástechnikai rendszert, operációs rendszert használjanak. A biztonságértékelési követelmény EAL 2 (CC). EMI/EMC üzleti környezetben való alkalmazáshoz

- **Level 3.**

Az előbbieken túlmenően itt elő van írva, olyan bontás védettség, amely erőszakos behatolás esetén a biztonság kritikus információkat megsemmisíti. Az operátor hitelesítése azonosítás bázisú., és ellenőrzi, hogy milyen tevékenységre vonatkoznak az operátor jogosultságai. A nyilvános szöveg input, és output útvonala bizalmas útvonal kell legyen elkülönített portra. A Level 2–vel azonos feltételekkel használhat softwaret, és firmwaret, azzal, hogy az operációs rendszer EAL 3 értékelésű legyen. EMI/EMC otthoni környezetben való alkalmazáshoz.

- **Level 4.**

A legmagasabb szint, amelynek komplett fizikai védelmet kell biztosítani a modul körül, fizikai támadásjelző képességgel. A jelzet támadás esetén minden nyílt szöveget meg kell, hogy semmisítsen. Alkalmazható fizikailag nem védett környezetben. Az operátor hitelesítése azonosítás bázisú. Az operációs rendszernek az EAL 4 követelményeit kell teljesíteni. EMI/EMC otthoni környezetben való alkalmazáshoz.

12.4. BIZTONSÁGI SZEMPONTBÓL FONTOS SZABÁLYOZÁSOK

12.4.1. A SZABÁLYOZÁSOK VÁLTOZATAI

A szabályozások lehetnek, szabályzatok, utasítások, eljárás rendek, amelyek fogalma a következőket takarja:

- *A Szabályzat magatartást, cselekvést meghatározó szabályok összessége.*
  A szabályzat HOGYAN orientált.

- *Az Utasítás valaminek a végrehajtására kiadott rendelkezés.*
  Az Utasítás tevékenység orientált.

- *Az Eljárás rend valamilyen üzleti folyamat vagy informatikai alkalmazás vagy rész folyamat során végrehajtandó tevékenységek, és végrehajtásuk időbeli sorrendjének szabályozása.*
  Az Eljárási rend sorrend orientált.

Tehát az Utasítás nem tartalmazza a hogyant, szemben a szabályzattal, míg az Eljárás rend nem tartalmazza a hogyant, illetve a kinek a feladatát, az előbbi kettővel szemben.

12.4.2. VÁLLALATI STRATÉGIÁK

Általános Vállalati Stratégia
Funkcionális Stratégiák:
Üzleti Stratégia
Termelési Stratégia
Informatikai Stratégia

12.4.3. UTASÍTÁSOK

Humán Politika
Adat-, és Titokvédelmi Utasítás
Iratkezelési Utasítás
Selejtezési Utasítás
Tűzvédelmi Utasítás
Outsourcing Utasítás

12.4.4. IT SZABÁLYZATOK

IT Biztonsági Politika
IT Üzletmenet folytonossági Terv
IT Működési Szabályzat
IT Fejlesztési Szabályzat
Vírusvédelmi Szabályzat

12.4.5. IT ELJÁRÁS RENDEK

Jelszó és Jogosultság kezelés Rendje
Az Alkalmazások Eljárás Rendjei (mentési, és újraindítási rend beleértve)
Átadás-átvételi Rend
Help Desk Eljárás Rend
Szoftver Licensz Nyilvántartási Rend
Program Változás Kezelés Rendje
Hálózat Üzemeltetés Eljárás rendje
Védelmi Intézkedések Nyilvántartási Rendje
Konfiguráció Kezelési Rend
Átadás/átvételi Eljárási Rend

12.5. BIZTONSÁGI SZEMPONTOK EGYES SZABÁLYOZÁSOKHOZ

Az alábbi szabályozások készítése nem képezi a Biztonsági vezető feladatát, a készítésében általában nem vesz részt, de véleményezésre meg kell kapnia, a biztonsági követelmények érvényesítése érdekében. Ehhez néhány, a legfontosabb szabályozásnál az IT biztonsági vezető részéről képviselendő biztonsági követelményt, az alábbiakban megadunk.

12.5.1. ADAT, ÉS TITOKVÉDELMI UTASÍTÁS

Az Adat, és Titokvédelmi Utasítás meghatározza a titkot képező erőforrások biztonság kritikussága függvényében a védelem kívánt erősségét, osztályozza biztonsági szempontból azokat. Az osztályozás tárgyát kell, hogy képezze az adatok (személyes, és minden egyéb), a helyiségek, és az eszközök osztályozása. Ez gyakorlatilag azt jelenti, hogy három osztályozási rendszert kell kialakítani, annak érdekében,

hogy majd az egyes osztályokhoz hozzárendeljük a megfelelő védelmi intézkedéseket.

12.5.2. IRAT KEZELÉSI UTASÍTÁS

Az Iratkezelési Utasításnak ki kell térnie egyrészt a papíralapú, másrészt az elektronikus iratokra egyaránt. Át kell fognia az iratok keletkezésétől, a kezelésükön keresztül, a selejtezésükig a teljes életciklust. Gondoskodni kel arról, hogy megfelelő védelmi intézkedések garantálják az egyikből, a másikba, illetve fordítva, az átment esetében, hogy az iratok megőrizzék biztonsági osztályozásukat.

12.5.3. SELEJTEZÉSI UTASÍTÁS

A Selejtezési Utasításnak ki kell térnie bármely papír vagy elektronikus adathordozó, illetve bármely erőforrás selejtezési szabályaira. A fő biztonsági szabályok:

- A selejtezés csak bizottság előtt történhet, amely a tevékenységéről jegyzőkönyvet köteles felvenni.
- A selejtezés bármilyen mennyiségről van szó nem történhet csak egyenként.
- Az adathordozókat (papír, elektronikus) a selejtezés előtt érvényteleníteni kell.
- Gondoskodni kell arról, hogy a leselejtezett eszközökkel jogosulatlanul ne juthasson senki bizalmas adatok birtokába. Ez mágneses adathordozók esetében jelentheti azt, hogy az adathordozót nem lehet értékesíteni (pl. egy PC értékesítésekor a törölt winchester is biztonsági kockázatot jelent).

12.5.4. OUTSOURCING UTASÍTÁS

Az outsourcing veszélyforrást képez, mivel a harmadik féltől csak a szerződésben rögzített kötelezettségek kérhetők számon, azok sem túl egyszerűen. A biztonsági követelményeket a szerződésnek feltétlenül tartalmazni kell. Ezek a következők:

- Mire vonatkozik a szerződés (külső fejlesztés, belső fejlesztés, üzemeltetés kiadása, munkaerőbérlés stb).
- Köteles-e a felhasználó megbízásából elvégzett tevékenységeinél minden jogi követelményt, illetve szabályt, és szabványt 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.

12.5.5. ÁTADÁS/ÁTVÉTELI ELJÁRÁS REND

Az Átadás/átvételkor érvényesítendő biztonsági követelmények:

- Az átadás/átvétel során meg kell győződni arról, hogy a fejlesztés/beszerzés elindításakor megadott biztonsági követelmények teljesülnek-e. Ide tartozik, amennyiben a szállításra is voltak megadva biztonsági követelmények, azok megvalósulását is ellenőrizni kell.
- Az eljárás folyamán gondoskodni kell arról, hogy éles adatokhoz jogosulatlanul ne lehessen hozzáférni. Lehetséges az átadónak hozzáférési jogosultságot adni, de azt az eljárás befejezése után vissza kell vonni.
- A szállító, amennyiben harmadik fél „fenyegetés mentességi” nyilatkozatot kell írásban adjon, amelyet a szerződéskötéskor elő kell írni, továbbá nyilatkoznia kell arról, hogy a leszállított termék jogtiszta.

12.5.6. PROGRAM VÁLTOZÁSKEZELÉSI REND

A programokon változtatni csak az erre jogosult személy változtathat. Gondoskodni kell arról. Hogy

- A változtatási jogosultság nem lehet örök érvényű. Különösen nem, ha azt a fejlesztő, programozó kapja meg. Ebben az esetben, csak meghatározott rövid időre vonatkozhat.
- A változtatásra jogosult köteles
  - ✓ A változtatást a dokumentációkon átvezetni
  - ✓ Gondoskodnia arról, hogy az új változat mindenütt, ahol az IR-ben alkalmazzák az adott programot át vezetésre kerüljön.
  - ✓ Az új változat teszteléséhez felhasznált éles adatok nem kerülhetnek vissza az éles rendszerbe.
- A feladat szétválasztás elve alapján a programváltoztatásra jogosult nem lehet a rendszer gazda.
- A program korábbi változatát, a lecserélt változatot archiválni kell.

12.5.7. KONFIGURÁCIÓ KEZELÉSI REND

A konfiguráció változtatása a legkülönbözőbb okok miatt válhat szükségessé. Alapvető biztonsági követelmény, hogy a változtatás végrehajtásakor meg kell győződni arról, hogy az új elemek kielégítik a biztonsági követelményeket, amely a technológia minden elemére létezik.

12.5.8. SZOFTVEREK REGISZTRÁCIÓS NYILVÁNTARTÁSA

A vásárolt szoftverek jogtisztaságáról a szállítónak nyilatkozni kell, majd azok regisztráltatását nem csak végre kell hajtani, hanem nyilván is kell tartani. Ez jelenti a vállalat regisztrációs kérelmét, és a regisztrálás tényét elismerő szállítói nyilatkozatot. Előfordul az, hogy a regisztrálás meghatározott feltételek mellett áll fenn, és pl. határidőhöz is kötött. A nyilvántartásnak gondoskodni kell arról, hogy ez a határidő ne járjon le.

12.5.9. VÉDELMI INTÉZKEDÉSEK NYILVÁNTARTÁSI RENDJE

Védelmi intézkedések bevezetése, és törlése csak a biztonsági vezető engedélyével történhet. Ezért az engedélyezett védelmi intézkedésekről, és azok törléséről vagy módosításáról a biztonsági szervezetnek nyilvántartást kell vezetnie.

12.6. A KÖLTSÉGHATÉKONYSÁG PROBLÉMÁJA

A költséghatékonyság biztosítása a biztonságszervezőtől elvárt feladat. Ennek a gyakorlatba történő átültetése azonban igen sok problémát vet fel. Egyrészt a költségek, amelyek egy biztonsági esemény bekövetkezésének hatására fellépnek, vagyoni (tangible) és nem vagyoni (intagible) károkat egyaránt okoznak. A nem vagyoni károk azonban számítással nem, csak becsléssel határozhatóak meg. A károk, illetve a bekövetkezhető veszteség egy védelmi intézkedés kockázat csökkentő hatását vizsgálva az összehasonlítási alapot képezik.

Habár nincs az irodalomban egységes vélemény, de általában azt mondják, hogy a várható veszteségnél, ne legyen nagyobb a védelem megvalósításának, üzemeltetésének költsége (éves szinten).

Ezzel szemben további probléma, hogy a biztonsági követelmények egy védelmi intézkedés, illetve az egész rendszer védelme költséghatékonyságával szemben megkövetelhetik a szervezet biztonsági érdekeinek akár a költséghatékonyság rovására történő érvényesítést. Ebből következik, hogy általában előfordulhat, hogy egyes védelmi intézkedéseknél, de menné biztonság érzékenyebb egy szervezet tevékenysége, annál inkább, az egész rendszernél, hogy a biztonsági érdekek felülírják a pénzügyi érdekeket.

Egy biztonsági auditnál, tehát ezeket egyaránt kell vizsgálni.

12.7. FELHASZNÁLT IRODALOM

[1] F. L. Bauer: Kryptologie Methoden und Maximen. Springer Verlag, 1994.
[2] J. Butler: Contingency Planning and Disaster Recovery Strategies. Computer Technology Research Corp., 1994.
[3] R. J. Bud Bates: Disaster Recovery Planning Networks, Telecommunication and Data Communications. McGraw-Hill Inc., 1991.
[4] Debra Cameron: Security Issues for the Internet and World Wide Web. Computer Technology Research Corp., 1996.
[5] Debra Cameron: Electronic Commerce. Computer Technology Research Corp., 1997.
[6] David Chaum: Achieving Electronic Privacy. Scientific American, August 1992, 76-81. Magyarul: Személyes adatvédelem - rejtjelezéssel, Tudomány, 1992. október.
[7] Dr. Cserép Attila és több Szerző: Vagyonvédelmi nagykönyv. Cedit Kft., 1996.
[8] Dénes József, Vasvári György: A távközlés biztonsága. Magyar Távközlés, 1994 nov,
[9] Dénes József, Vasvári György: A távközlési hálózatok biztonsági kérdéseiről. Magyar Távközlés, 1996, augusztus.
[10] J. Essinger: Computer Security within Financial Institutions. Financial Times, Financial Publishing, 1996.
[11] K. F. Hindenburg: Archiv der reinen und angewandten Mathematik. Schäferischen Buchhandlung,1795.
[12] W. S. Jevons: The Principles of Science. New York: Dover, 1958.
[13] D. Kingsley: Security&Control in an Oracle Enviroment. ISACA. 1993.
[14] Kónya Judit: Banküzemtani alapismeretek. Közgazdasági Kiadó, 1994.

[15] B. M. Leiner és több Szerző: The Past and Future History of the Internet. February 1997/Vol.40.No.2. Communication of The ACM.
[16] J. Levine: United States Cryptographic Patents 1861-1989. Cryptologia Terre Haute Indiana, 1991.
[17] B. Menkus: Business Continuity. IS AUDIT & CONTROL JOURNAL VOLUME I, 1994.
[18]Nemetz Tibor,Vajda István: Algoritmusos adatvédelem. Akadémiai Kiadó, 1991.
[19] D. B. Parker: Restating the Foundation of Information Security. Transnational Data and Communication Report, March/april, 1991.
[20]R.Slade: Guide to Computer Viruses. Springer-Verlag.1996.
[21]Fred Simonds: Network Security, Mc Graw Hill Inc. 1996.
[22]G. J. Simmons: Contemporary Cryptology. IEEE Press, 1991.
[23] G. J. Simmons: Identification of Data, Devices, Documents and Individuals. Proceedings 25th Annual 1991. IEEE International Carnahan Conference on Security Technology.
[24]K. Slater: Information Security in Financial Services. Stockton Press, 1991.
[25]Terplán Kornél: Lokális hálózatok menedzselése. Panem-McGraw-Hill, 1995.
[26]J. Toigo: Disaster Recovery Planning. John Wiley & Sons, Inc. 1996.
[27]S. R. Vallabhaneni: CISA Examination Review Book. EDP Auditing Publication.
[28]Vasvári György: Bankbiztonság. Információs Társadalomért Alapítvány. 2006.
[29]Vasvári György: Biztonsági rendszerek szervezése. Prosec Kft. 1997.
[30]Audit Guidelines COBIT 4.1, Information System Audit and Control Foundation, 2000.
[31]CISA Review Technical Information Manual 1998. ISACA Inc. 1998.
[32]Massachusetts Institute of Technology. Business Continuity Plan.
[33]The Institute of Internal Auditors Research Foundation, Module 9 Security, Module 10 Contingency Planning, 1991.
[34]UNIX: Its Use Control, and Audit. ISACA. 1995.
[35]USE Planning Gide. SWIFT, 1992.
[36]US. General Accouting Office. Year 2000 Computing Crisis: Business Continuity and Contingency Planning. Marc. 1998.
[37]Common Criteria, Common Methodology for Information Security Evaluation, Version 2.1.
[38]Information Security (An Integrated Collection of Essays).IEE PRESS.1995.
[39] A.S. Tanenbaum. Számítógéphálózatok. Panem-Prentice-Hall.1999.
[40] Control Objectives for Net Centric Technology (Volume I.-IV.). ISACF: 1999.
[41] A.M WILLhite, D.R. Norton. Establish a Basline Assesment to Manage Risk Usiong RISK Matrix. http//www.mire. org/resources/centers/sepo/risk/New *risk*_INFOSEC99.html
[42] Horváth, Lukács, Tuzson, Vasvári. Informatikai Biztonsági Rendszerek. E&Y. BMF KANDÓ KAR. 2001.
[43] Control Objectives for Enterprise Governance. IT Governance Intitute. 2003.
[44] IT Governance Executive Summary. IT Governance Institute 2003.
[45]Information Security Governance: Guidance for Boards of Directors and Executive Management. IT Governance Institute. 2003.
[46] IT Strategy Committee. IT Governance Institute. 2003.
[47] CISM Review Manual. ISACA. 2003.
[48] Nyilas S. – Nagy F. Amit az ipari kémkedésről tudni kell. Raab Karcher Biztonsági Szolgálat Kft. 1998.
[49] K. D. Mitnick. A megtévesztés művészete. Perfact-Pro Kft. 2003.

{50] Több Szerző. Információ- biztonság. Cedit Információtechnikai Kft. 1997.
[51] SLA TOOLKIT. EASYTECH SOLUTION: 2000.
[52] Ladó László. Szervezéselmélet és – módszertan. Közgazdasági és jogi könyvkiadó. 1979.
[54] Governance, Control and Audit for Information and Related Technology. COBIT 4.1. ITGI. 2007.
[55] Control Objectives, Management Guidelines, Maturity Models. COBIT 4.1. ITGI. 2007.
[56] „International Convergence of Capital Measurment and Capital Standards" BASEL COMMMITTEE on BANKING SUPERVISION 2004.
[57] The Application of Basel II. to Trading Activities and Double Default Effects. BASEL COMMITTEE on BANKING SUPERVISION. July. 2005.
[58] Sound Practices for the Management and Supervision of Operational Risk. Bank for International Settlements. 2001.
[59] Critical Elements of Security Program Succes. ISACA. 2005.
[60] F. Björck: Security Scandinavian Style. Stockholm Universíty. 2001.
[61] A. Mizzi: Return on Information Security investment. http://www.geocities.com/amz/ .
[62] Enterprise Risk Management Framework. Draft. COSO. 2004. (COSO II.)
[63] A strategy for incorporating risk assessment in the compliance and ethic agenda. AON. 2006.
[64] K.W. Knight: Integrated Risk Management Implementation Guide. Treasury Board of Canada. 2001-2003.

A Szerző kéri, hogy az anyagban észrevett bármely hibáról az olvasó az alábbi címen értesítse.

Köszönettel

VASVÁRI GYÖRGY
nyugdíjas CISM
informatikai biztonsági szakértő
információ rendszer ellenőrzési szakértő

Elérhetőségek:
2096. Üröm. Damjanich utca 13/A.
Mobil: 06-20-9418-467
E-mail: gvasvari@tiphaz.hu