Vállalati információbiztonság szervezése

Dr. Michelberger Pál

Óbudai Egyetem, Keleti Károly Gazdasági Kar

Szervezési és Vezetési Intézet

michelberger.pal@kgk.uni-obuda.hu

Lábodi Csaba

QLCS Kft.

csaba.labodi@gmail.hu

Absztrakt: Az állami, önkormányzati, üzleti és nonprofit szervezeteknek már a múlt században is komoly feladatot jelentett az információs vagyonuk (partnerek adatai, technológiák és konstrukciók leírásai, beruházási tervek, személyes adatok, stb.) védelme. A titkos ügykezelési, valamint szervezeti és működési szabályzatok információvédelmi szempontból is szabályozták az ügyviteli folyamatokat. Az információ technológia nagymérvű alkalmazása és nélkülözhetetlensége újabb, eddig ismeretlen kockázatokat eredményeztek. Szükséges tehát az információ- és adatkezelés minden részletre (emberi erőforrás, információtechnológia, szervezet, folyamat) kitérő „holisztikus" szabályozása.

1 Informatikai és információ biztonság

Az egyre inkább tudásalapúvá váló társadalomban és gazdaságban az információ a gazdálkodó szervezet számára olyan érték, amely a vezetői döntések, ill. az üzleti sikeresség alapja és az alkalmazott információs technológia „erőforrása", ezáltal a működés hatékonyságának meghatározó eleme. Vonatkozhat többek között termékre, szolgáltatásra, technológiai ismeretekre és a rendelkezésre álló erőforrásokra, valamint az üzleti partnerekre is. Ha hiányoznak, pontatlanok, vagy nem időszerűek, esetleg illetéktelenek kezébe kerülnek, akkor ez a vállalat számára károkat okozhat. Az információt tehát védeni kell...

Ez ma az információk (ISO/IEC 27001)

- **bizalmasságát** (az információ csak az arra felhatalmazottak számára legyen elérhető)

- **sértetlenségét** (az információk teljességének és pontosságának megőrzése)
- és **rendelkezésre állását** jelenti (a felhatalmazott felhasználók akkor férjenek hozzá az információhoz, amikor az szükséges)

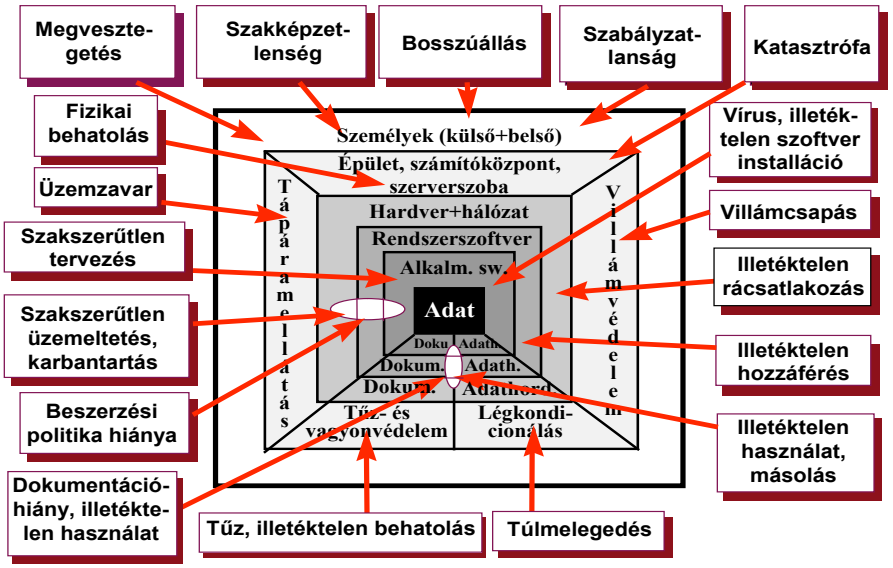
Az **információbiztonság lényegesen összetettebb problémakör, mint az informatikai biztonság.** Ma már nem elég vírusirtókban, tűzfalakban, megbízhatóan működő hardverben és egyértelmű azonosító rendszerekben gondolkodni. A technológiai háttér tudatos kialakítása nem elégséges. Az információ sértetlenségét, a rendelkezésre állását és a bizalmas kezelését azonban elsősorban a belső munkatársak (vállalatirányítási információs rendszerek és intranet révén) és a vállalati adatbázisokhoz interneten, extraneten és elektronikus adatcsere révén hozzáférő stratégiai partnerek (beszállítók, viszonteladók, kooperációs partnerek és pénzügyi szolgáltatók) gondatlan, esetleg szándékos károkozása veszélyezteti. Az információbiztonsághoz további jellemzők is kapcsolhatók, mint a **hitelesség, számon-kérhetőség, letagadhatatlanság és a megbízhatóság.**

Az információ-vagyon védelme érdekében legáltalánosabban az információ- és az információhordozók kezelését szabályozzuk. Ez független attól, hogy milyen az információ megjelenési formája. A védelem akkor működik helyesen, ha meghatározzuk a védendő információkat, a külső és belső fenyegetéseket, ill. azok kockázatát valamint, a védelemhez szükséges szabályozást és eszközrendszert (ISO/IEC 27002). A vállalati „információ vagyont" fenyegető veszélyforrások a teljesség igénye nélkül is sokrétűek lehetnek:

- hibás szoftveralkalmazások
- üzemzavar
- szakszerűtlen információtechnológiai tervezés és üzemeltetés
- illetéktelen használat, ill. hozzáférés
- katasztrófa helyzet (tűzeset, árvíz, földrengés)
- vírusok, kémprogramok
- hálózat szándékos túlterhelése (sniffing) és eltérítése (spoofing)
- meg nem engedett szoftverhasználat

Az információvédelem célja tehát, hogy strukturáltan biztosítsuk az üzletmenet folytonosságát és szabályozott működéssel mérsékeljük a biztonsági eseményekből adódó károkat. Információbiztonságot a kockázatokat figyelembevevő óvintézkedésekkel lehet elérni. Ezek a vállalati folyamatokat leíró szabályzatokból, folyamatokat tükröző szervezeti felépítésből és az ezeknek megfelelő információtechnológiai eszközök (hardver, szoftver, telekommunikációs elemek) szabályozott működtetéséből állnak (1. ábra).

Az informatikai rendszerek estében megkülönböztetünk fizikai és operatív védelmet. Az első esetben a megfelelő, infrastruktúrát védő környezet kialakításáról van szó (környezeti ártalmak, szándékos vagy vétlen rongálás), míg a másodiknál a munkavégzés, az információtechnológia használatának szabályozásáról beszélünk (naplózás, vírus-irtás, azonosítás, illetékesség megállapítása stb.).



1. ábra

Informatikai rendszerek fenyegetettségei

Forrás: Informatikai Tárcaközi Bizottság 12. sz ajánlása, Informatikai rendszerek biztonsági követelményei, Miniszterelnöki Hivatal

Az információbiztonság állapot. A gazdálkodó szervezetek hosszú távú működéséhez hamis biztonságérzetet nyújtó eszközök helyett biztonságot nyújtó irányítási rendszer alkalmazása szükséges.

Az információvédelemben több biztonsági szintet is megkülönböztethetünk (Ji-Yeu Park et.al. 2008):

1. Információtechnológiai infrastruktúra (hardver-, szoftver- és hálózatvédelem)
2. Információkezelés (adatfelvétel, -módosítás, -törlés, informálódás, ill. lekérdezés)
3. Ügyviteli folyamatok (folyamatszabályozás, workflow)
4. Szervezet (információbiztonsági stratégia, kockázatkezelés)

Erre jó példa a jogosultsági rendszer „holisztikus” kialakítása. Mind a négy szinten vannak ezzel kapcsolatos feladatok:

- IT szint – felhasználó azonosítás
- információkezelési szint – csak a munka elvégzéshez minimálisan szükséges adathozzáférések biztosítása
- folyamat szint – kritikus folyamatok megosztása, helyhez és személyhez kötött jogosultság (vállalatoknál gyakori a jelszó „átadása” és ugyanazzal a jelszóval történő egyidejű, több helyen történő bejelentkezés…)
- szervezeti szint – kockázatkerülés, jogosultsági csoportok kialakítása és a jogosultsági rendszer állandó felügyeletének szabályozása

Egy másik forrás kis és közepes vállalatok számára készülő információbiztonsági irányítási rendszer esetében szintén négy vizsgálandó és szabályozandó elemet ad meg (Hangbae Chang et.al. 2006):

1. IT elemek (vásárolt hardverek és alapszoftverek, hálózati eszközök)
2. a szervezet informatikai tudása és gyakorlata – „humán információtechnológia” (ahogy a vállalat az IT elemeket használja…)
3. információszolgáltatás és -megosztás a vállalaton belül (a végfelhasználók számára)
4. vállalati alkalmazások (pl. ERP rendszerek) üzemeltetése (felhasználók képzése, támogatása)

Lényeges továbbá az információbiztonságot támogató környezet kialakítása is, amely elfogadott információbiztonsági politikát, meghatározott felelősségi köröket, képzést és pénzügyi források biztosítását jelenti.

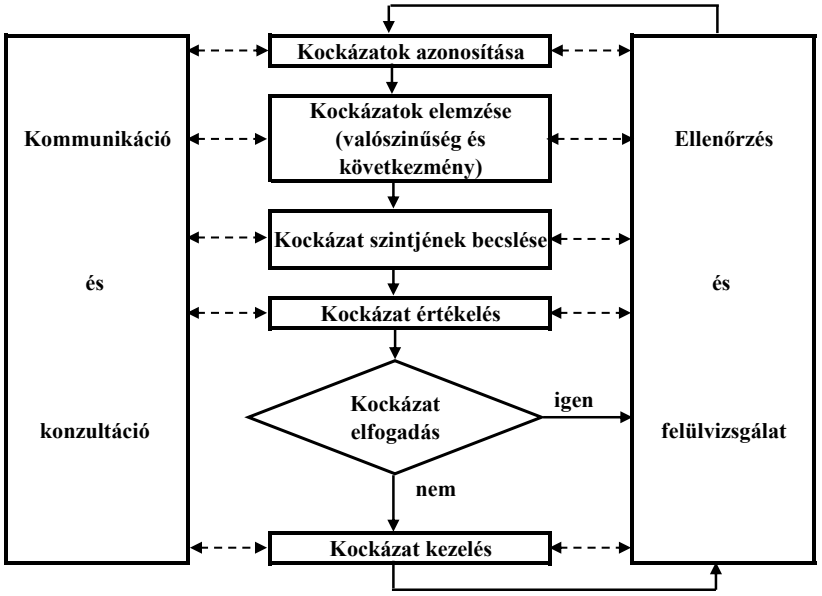
Csak ez után teremthető meg az információbiztonság – mint állapot – amelynek többek között része az informatikai eszközök, dokumentációk teljes körű nyilvántartása, a kockázat elemzés (informatikai eszközökre és környezeti kihívásokra) és a felhasználók jogosultságának kezelése (dokumentációhoz, hálózathoz, szerverhez, munkaállomáshoz, alkalmazói szoftverhez és magához az információkhoz).

2 Vállalati kockázatelemzés

A kockázat olyan potenciális események, zavarok bekövetkezése a vállalaton belül és annak környezetében (akár piacán is…), amelynél veszélybe kerül a vevői igény kielégítése vagy bármely vállalati érintett (stake- és stockholder) biztonsága.

Az biztonsággal kapcsolatba hozható incidensek kockázata kifejezhető időegységre eső pénzösszeggel [Ft/év], vagy ha ez nem meghatározható, akkor „osztályzattal", ami a kockázat nagyságrendjét és elviselhetőségét mutatja. A kockázat függ a káros események **bekövetkezési valószínűségétől** [1/év] és ezen események bekövetkezéséből származó és **pénzben kifejezett kártól** [Ft] is (2. ábra).

A hagyományos kockázati megközelítés mellett – pontosan meghatározható kockázati adatok hiányában – beszélhetünk **„sebezhetőségről"** is, amelyek a folyamatokat fenyegető veszélyek eredetét mutatja.



2. ábra
A kockázatkezelés folyamata (Standards Australia, AS/NZS 4360 alapján)

3 Információbiztonság alapjai (szabványok és ajánlások)

Számos nemzetközileg elismert dokumentum készült az informatikai- és az információbiztonság szabályozására. Néhány – általam fontosnak tartott – anyagot említek meg ebben a fejezetben. Természetesen mindegyiknek más a

megközelítése és a célterülete, de mindegyik foglalkozik a vállalati információk védelmével.

A szoftverminőség-vizsgálatok alapja egy szabványos szempontrendszer (Tóth, 1999). A **„Szoftvertermékek értékelése, minőségi jellemzők és használatuk irányelvei"** című szabvány (MSZ ISO/IEC 9126) egy hierarchikus szempontrendszert ad. A minőségi jellemzőket a szerzők hat csoportba sorolták (funkcionalitás, megbízhatóság, használhatóság, hatékonyság, karbantarthatóság, hordozhatóság), törekedve az átfedések nélküli teljességre. A szabvány mellékletében megtalálható a szempontok további „bontása" is. Ezek azonban – általános ajánlásról révén szó – nincsenek teljes részletezettséggel kidolgozva. A hat csoport „dimenziói", tartalma és megfogalmazásai beilleszthetők egy átfogó, informatikai megoldásokat biztonsági szempontból is értékelő kritérium rendszerbe. Csoportonként a következő szempontok lehetnek fontosak:

Funkcionalitás (mit kell kielégítenie a szoftvernek?)

- megfelelőség (képes-e az előre meghatározott feladatok elvégzésére, funkciók teljesítésére?)
- szolgáltatott outputok pontossága
- interoperabilitás (más rendszerekkel való együttműködési képesség)
- vonatkozó szabványoknak, törvényi szabályozásnak és konvencióknak történő megfelelés
- biztonság (védelem jogosulatlan – szándékos vagy véletlen – hozzáférések ellen)

Megbízhatóság (adott ideig tartó működőképesség megtartása, meghatározott körülmények között)

- működési hiba előfordulás várható gyakorisága
- hibatűrő képesség (meghatározott teljesítményszint biztosítása, hibák, ill. előírt körülményektől történő eltérés esetén)
- helyreállíthatóság (elfogadható teljesítményszint és sérült adatok visszaállítási képessége, ideje működési zavarok esetén…)

Használhatóság (a felhasználóktól elvárt, a rendszer használatához szükséges „erőfeszítések" mértéke)

- érthetőség (mennyi erőforrás és idő árán ismerhető meg a szoftver logikája és alkalmazhatósága?)
- tanulhatóság (milyen könnyen vagy nehezen sajátítható el a szoftver működtetése, az adatbevitel, vagy akár a lekérdezési lehetőségek?)

- üzemeltethetőség (mekkora terhet jelent a rendszer működtetése, és annak ellenőrzése?)

Hatékonyság (a szoftver alkalmazásával biztosított teljesítmény és használathoz szükséges erőforrások viszonya)

- válasz-, feldolgozási és végrehajtási idők, futási sebességek
- erőforrás-kihasználás (a vállalt funkciók ellátásához szükséges erőforrások mennyisége és használati ideje)

Karbantarthatóság (a módosítások elvégzéséhez (hibafelismerés és -javítás, fejlesztés, megváltozott környezethez történő adaptálás stb.) szükséges erőfeszítések

- elemezhetőség (hiányosságok és hiba-okok megállapítása, módosítandó részek azonosíthatósága)
- változtathatóság (módosítás, környezet változtatás, hibajavítás erőforrás- és időigénye)
- stabilitás (a változtatás váratlan következményeinek kockázata)
- tesztelhetőség (módosított szoftver ellenőrzésének erőforrás- és időigénye)

Hordozhatóság (a rendszer egyik hardver-, szoftver- vagy szervezeti környezetből a másikba történő áttelepítésének nehézsége, kockázata)

- adaptálhatóság (különböző, meghatározott környezetekben történő alkalmazásba-vétel lehetőségei és nehézségei)
- üzembe helyezhetőség (üzembe helyezés erőforrás- és időigénye meghatározott környezetben)
- összhang (hordozhatósággal kapcsolatos szabványoknak és konvencióknak való megfelelés)
- kicserélhetőség (másik szoftver adott környezetben történő helyettesítésének képessége)

A hardver esetében a megbízhatóságra más definíciót adhatunk meg. Általános értelemben a megbízhatóság (dependability) gyűjtőfogalom, amelyet a használhatóság és az azt befolyásoló tényezők (hibamentesség, karbantarthatóság és a karbantartás-ellátás) leírására használnak. Szűkebb értelemben (reliability) a terméknek az a képessége, hogy előírt funkcióját adott feltételek között, adott időszakban ellátja.

A használhatóság (availability) hardver termékeknél, az a képesség, hogy adott időpontban vagy időszakaszban, adott feltételek között ellátja előírt funkcióját, feltéve, hogy a szükséges külső erőforrások rendelkezésre állnak.

A karbantarthatóság (maintainability) hardver esetén a terméknek az a képessége, hogy meghatározott feltételek között olyan állapotban tartható, ill. állítható vissza, amelyben előírt funkcióját teljesíteni tudja, ha karbantartását adott feltételek között és előírt eljárások, valamint erőforrások felhasználásával végzik el (MSZ IEC 50 (191)).

A több részből álló **ISO/IEC 14598** jelű, a szoftverekkel szemben támasztott minőségi követelmények kiértékelési eljárásait meghatározó nemzetközi szabványt még nem honosították Magyarországon. A szoftverek értékelése során kiemelt szerepet kap a vizsgálat megismételhetősége és a vizsgálatot végző személyektől való függetlenség. Fontos, hogy az értékelési eredmény objektív, tényszerű és elfogultságtól mentes legyen.

Szoftverminősítés kiértékelési szintjei és felhasználási területei az ISO/IEC 14598 szerint

Értékelési szint	Kockázat				Tipikus felhasználási terület
	biztonsági	gazdasági	védelmi	környezeti	
A	tömeg-katasztrófa	pénzügyi katasztrófa	stratégiai adat- és szolgáltatási kockázat	helyrehozhatatlan környezeti szennyezés	vasút, atomtechnika
B	emberi életveszély	nagy veszteség	kritikus adat- és szolgáltatási kockázat	helyrehozható környezeti szennyezés	egészségügy, pénzügy
C	tulajdoni kár, emberi sérülésveszély	jelentős veszteség	hibakockázat	helyi szennyezés	tűzriasztás, folyamatirányítás
D	jelentéktelen tulajdoni kár, emberekre veszélytelen	jelentéktelen veszteség	kockázat nincs	kockázat nincs	szórakoztatás, háztartás

1. táblázat

A szoftverminősítéssel kapcsolatos szinteket a szabvány négy szintre bontja és e mellett négy - védelmi szempontból is értékelhető – kockázati típust ad meg (1. táblázat).

Az **MSZ ISO/IEC 12207** jelű nemzetközi szabvány „Informatika. Szoftver életciklus folyamatok” címet viseli. Egységes fogalmi keretet ad a szoftverek teljes életciklusára az ötletek megfogalmazásától a szoftver visszavonásáig. Kiemelten kezeli a szoftvertermékek és szolgáltatások beszerzési és szállítási folyamatait. A szabvány alkalmazási területeinél a szerzők egyértelműen közlik, hogy a dokumentum rendszerek, szoftvertermékek és szoftverszolgáltatók beszerzői, valamint szoftvertermékek szállítói, fejlesztői, üzemeltetői, karbantartói és felhasználói számára készült. Az életciklust az alábbi öt folyamatra lehet bontani:

a. Beszerzés
b. Szállítás
c. Fejlesztés
d. Üzemeltetés
e. Karbantartás

Az életciklusnak vannak ún. támogató folyamatai (Dokumentálás, Konfigurációkezelés, Minőségbiztosítás, Igazolás, Érvényesítés, Együttes átvizsgálás, Felülvizsgálás, Problémamegoldás), amelyek elősegítik a szoftver alkalmazásának sikerességét. A szervezeti folyamatok (Irányítás, Infrastruktúrabiztosítás, Megújítás, Képzés) a személyzeti és infrastrukturális háttér biztosítására és folyamatos megújítására szolgálnak.

A **Common Criteria** (továbbiakban CC) az Egyesült Államokból származik, de Kanada és az Európai Unió is elfogadta. A dokumentum teljes címe alapján (Common Criteria for Information Technology Security Evaluation – Közös követelményrendszer az **informatikai biztonság** minősítéséhez) is megállapítható, hogy az informatikai termékek és rendszerek biztonsági szintjének mérésére és értékelésére készült (www.commoncriteriaportal.org). 1999 óta európai, 2002-től, ill. 2003-tól magyar szabvány változata is elérhető (**MSZ ISO/IEC 15408-1, -2, -3**). A biztonsági vizsgálatokat végző szervezetek számára egyértelműen meghatározza, hogy a rendszernek mit kell nyújtania és ezt, hogyan kell megismételhetően megvizsgálni. A fejlesztők számára biztosítja a biztonsági megoldások egyértelmű leírását és megadja a szállítandó termékkel szemben támasztott követelményeket. A fogyasztóknak (felhasználóknak) lehetővé teszi, hogy világosan megfogalmazhassák a termékek és a rendszerek biztonsági funkcióival szembeni elvárásaikat és összehasonlítsák a különböző biztonsági megoldásokat. Az értékelési szempontok a szabvány 2. (biztonsági funkciók) és 3. részében (garanciakövetelmények) szerepelnek.

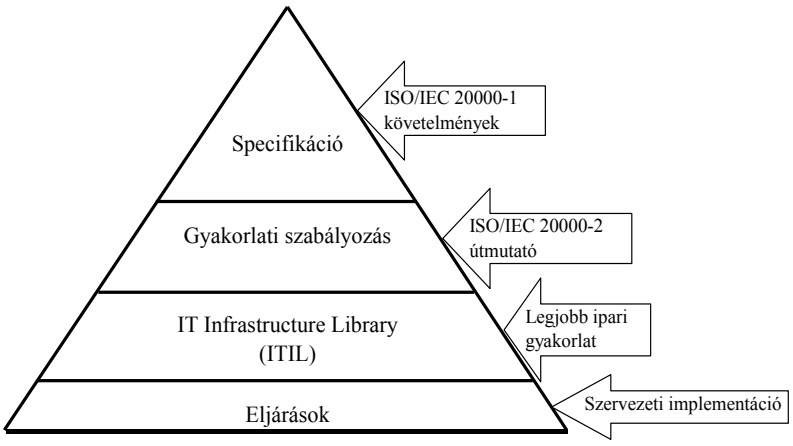
Az **ISO/IEC 2700x** egy brit eredetű információbiztonsági irányítási rendszer, ill. szabványcsomag, amely az információvédelmi tevékenységhez ad útmutatót (www.iso27001security.com). A vállalatok a biztonsági követelményeket és az ezzel kapcsolatos intézkedéseket az üzleti célok és a szervezeti stratégia alapján határozzák meg. Kiemelt szerepet kap az információbiztonság (sértetlenség, bizalmasság és rendelkezésre állás). Nem kötődik egyetlen információtechnológiához sem. A szabvány (**ISO/IEC 27001**) a vállalati működését és az ezzel kapcsolatos követelményeket 11 védelmi területre és ezen belül 39 célkitűzésre és 133 óvintézkedésre osztja. A kialakított és dokumentált információbiztonsági irányítási rendszer tanúsítása független tanúsító szervezet által elvégezhető (ISO/IEC 27002). A szabványcsomagban található még néhány – önálló szabványként megjelenő – kiegészítő rész is (pl. információbiztonsági kockázat kezeléssel kapcsolatos előírások – ISO/IEC 27005). A fejlesztés nem áll meg. Tervezik további szabványok megjelentetését is (pl. bevezetési útmutató –

ISO/IEC 27003; szektorok közötti kommunikáció szabályozása információbiztonsági szempontból – ISO/IEC 27010; a telekommunikáció információbiztonsága – ISO/IEC 27011).

Az **MSZ ISO/IEC 20000-1, -2** szabvány az információs rendszerek üzemeltetési kérdéseivel foglalkozó, brit eredetű ITIL (Information Technology Infrastructure Library) ajánlás alapján ill. azzal összhangban készült (www.itsmfi.org). A dokumentum első része egy formális követelményrendszer az elfogadható informatikai szolgáltatásokkal kapcsolatban, míg a második rész útmutató a szolgáltatásirányításhoz és az első rész szerinti audithoz (3. ábra).

A szolgáltatás menedzsment tevékenységek a ma népszerű, a többi szabványban is alkalmazott PDCA modellhez kapcsolódnak. A menedzsment rendszer, az informatikai szolgáltatások tervezésének és megvalósításának kérdésköre, valamint az új szolgáltatások tervezése mellett öt alapvető területe van a teljes szolgáltatás menedzsmentnek

1. Szolgáltatásbiztosítás (szolgáltatási szint, szolgáltatási jelentések, kapacitás, szolgáltatás folytonosság és rendelkezésre állás, információ biztonság, informatikai szolgáltatás költségtervezése és pénzügyi kezelése)
2. Szabályozási folyamatok (konfiguráció- és változás menedzsment)
3. Kiadási folyamatok (dokumentumok, működési leírások kiadás kezelése, a jóváhagyott változások dokumentálása)
4. Megoldási folyamatok (incidens- és problémakezelés)
5. Kapcsolattartás (ügyfélszolgálat, üzleti- és szállítói kapcsolatok kezelése)



3. ábra
Kapcsolat az ISO/IEC 20000-es szabványcsomag és az ITIL között

Az ISACF (Information Systems Audit and Control Foundation, IT Governance Institute, USA – Információs Rendszerek Ellenőrzésével és Vizsgálatával foglalkozó Alapítvány) kidolgozott egy ajánlást „**COBIT**" (Control Objectives for Information and related Technology – Ajánlás információ technológia irányításához, kontrolljához és ellenőrzéséhez) címmel (www.itgi.org/cobit).

Az anyag gyakorlatilag irányítási eszköz, amely segít megérteni és kezelni az információval, valamint az információ technológiával kapcsolatos kockázatokat és előnyöket. Elsősorban üzleti vállalkozások számára készült, nemzetközileg elfogadott és fejlesztett „keretrendszer", amelynek célja az információ technológiai szolgáltatások és a szervezet működési folyamatainak összehangolása, valamint az informatikai szolgáltatások biztonsági és irányítási jellemzőinek mérhetővé tétele.

A COBIT a legjobb gyakorlatot meghatározott szempontok szerint csoportosító dokumentumok gyűjteménye. A szervezeti (üzleti) célok teljesítéséhez szükséges információk biztosítása érdekében az informatikai erőforrásokat összetartozó eljárások keretében kell kezelni. Segítségével áthidalható az üzleti kockázatok, az ellenőrzési igények és a technikai jellegű kérdések közötti szakadék. A felső vezetés, a felhasználók, az informatikusok és az információs rendszer ellenőrei egyaránt használhatják. A COBIT tényleges célja az informatikai biztonság elérése és megtartása minimális kockázat, ill. maximális haszon mellett…

A felépítés a következő:

- Vezetői összefoglaló
- Keretrendszer
- Részletes kontroll irányelvek (34 eljárás, ill. folyamatra + vezetői útmutatók és érettségi modell + auditálási útmutató, kritikus sikertényezők, kritikus cél és teljesítménymutatók)
- Mellékletek (összefoglaló áttekintés, esettanulmányok, gyakran feltett kérdések)

Az ajánlás 34 „irányítási" célt fogalmaz meg az informatikai folyamatokkal kapcsolatban, azokat négy részterületre bontva:

- tervezés és szervezés
- beszerzés és megvalósítás
- szolgáltatás és támogatás
- figyelemmel kísérés értékelés

A 34 folyamat mellett 215 részletes célkitűzés, ill. kontroll irányelv készült.

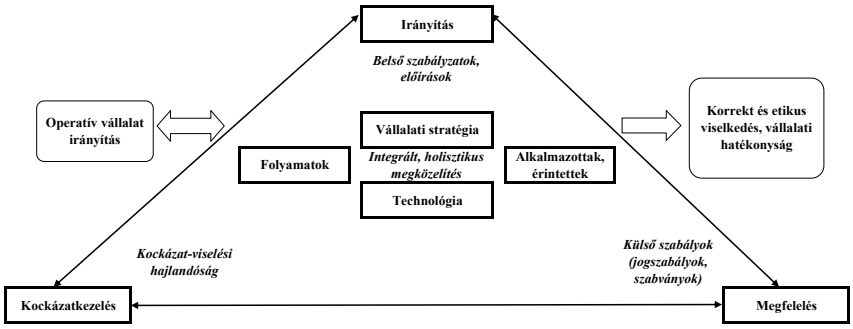
Az információs és kommunikációs technológiák vállalaton belüli irányításához nyújt segítséget az ausztrál eredetű, vezetői keretrendszernek is értelmezhető

nemzetközi szabvány; az **ISO/IEC 38500**. Olyan szabályozási kör alakítható ki a dokumentum alapján (4. ábra), amely az üzleti folyamatok információtechnológiai oldalról történő kiszolgálását felügyeli, értékeli és ez alapján irányítja azt. Foglalkozik a vezetők felelősségével, a vállalati stratégia információtechnológiai vonatkozásaival, információtechnológiai eszközök beszerzésével és azok teljesítményével és az üzleti céloknak történő megfeleléssel, valamint az emberi viselkedéssel is.

A szabvány alapján kidolgozható **GRC modell** elemei a következők

- Irányítás (Governance) – vállalati célok, folyamatok és a folyamatokat működtető szervezet, különös hangsúllyal célok elérését is támogató információtechnológiára (ISO/IEC 38500)
- Kockázatkezelés (Risk Management) – várható események és kockázataik azonosítása valamint elvárható biztonsági szint megfogalmazása az összes vállalati folyamatra, ill. kiszolgáló információtechnológiai eszközökre (COSO ERM)
- Megfelelés (Compilance) – a vállalatnak meg kell felelni a belső előírásoknak és szabályzatoknak, a jogszabályoknak, szabványoknak és szerződéses követelményeknek

A modell alkalmazása egy átfogó, a változó körülményeknek megfelelően folyamatosan alakuló követelményjegyzéket is jelent. A vállalat vezetése tisztában van a kockázatokkal és, hogy adott pillanatban milyen elvárásoknak felel meg. Önfenntartó szabályozási kör, amely kockázatalapú vezetői döntésekhez vezethet. Kezeli a vállalati stratégiát, anyagi és ügyviteli folyamatokat, technológiát, munkavállalókat egyaránt.



4. ábra
GRC modell (Racz et.al., 2010 alapján)

4 Üzletmenet folytonossági és katasztrófa elhárítási tervek

Az információs rendszerek üzemszerű működésének fenntartása érdekében a szervezetek a kockázatokkal összhangban írásos dokumentumokat, forgatókönyveket állítanak össze. Váratlan események bekövetkezésekor ezek alapján állítják helyre az informatikai rendszer normál működését.

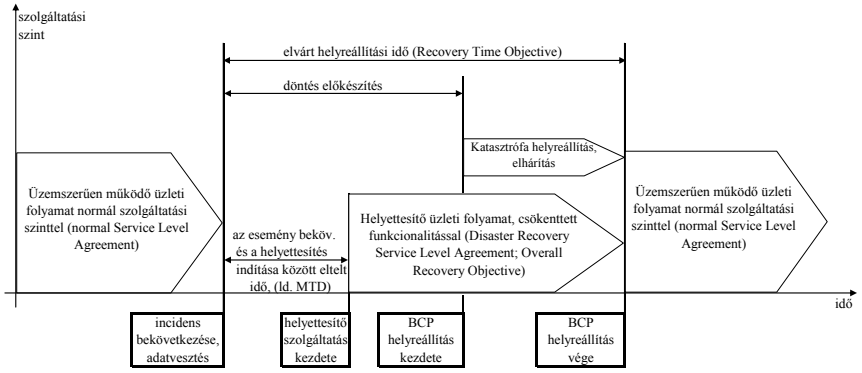
Az **Üzletmenet Folytonossági Terv** (Business Continuity Plan - BCP) célja a szervezeti (üzleti) folyamatokat támogató informatikai erőforrások meghatározott időben és funkcionális szinten történő rendelkezésre állásának biztosítása, valamint a váratlan eseményekből bekövetkező károk minimalizálása. Szükséges a dokumentumban számba venni az egyes folyamatok lehetséges fenyegetettségeit, ezek bekövetkezési valószínűségét, a folyamat kieséséből származó esetleges károkat. Az ún. üzleti hatáselemzés (Business Impact Analysis - BIA) során határozzuk meg a működés fenntartásához szükséges eljárásokat (5. ábra).

A **Katasztrófa Elhárítási Terv**ben (Disaster Recovery Plan - DRP) helyettesítő megoldásokat adunk meg súlyos károkat okozó és az informatikai szolgáltatás tartós meghiúsulását okozó események bekövetkezésére, úgy, hogy a következmények negatív hatásai minimalizálhatók és az eredeti állapot visszaállítása még elfogadható költségek mellett meggyorsítható legyen. Helyettesítő intézkedéseket és eszközöket tartalmaz, ha a szervezet számára kritikus folyamatokat kiszolgáló erőforrások korlátozottan működőképesek, vagy működésképtelenek. Általában a katasztrófa elhárítási terv az üzletmenet folytonossági tervhez kapcsolódik.

A jó BCP, ill. DRP szervezeti folyamatokat vizsgál, valamint számol ezek kapcsolataival. Kockázatarányos, végrehajtható beavatkozási utasításokat tartalmaz. A szervezet felső-vezetése ismeri, elfogadja és betartatja a benne leírtakat. Folyamatosan tesztelik, karbantartják és fejlesztik.

Az üzletmenet folytonossági- és katasztrófa elhárítási tervek elkészítése az összes szervezeti folyamat felmérését megköveteli és több hónapos bevezetési időt igényel. A belső interjúk feldolgozásához és az eredmények rendszerbe foglalásához szükséges lehet külső tanácsadó igénybevétele. A teljes rendszer kialakításához nélkülözhetetlenek a szervezet működését jól ismerő belső szakemberek. Bevezetési és fenntartási költségeik elérhetik a több millió forintot is. Kiemelt feladat a felelős vezetők és a beosztott munkatársak folyamatos oktatása továbbképzése.

Az üzleti hatáselemzés során kockázati szempontból osztályozzuk (alacsony-, közepes-, magas prioritás) a szervezet folyamatait. Meghatározzuk a legnagyobb megengedhető kieső időket (Maximum Tolerable Downtime – MTD). Vizsgáljuk a potenciális fenyegetettségek hatásait és bekövetkezési valószínűségüket is.



5. ábra
Az üzletmenet folytonosság modellje

5 Információbiztonsági irányítási rendszer kialakítása

A szervezeteknek nincs mindig elegendő emberi, anyagi és technikai erőforrása az információvédelem megfelelő kezeléséhez. Ezeknél a szervezeteknél különösen fontos lehet a kapcsolódó tevékenységek, feladatok átláthatóvá tétele. Egy egyszerű, angolszász területeken honos menedzsment módszer alkalmazásával lehet valamit javítani az erőforrások hiánya miatti rossz helyzeten. Az ún. **CATWOE problémaelemzési modell** (lépéssorozat) alapján közelíthetjük meg a kívánt információbiztonságot, ill. információbiztonsági irányítási rendszert (Anas Tawileh et. al. 2007)

C (Vevő-Customer) – Melyik vállalkozásnak lesz információbiztonsági irányítási rendszere?

A (Szereplők-Actors) – Ki fogja kialakítani és működtetni az irányítási rendszert?

T (Átalakítási folyamat-Transformation process) – Melyik az irányítási rendszer legfontosabb célja?

W (Világnézet-Worldview) – Hogyan fogja a vállalkozás elérni ezt a „legfontosabb” információbiztonsági célt?

O (Tulajdonos-Owner) – Ki a tulajdonosa szervezetnek és az irányítási rendszernek?

E (Környezet-Environment) – Mi a környezeti kényszerek hatása az információbiztonsági irányítási rendszerre a szervezeten belül?

Ha tudunk válaszolni a kérdésekre, akkor már „csak" egy négylépéses, visszacsatolással bíró, PDCA ciklushoz hasonló „szabályozási körbe" kell belekényszeríteni a vállalkozást (ld. 6. fejezet eleje)

- a vállalati információbiztonsági célok definiálása
- a szükséges tevékenységek azonosítása
- a tevékenységek végrehajtása
- az információbiztonsági irányítási rendszer felügyelete

5.1 Kritikus vállalati területek

Azoknál a vállalatoknál különösen fontos az információvédelem, amelyek

- működésük alapjául információk szolgálnak, vagy azt alapvetően az adatok és információk határozzák meg
- informatikai úton kapcsolódnak partnereikhez, az elektronikus kapcsolat meghatározó
- a külső kapcsolatokban (pl. logisztikai szervezetek)
- más (pl. kooperációs partner, ügyfél) szervezetek, személyek adatainak fogadásával, feldolgozásával, tárolásával, továbbításával foglalkoznak
- informatikai rendszerek kidolgozását, fejlesztését, üzembe helyezését, telepítését végzik (pl. informatikai cégek)
- olyan kutatási-fejlesztési tevékenységet végeznek, ahol a keletkező eredmény és érték alapvetően információ formájában testesül meg
- bizalmas, személyes információt birtokló, keletkeztető, ezekkel tevékenykedő szervezetek

Ez napjainkban egy újabb területtel egészíthető ki

- mobil eszközöket és internetet – távoli szolgáltatások elérésére – használó vállalatok.

5.2 Auditálás, mint lehetőség

Az auditálás független, a tevékenységre jogosult külső szervezet által végzett felülvizsgálati tevékenység.

Az auditálás különböző szabványok követelményei alapján kiterjedhet a szervezet fő és mellékfolyamataira, az általa folytatott tevékenység környezetvédelmi szempontjaira, a kapcsolódó munkavédelmi kérdésekre, különböző ágazati specifikációk teljesülésére, magára az információ biztonsági irányítási rendszerre az MSZ ISO/IEC27001 követelményei szerint, vagy információtechnikai termékekre, termék családokra az MSZ ISO/IEC 15408 alapján.

Az irányítási rendszereket tanúsító szervezet által kiadott tanúsítvány bizonyíték

- a nemzetközileg elfogadott szabványok szerint elvégzett objektív vizsgálat lebonyolítására, valamint a
- a nemzetközileg elfogadott szabványok követelményeinek való megfelelésre

Az információtechnológiai termékekre vonatkozóan a kiállított tanúsítvány bizonyíték továbbá arra, hogy a termék fejlesztője felelősséget vállal a termékért egy általa vállalt garanciaszintig.

A tanúsítás javítja a szervezet és termékeinek megítélését, hírnevét. Az üzleti partnerekben tartós bizalmat ébreszt a vállalat iránt megalapozva ezzel annak üzleti sikerét.

Az irányítási rendszer auditálása is kiterjed az ügyfelek szempontjainak, követelményeinek teljesíthetőségére, a rendszer által nyújtott garanciák vizsgálatára. A most felsorolt területek átfogják az irányítási rendszer kiépítésekor figyelembe vett követelményrendszer előírásait, ill. ezek megfelelő szabályozását és dokumentálását

- a biztonságpolitika
- kockázat elemzés és kezelés
- üzletmenet folytonossági terv
- katasztrófa elhárítási terv
- alkalmazhatósági nyilatkozat
- adatvédelem, vírusvédelem
- incidensek, események rögzítése, kivizsgálása
- munkakörökhöz, személyekhez kötődő biztonsági előírások, vonatkozó jogszabályok, egyéb (külső) előírások, szakmai ajánlások megléte, ismerete és ezeknek való megfelelés
- adminisztratív (ügyviteli) – környezeti (őrzés-védés) – információs technológiai szabályozások, ismeretek és gyakorlat megléte, ezek egyidejű működése

5.3 A kialakítás lépései (összefoglalás; részletesen ld. 6. fejezet)

- Információvédelmi átvilágítás vezetői döntés alapján, ideiglenes szervezet kialakítása és kockázati tényezők meghatározása
- Kockázatértékelés és elemzés (védelmi igény meghatározása, fenyegetettség vizsgálat, kockázatkezelési módok meghatározása)
- Dokumentálás (információvédelmi célok és politika meghatározása, kockázati és védelmi területek definiálása, folyamatok és felelősségek rögzítése, ellenőrzési rendszer kidolgozása →üzletmenet folytonossági és katasztrófa-elhárítási tervek
- Bevezetés (szabályozás hatályba léptetése, oktatás, belső auditok és vezetői átvizsgálások rendjének kidolgozása)
- Auditálás

Az információbiztonsági irányítási rendszert bevezető és üzemeltető szervezetben a következő „munkakörök" szükségesek:

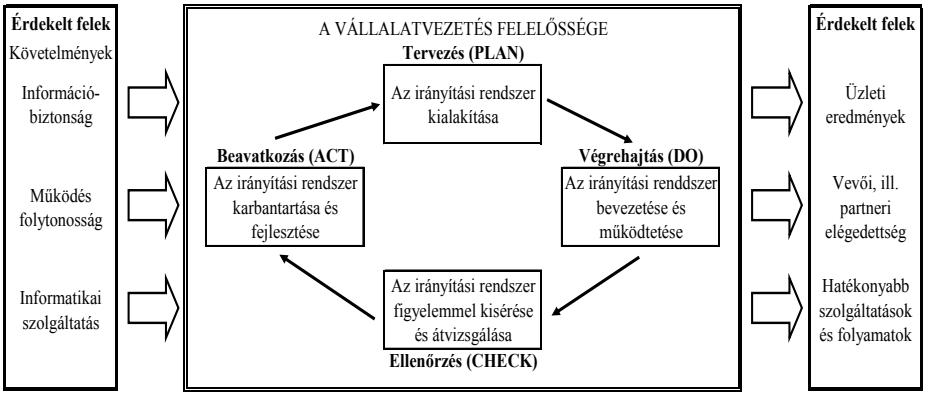
- információvédelmi vezető
- adatvédelmi felelős
- IT biztonságért felelős vezető
- funkcionális területek vezetői
- adatgazdák
- belső auditorok

Integrált (környezet-, minőség- és információbiztonsági) irányítási rendszerek esetében javasolt közös szervezet kialakítása.

6 Integrált irányítási rendszerek

Az ISO szabványokra épülő menedzsment rendszerek a részfolyamatokat, a mellékfolyamatokat és szabályozási rendszer elemeket hangolják össze, biztosítva, hogy a menedzsment képes legyen folyamatos felügyelet és rendszeres ellenőrzés alatt tartani tevékenységének meghatározó elemeit képező folyamatokat, eszközöket és erőforrásokat. A rendszerszabványok együttes, integrált alkalmazása összetettebb feladatok megoldását is lehetővé teszi. Egy időben valósulhat meg a fő- és mellékfolyamatok felügyelete, a folyamatképesség fenntartása és fejlesztése, a hibamentesség elérése, erőforrások felhasználásának csökkentése, kiadások csökkentésével a nyereségesség növelése, munkakörnyezet

fejlesztése. Jelentkezhet egyéb, szintén a felső vezetés feladatkörébe tartozó terület hatékony és egységes kezelésének igénye is, mint pl. a pénzügyek, a likviditás, gazdasági döntések, jogi környezet változásainak kezelése, logisztika, motivációs technikák alkalmazása, kommunikáció és marketing. A **PDCA** (Plan-Do-Check-Act) modell alapú, folyamatközpontú integrált irányítási rendszerek egyik fenntartó eleme az információtechnológiai infrastruktúra használata.



6. ábra
PDCA modell információbiztonsági folyamatokra

Kialakításával a komplex feladatok menedzselése egyszerűbbé, átláthatóbbá, eredményesebbé és hatékonyabbá válik, az értékteremtés rendszerének részeként hozzájárul az üzleti elvárások, a versenyelőny megszerzésének megvalósításához (6. ábra).

Az ISO/IEC 2700x szabványcsomag folyamatos átalakításának, fejlesztésének egyik nem titkolt célja a különböző szabványos irányítási rendszerek (pl. minőség- és környezetirányítási rendszerek) egységes alapon történő kezelése, valamint az üzleti folyamatok többszörös szabályozásának elkerülése. Az ISO/IEC 27001-es szabvány mellékletében egy a szabványok közötti kapcsolatot, ill. felépítésük hasonlóságát bemutató táblázat található. Már Magyarországon is sok szervezet alakít ki és működtet ún. integrált irányítási rendszereket. A kisebb, nem túl tőkeerős vállalatoknak vélhetően ez az egyik járható út, hogy megfeleljenek az üzleti környezetük elvárásainak. Az irányítási rendszerek ellenőrzése, előauditjai és háromévente ismétlődő tanúsítása magában hordozza a szervezet folyamatos fejlődésének lehetőségét.

Az on-line vállalati kapcsolatok bővülése miatt a kisebb szervezeteknél megfigyelhető, hogy az IT rendszerek felügyeletét (informatikai biztonság) és az üzleti folyamatokhoz kapcsolódó információbiztonságot szeretnék egységes szabályozás szerint kezelni.

Az integrált irányítási rendszer kialakításából és működtetéséből számos, általában nem számszerűsíthető előnye származhat a vállalatoknak:

- egységes dokumentációs rendszer
- párhuzamos „ügyviteli" szabályozások megszűnése
- folyamatközpontúság
- racionális ellenőrzési lehetőségek és megelőzési tevékenységek
- egyértelmű felelősség- és hatáskör meghatározás
- fokozott szállítói és vevői bizalom
- potenciális piaci versenyelőny
- csökkenő auditálási idő és költség
- átfogó jogkövető tevékenység

A szabványos irányítási rendszerek bevezetésében sok a hasonlóság.

Helyzetfelmérésnél minden esetben külső és belső folyamatokat elemzünk. A szabályozott, dokumentált folyamatok átlátható szervezetet hoznak magukkal. A részletesen kidolgozott szabályozás rugalmasabb vállalati működést, átalakult szervezeti kultúrát, reprodukálható és dokumentált fő- és mellékfolyamatokat, valamint munkatársakra lebontott felelősségi köröket eredményez. Az irányítási rendszer ellenőrzése és ismételt tanúsítása biztosítja a szervezet folyamatos fejlődését és a partnerek elégedettségét (jobb minőség, környezetkímélő működés v. információk rendelkezésre állása).

6.1 Szabványos irányítási rendszerek és a befogadó vállalati környezet

A mai vállalatoknak számos megfelelési kényszere van. Az alapítás jogi feltételeinek teljesítése mellett sokrétű, egymást átfedő – néha egymásnak ellentmondó célokat megfogalmazó – követelményrendszernek kell megfelelniük egyszerre. A teljesség igénye nélkül az alábbi „irányítási rendszerek" szabályozhatják a vállalatok működését:

- pénzügyi előírások és likviditási kényszer
- számviteli szabályok és tulajdonosi elvárásokból adódó nyereségesség igénye
- várható piaci igényeken és a vállalati erőforrások kihasználásán alapuló, különböző időhorizontú üzleti, ill. termelési tervek
- különböző funkcionális területeket szabályozó – tervező és visszacsatolásszerű ellenőrzést támogató – kontrolling rendszerek

- stratégiai döntéstámogató rendszer (Balanced ScoreCard), amely pénzügyi oldal megfelelő működése mellett figyelembe veszi, ill. méri a vevői elégedettséget, a vállalati folyamatokat és a rendelkezésre álló emberi erőforrás minőségét is
- vállalati folyamatok belső szabályozása (Szervezeti és Működési Szabályzat, ügyviteli előírások, workflow, vállalati információs rendszerek)
- speciális iparágak (pl. energetikai gépgyártás, élelmiszer- és gyógyszeripar) termeléséhez és készletgazdálkodásához köthető biztonsági és termeléskövetési előírások
- jogi szabályozások a környezet- és fogyasztóvédelem, valamint a foglalkoztatás és adózás területén (pl. hulladékkezelés, jótállás, szavatosság, termékfelelősség, termékek forgalomba-hozatali engedélyeztetése, vevőszolgálati elvárások)
- vevők egyedi, minőséggel, szállítási készséggel és kommunikációs képességekkel (pl. EDI, extranet) kapcsolatos igényei, előírásai
- munkavállalói elvárások (kollektív szerződés, vállalati kultúra)
- beszállítókkal és kooperációs partnerekkel történő kapcsolattartás esetleges kötöttségei

Ebbe az összetett módon szabályozott vállalati környezetbe kerülhetnek kialakításra – elsősorban vevői, partneri és esetenként tulajdonosi elvárások alapján – a hasonló felépítésű szabványokon alapuló irányítási rendszerek (minőség-, környezet- és információvédelem irányítása).

6.2 A projekt indítása

Az új (pl. információbiztonsági) irányítási rendszer kialakításának igénye adódhat üzleti partnerek elvárásaiból, de lehet belső vállalati késztetés is. Mindkét esetben fontos a felső- és középvezetők meggyőzése a projekt szükségességéről. Ez azért is nehéz, mert a rendszer üzemeltetéséből adódó haszon nehezen számszerűsíthető. A rendszer bevezetéséhez több vállalati „szakterület” (szervezés és vezetés, ügyvitel, információtechnológia, vagyonvédelem, belső vállalati kommunikáció, jogi szabályozás) összehangolt munkájára van szükség.

Előnyt jelenthet, ha már van valamilyen nemzetközi szabványon alapuló irányítási rendszer. A korábbi bevezetés, ill. tanúsításra történő felkészülés tapasztalatai hasznosíthatók.

A bevezetéssel megbízott csoport összeállításánál figyelni kell:

- beosztott emberi erőforrások szükséges mennyiségére

- inhomogén összetételű, de a szervezeti hierarchia közel azonos szintjén álló szakemberekből összeállított projektcsoport kialakítására (a szervezet minden funkcionális területről legyen nem vezető beosztású, de kellő vállalat-specifikus ismerettel bíró tag…). Ez a későbbi munkamegosztás szempontjából fontos. A csoport tagjait meg kell ismertetni az irányítási rendszerekkel foglalkozó szabványokkal. Ez már a projekt elején felveti külső – ilyen területen referenciával bíró – tanácsadó cég bevonásának szükségességét…

A rendszer kiépítésének első lépése a vezetői döntés és a munkát elvégző ideiglenes szervezet kialakítása után az információvédelmi átvilágítás és helyzetfelmérés.

Általánosságban elmondható, hogy az irányítási rendszerek kiépítésének előkészítő fázisában alapvetően a védelmi igény feltárása, a fenyegetettség-elemzése, a kockázatelemzés és a kockázat kezelés témakörei kerülnek terítékre különböző formában, melynek során a következő alapvető kérdésekre keresünk választ:

- Milyen jellegzetességekkel bír az alkalmazott információ-, ill. adatkezelési gyakorlat?
- Képes-e a szervezet információtechnológia rendszere zavartalanul, megfelelő szinten ellátni az összes külső és belső információszolgáltatási igényt, amely a szervezet működésével kapcsolatban felmerül, vagy megfogalmazható?
- Adatbiztonsági szempontból megfelelő színvonalú-e a rendszer?
- Megfelelően szabályozott-e az adatokhoz való hozzáférés joga és annak módja?

Az információvédelmi átvilágítás „információtechnológiai csoportosításban” érinti a környezeti infrastruktúra, az adathordozók, a hardver, a szoftver, a dokumentumok, az adatok, a kommunikáció, és az emberi tényezők területét is.

Az átvilágítás információvédelmi fejezetének fontos része a részletes és minden egyes informatikai elemre és kapcsolatra kiterjedő hardver-, szoftver-, és kapcsolatrendszer „leltár” felvétele, amely alapján érdemben lehet a „fenyegetettség-veszély” meghatározást és elemzést elvégezni, valamint a szükséges szabályozó rendszert kialakítani.nformációvédelmi átvilágítás vezetői döntés alapján, ideiglenes szervezet kialakítása és kockázati tényezők meghatározása.

6.3 Projekt-tervezés és a megvalósítás kezdeti lépései

Első lépés a **projekt céljának meghatározása és elfogadtatása**, az előzmények és vállalati adottságok figyelembevétel; információvédelmi irányítási rendszer megtervezése, kialakítása és működtetése.

Ezek után következhet a szükséges tevékenységek, azok időadatainak és logikai kapcsolataiknak a megállapítása. Természetesen minden irányítási rendszer kialakítása helyzetfelméréssel kezdődik, amely „információbiztonsági" esetben az információs vagyonelemek (ingatlan, hálózati eszközök, munkatársak tudása és képessége, hardver és szoftver eszközök, adatbázisok…) számbavételét jelenti. Ehhez ismerni kell a vállalati folyamatokat, a folyamatok elemeihez tartozó be- és kimenő információkat. Kik az információszolgáltatók és az információfogadók? Milyen információtechnológiai elemek támogatják a folyamatok végrehajtását? Vizsgálni kell a működés közben előforduló eseményeket is (normál üzem, üzemszünet, hiba, üzemzavar, leállás, üzemképtelenség, katasztrófa).

Az előbbiek előre vetítik a kockázatértékelést, a lehetséges fenyegetettségek összegyűjtését, különös figyelemmel az információ sértetlenségére, a rendelkezésre állására és a bizalmas kezelésére. Kockázatértékelésnél – ami történhet szervezeti egységenként, eseményenként vagy akár folyamatonként is – a várható eseményeket osztályozni kell súlyosság, gyakoriság és észlelhetőség szerint.

A **kockázatértékelés** során megállapítják a vizsgálati területeken értelmezhető gyenge pontokat és fenyegető tényezők, megtörténik ezek értékelése, elemezése, rangsorolása. Csoportosítják az egyes fenyegetettségekhez kapcsolódó esetleges károkat és kockázatokat. Hozzárendelik a kivédésükhöz, elfogadható mértékre történő csökkentésükhöz és kezelésükhöz szükséges és/vagy lehetséges intézkedéseket.

Ennek megfelelően a kockázatértékelés és elemzés lépései az alábbiak:

- a védelmi igény feltárása, az információvagyon meghatározása, a szervezet számára kiemelten fontos adatok feltárása és ütemezése
- fenyegetettség elemzés; a fenyegető tényezők összegyűjtése
- kockázatelemzés; a fenyegetettség hatásainak vizsgálata
- kockázatok kezelése és a védelmi intézkedések meghatározása; a kockázatok kivédése, ill. minimalizálása a kockázatelemzés alapján a lehetséges módozatok meghatározásával

Az elemző munka végén a team tagjai tájékoztatják felsővezetőket az elvégzett munkáról és megpróbálják meggyőzni őket néhány kiemelten fontos kockázat, ill. legnagyobb fenyegetések elleni védelmi intézkedés szükségességéről. Ha ez zöld utat kap, akkor meg kell adni az intézkedés felelősét, határidejét és tényleges

célját. Ez ismétlődő feladat. A védelmi intézkedéseket és a kockázatértékelést rendszeresen, általában évente felül kell vizsgálni.

Az irányítási rendszer egyik legfontosabb eleme a kapcsolódó dokumentumok (információvédelmi kézikönyv, információvédelmi szabályzat) összeállítása, amelynél érdemes a már említett szabványra támaszkodni. Az ún. „alkalmazhatósági nyilatkozat" az mutatja az összefüggést a szabvány követelményei és a kialakított szabályozás között. Nyilatkozni kell továbbá, hogy a szervezet melyik szabványpontoknak nem kíván megfelelni. A dokumentáció elkészítése, többszörös, ill. többszintű ellenőrzése és átdolgozása az egyik leghosszabb projektlépés, akár több hónapot is igénybe vehet. Felhasználhatók az esetleg már meglévő környezet- és minőségirányítással kapcsolatos „tanúsított" dokumentumok.

Az elfogadás után hagyjunk időt az összes érintett munkatárs oktatására is… Fel kell készíteni őket a vállalati kultúra eseteges változására!

A kialakítandó irányítási rendszer, ill. dokumentáció csomag három fő területre fókuszál

a. személyekkel kapcsolatos védelem (átvilágítás munkaerő felvételnél, rendszeres oktatás, felkészülés a rendkívüli helyzetekre, naprakész jogosultsági rendszer…)
b. fizikai és környezeti biztonság (vagyontárgyak nyilvántartása és osztályozása, a szervezet telephelyeinek és infrastruktúrájának védelme, jogosulatlan hozzáférés megakadályozása, karbantartás…)
c. ún. üzletmenet-folytonosság menedzsment az üzemszerű működés fenntartásának érdekében (üzletmenet-folytonossági és katasztrófa elhárítási tervek)

A **dokumentáció** elkészítése során szükséges figyelembe venni a szervezet nagyságát és struktúráját, a folyamatok összetettségét és azok kölcsönhatásait, a szervezet működésére vonatkozó külső- és belső előírásokat, a szakmai sajátosságokat és hagyományokat.

Dokumentációs és szabályozórendszer kialakítása az általános célok elérése mellet a szervezet működésének és védelmi céljainak függvényében konkrét feladatok megvalósítását igényli, melybe bele tartozik:

- a védelmi igények és követelmények, valamint a védendő értékek (pl. alkalmazás, adatok hardver, szoftver, adathordozó, dokumentumok, személyi és szervezeti környezet, építészeti környezet, kommunikációs rendszerek, eszközök, szervezeten belüli személyi kockázatok) felmérése alapján történő kockázatelemzés
- az információvédelemi célok és politika meghatározása

- a rendszer érvényességi területének, valamint egységes vezetői elvek és szabályok rögzítése egy vezetői kézikönyvben, mely összefoglalja az irányítási rendszer folyamatait és rögzíti a rendszer elemeinek kapcsolatát, meghatározva a kapcsolódó feladatokat és azok felelőseit
- kockázati- és védelmi területek és szintek meghatározása
- a célok és a működés ismeretében a kapcsolódó folyamatok, módszerek és szabályozások (pl. géptermi belépés rendje, archiválási utasítás, jelszókezelés rendje, informatikai szabályzat) kidolgozása
- az információvédelemhez rendelt feladatok és a kapcsolódó felelősségek meghatározása
- a rendszer tervezett és automatikus felügyeletének, valamint eseti ellenőrzésének kialakítása, az elfogadási kritériumok rögzítése
- a hibák felismerése és a szükséges válasz-intézkedésekhez kapcsolódó prioritások meghatározása
- a feljegyzések kezelési rendjének kialakítása, mellyel a szervezet biztosítja a kívánt információvédelmi célok elérésének megfelelő dokumentálását, igazolja az előírt követelményeknek való megfelelést és bizonyítja az információvédelmi rendszer hatásos működését, alkalmazhatósági nyilatkozat kidolgozása, melyben kifejtésre kerül, hogy a rendszer hogyan tesz eleget a funkcionális követelményeknek, ill. a megvalósítás és az üzemeltetés hogyan felel meg a kitűzött biztonsági céloknak

6.4 Projekt- és az irányítási rendszert üzemeltető szervezet

A kialakítandó projekt-szervezet és később az információvédelmi irányítási rendszer „üzemeltetésért” felelős szakemberek száma függ a szervezet profiljától és nagyságától (létszám, vagyonelemek száma) is. Az információvédelmi irányítási rendszer folyamatos fejlesztése érdekében előnyös, ha létrejön egy rendszeresen együttműködő „fórum”, amelynek a munkájában részt vesz:

- az információvédelmi vezető
- az adatvédelmi felelős
- az IT biztonságért felelős vezető
- a funkcionális területek vezetői és az ún. „adatgazdák”

A fórum véleményezi az információkhoz történő hozzáférést szabályozó jogosultsági rendszert, kijelöli azokat a területeket, amelyeket információvédelmi szempontból fontosak (pl. értékesítési-, megrendelési és outsourcing szerződések

kezelése), és gondoskodik a védelmi rendszer vállalati felülvizsgálatáról (belső és külső audit). Ez utóbbihoz kiképzett belső auditorok is szükségesek.

A szabványok felépítésének hasonlósága miatt előnyös integrált irányítási rendszereket és ezzel foglalkozó összevont szervezetet létrehozni, úgy, hogy az információvédelem (estenként az információ technológia kezelése is), a környezetvédelem és a minőségbiztosítás egy kézben legyen. Ez a felállás teljesen új, holisztikus gondolkodást igényel a szervezet vezetőitől.

Az irányítási rendszer bevezetése során a szabályozások elkészítésével együtt és azt követően számos gyakorlati feladatot szükséges elvégezni, többek között:

- a szabályozás hatályba léptetése, az alkalmazásukkal és a menedzsment rendszer működésével kapcsolatos ismeretek oktatása és az elsajátítás mértékének meghatározása
- a kialakított szabályozási rendben rögzítettek rutinszerű alkalmazásának bevezetése, és felügyelete
- fizikai védelem rendszerének kialakítása, üzletmenet folytonosság biztosítása háttérszerződésekkel, fejlesztések-, eszközcserék-, eszköz elidegenítés és megsemmisítés-, külső terminálok-, mobil eszközhasználat- stb. biztonsági követelményeinek biztosítása, alkalmazottakkal kapcsolatos védelmi módozatok kimunkálása és bevezetése
- a belső auditok lebonyolításához szükséges team és ellenőrzési rend kialakítása, az ehhez szükséges jogosultságok és erőforrások biztosítása a vezetés részéről, a kapcsolódó oktatások megtartása
- vezetői átvizsgálás lebonyolítása, majd a vizsgálat eredményei alapján a következő periódus fejlesztési céljainak meghatározása

Az általános szempontok alapján az alábbi területek szabályozása indokolt az irányítási rendszer kialakítása során:

- dokumentumkezelés
- humánpolitikai tevékenység
- az információkezelő eszközök védelmi osztályozása, fizikai és környezeti védelem
- a tevékenységek tervezése, fejlesztése, az információkezelés rendszerének fejlesztése,
- beszállítói szerződéskötések rendje és a beszállítók minősítése
- a „szabványos” munkafolyamatok
- az integrált irányítási rendszer felülvizsgálata

- a munkafolyamatok ellenőrzése és vizsgálata
- biztonsági zavarok, működési hibák kezelése
- a helyesbítő és a megelőző tevékenység

A 3. fejezetben tárgyalt nemzetközi szabványok és szakmai ajánlások alapján kidolgozott információbiztonsági irányítási rendszer segítheti a nonprofit szervezetek és üzleti vállalkozások beilleszkedését a környezetükbe és a velük szemben támasztott elvárásoknak történő megfelelést. A térnyeréshez vagy a pozíció megtartásához szükséges információtechnológiai- és folyamatfejlesztések könnyebben elvégezhetők, hiszen van egy követelményrendszert kiegészítő, ill. teljesítő szabályozás.

Az egymáshoz látszólag alig kapcsolódó szabványok és ajánlások közös alkalmazása azért is indokolt, mert az ellátási láncok integrált információs rendszereinek optimális működése nemcsak információtechnológiai kérdés. A hálózatba szervezett vállalatok számára létfontosságú, hogy ki, mikor és hogyan férhet hozzá a számára szükséges információkhoz, ill. mikor indíthat el vagy nyúlhat bele egy vállalaton belüli vagy vállalatok közötti üzleti tranzakcióba. A kockázatok kezelése nem szétválasztható az anyagi- és információs folyamatokban valamint az információtechnológiában.

6.5 Tanúsítás

A bevezetési projektnek kettős célja van. A működő információvédelmi irányítási rendszer létrehozása mellett fel kell készíteni a szervezetet egy független - esetenként külföldi - auditor látogatására is. Az auditálás általában több napig tart. A szabványban megadott pontok szerint vizsgálják a szervezetet, ill. az elkészített eljárásokra vonatkozó dokumentációt. Ez utóbbinak a megléte gyakran fontosabb, mint a logikusan felépített folyamatok kialakítása és működtetése. Az információtechnológia, ill. az informatikai szakemberek tevékenysége a szabványcsomagban megfogalmazott filozófia ellenére kiemelt szerepet kapnak (pl. a help-desk tevékenység eseményeinek naplózása...). Az egyébként háromévente ismétlődő külső tanúsítást egy – elsősorban felkészülést szolgáló, általában egynapos – belső audit előzheti meg, ami dokumentáció vizsgálatból és ún. helyszíni auditból áll. Célja a hibák feltárása és orvoslása, valamint a „biztonság-tudatosság" javítása a szervezeten belül. Az információvédelem az irányítási rendszerrel közvetlen kapcsolatban nem álló munkavállalók számára elsősorban a „tiszta asztal, tiszta képernyő" követelményét jelenti…

A tanúsítások kritikus területei, ill. jellemző hibái a következők lehetnek:

- nem tisztázott az információvédelmi irányítási rendszer (Information Security Management System – ISMS) alkalmazási területe
- nem teljes a vagyontárgyak és ezek tulajdonosainak azonosítása

- nem megfelelő az indoklás a kockázatokhoz (felmérés és kezelés) kapcsolt - a szabvány mellékletéből kiválasztott - óvintézkedések esetében
- az üzletmenet folytonosság szabályozásánál kritikus eszközök maradnak ki
- papíralapú adathordozók szerepének figyelmen kívül hagyása
- többszörös, de eltérő szabályozások
- nincsenek felelősök és határidők…
- formai hibák (verziószám, fejléc, oldalszám, dátum hiánya) a dokumentációban

6.6 Közös elemek a minőség-, környezet- és az információvédelem irányítási rendszerekben

A szervezetek egyik alapvető célja, hogy kielégítse partnereinek igényeit. A különböző irányítási rendszereket és tanúsítási követelményeiket leíró szabványok ehhez nyújthatnak segítséget. Közös jellemzőjük a folyamatközpontú megközelítés. Mindegyik az ISO 9001 felépítését követi. A szabványok végén található mellékletek a tartalomjegyzékek pontjait követve ezt a kapcsolatot részletesen bemutatják. A szabványalkotók egyik célja, hogy integráltan - a többszörös, egymástól eltérő szabályozást elkerülve - is bevezethetők legyenek ezek az irányítási rendszerek.

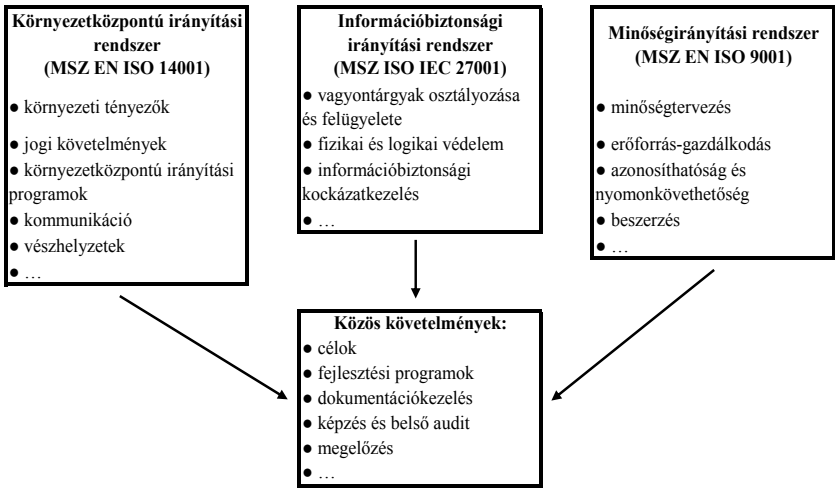
A bevezetés menete és a várható eredmények jellege mindhárom irányítási rendszer esetében hasonló;

A helyzetfelmérés során megismerik, tisztázzák és rögzítik az érintett területekhez kapcsolódó folyamatokat, ill. ezek szabályozását. Ez alapján kerülnek meghatározásra az elvégzendő feladatok.

A rendszer kialakítása a szabványoknak megfelelő szabályozott folyamatokat, átlátható szervezetet, minőségközpontú és/vagy környezettudatos, ill. információvédelemmel kapcsolatos kockázatkerülő v. megelőző működés alapjainak dokumentált lefektetését jelenti (kézikönyvek elkészítése).

Az érintett munkatársak képzésével egy időben folyik a szabályozások részletes kidolgozása és a működési feltételek megteremtése. Ez a külső igényeknek (partnerek által támasztott elvárások, jogszabályi előírások) történő megfelelést és szabályozott működést (reprodukálható és dokumentált termelés/szolgáltatás, átalakult szervezeti kultúra, munkatársakra lebontott információvédelemmel kapcsolatos felelősségi körök) hozhatja magával.

A kialakított irányítási rendszerek ellenőrzése, ún. előauditjai és ismétlődő tanúsítása magában hordozza a folyamatos fejlődés lehetőségét és kényszerét. Mindhárom irányítási rendszer bevezetése után nőhet a vevők, szállítók, egyéb partnerek elégedettsége és bizalma. Az **ISO 9001** alkalmazása esetenként költségcsökkentést, az **ISO 14001** környezetkímélő működést, az **ISO 27001** pedig az információk jogosultságnak megfelelő rendelkezésre állását eredményezi (7. ábra).



7. ábra
Integrált irányítási rendszer elemeinek kapcsolódásai

7 Információbiztonság és versenyképesség

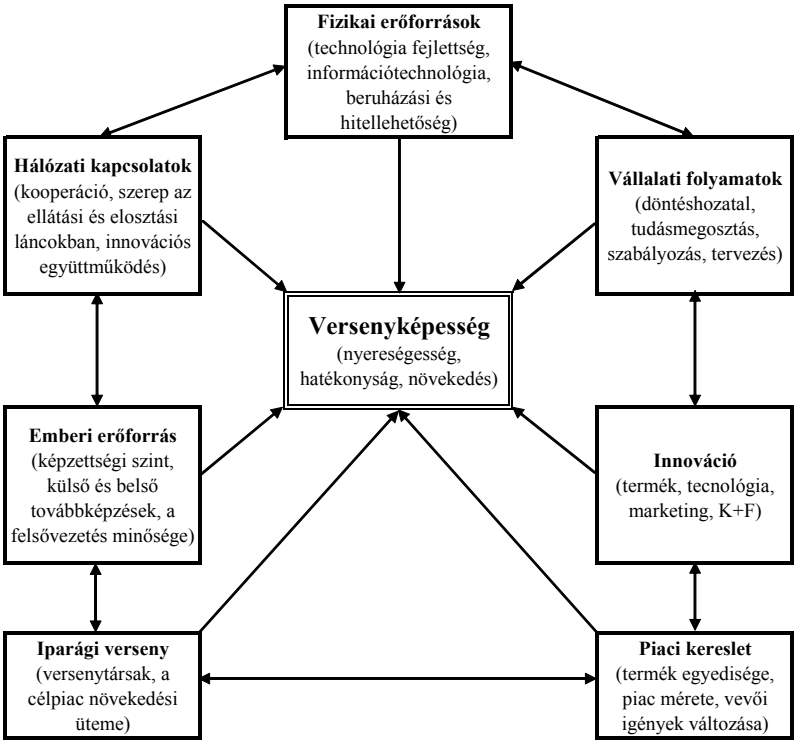
„Egy nemzetgazdaságban azokat a vállalatokat tekintjük versenyképesnek, amelyek társadalmilag elfogadható normák betartása mellett a számukra elérhető erőforrásokat minél nagyobb nyereségfolyammá képesek transzformálni, képesek a működésüket befolyásoló környezeti és vállalatukon belüli változások észlelésére és az ezekhez való alkalmazkodásra annak érdekében, hogy nyereségfolyam lehetővé tegye tartós működőképességüket." (Chikán-Czakó-Zoltayné, 2002.) A meghatározás a vállalati versenyképesség alapvető, de nem kizárólagos tényezőjének a nyereséges gazdálkodást tekinti. Fontos lehet az alkalmazkodóképesség is, amelynek egyik fokmérője lehet a működő, szabványokon alapuló irányítási rendszerek megléte.

Szerb László és szerzőtársa szerint a versenyképesség méréséhez egy minden részletre kiterjedő, többtényezős versenyképességi modellre van szükség, amely

szinte minden mérhető és nem mérhető szempont szerinti elemzést egyaránt megkövetel (8. ábra).

A vizsgálandó versenyképességi területek a következők:

- Fizikai erőforrások
- Vállalati folyamatok
- Innováció
- Piaci kereslet
- Iparági verseny
- Emberi erőforrás
- Hálózati kapcsolatok



8. ábra
Versenyképességi modell (elsősorban kis- és közepes vállalkozásokra; Szerb-Ulbert, 2009.)

Külső és belső tényezőkhöz egyaránt kapcsolhatók az irányítási rendszerek kialakítása. Az üzleti partnerek jogos elvárása lehet harmadik, külső fél által auditált környezet-, minőség- vagy információbiztonsági irányítási rendszer tényleges működése (pl. stratégiai beszállítói partnerség v. közbeszerzési eljárások feltételrendszere). A jó értelemben vett bürokratikus belső szabályozás hiánya vagy a szervezet működési zavarai is kikényszeríthetik ezek létrehozását és működtetését.

A hazai vállalkozások megváltozott gazdasági környezetének néhány jellemzője:

- vállalkozások alultőkésítettsége
- fizetőképes kereslet csökkenése
- nagyfokú bizalomhiány
- manipulált globális tőke dominanciája

Ennek hatása többek között a kis és közepes vállalkozások a piacról történő kiszorulásában, a lokális érdekek háttérbe szorulásában, és a bővítési törekvések számának csökkenésében jelentkezik.

A vállalkozások problémáinak megoldását egy racionálisan felépített, több szempontot is követelményrendszerébe integráló menedzsment rendszer alkalmazása is elősegítheti. Ennek hatékonysága különböző gyakorlatorientált megoldásokkal tovább fokozható. A versenyképesség biztosítása tehát nem egy feladatsor mechanikus teljesítését jelenti, hanem a gazdálkodó szervezet stratégiai céljainak elérését szolgáló összetett folyamatrendszer menedzselését változó gazdasági, piaci és kulturális viszonyok között.

A problémák kezelését Magyarországon két fontos tényező befolyásolja; a **bizalomhiány és a szervezeti folyamatok nem „egyenszilárdságú" felügyelete**. Ezek a gondok a meglévő irányítási rendszer(ek) – egyéni igényektől függő – információvédelem-központú átalakításával, bővítésével viszonylag egyszerűen orvosolható, még szűkös anyagi erőforrások mellett is.

A két tényező jelentősége nem elhanyagolható, mert külön-külön történő megjelenésük esetén is képesek befolyásolni a szervezetek piaci jelenlétét, működésének eredményességét.

Az információvédelem rendszerbe foglalt alkalmazása képes jó hatásfokkal javítani ezen az állapoton.

A szabályozottság, a vállalati folyamatok működése és felügyelete, valamint a visszacsatolás kapcsolatrendszere meghatározza a megfelelő működést az értékteremtési láncban. A „szabályozási körben" fontos, hogy a döntési pontokon rendelkezésre áll-e szükséges és elégséges információ. A vállalati információrendszer működése utal arra is, hogy a vezetés képes-e a szervezet működésével kapcsolatos releváns tényezőket gyűjteni, kiválasztani és reálisan

értékelni, valamint az ebből nyert következtetéseket az érintettekkel megosztani (Lábodi-Nahlik, 2008).

A piaci szereplők közötti bizalomhiány, mely a társadalom felszíne alatt meghúzódó morális válságból eredeztethető. Ennek kezelése hosszú folyamat, melynek eredményei nagyon ritkán érhetőek tetten. Kezelésük azonban a gazdaság működése szempontjából meghatározó jelentőségű.

A profitorientált szervezetek tevékenységeiben alapvető fontosságú a vevői igények és a piaci követelmények ismerete. Ebben jelentős szerepet kell kapnia a partneri bizalom megszerzésének és megtartásának. Jó példát jelenthet az a versenyelőnyt szerzett, takarítást végző vállalkozás, amely alkalmazottaival szembeni követelményeit és a munkavégzés körülményeit a potenciális megbízók igényei szerint alakította ki, figyelembe véve az információvédelem szempontjait is. Itt a védendő érték, információ nem a szolgáltató vállalkozás birtokában van. **A vevők, ügyfelek felé irányuló kommunikáció tartalmazza a megbízhatóságra utaló elemeket.** „Minket válassz, mert mi megbízhatók vagyunk…!" A megszerzett versenyelőnyt meg is kell tartani…! Bizalmi termékek vagy szolgáltatások piacán elszenvedett presztízsveszteség romboló hatású lehet a társaság hosszú távú terveire vonatkoztatva. Nem elég a kommunikációban megjeleníteni a biztonságot, hanem fenn is kell tudni azt tartani a tartós versenyelőny érdekében.

8 Kis- és közepes vállalkozások (KKV) információbiztonsága

A kis- és közepes vállalkozások „meghatározást" az Európai Unió gyakorlatához igazodva 2004. évi XXXIV. törvény szabályozza. A mikro- és kisvállalkozások kategóriahatárainak bemutatását átlépve, a tanulmány szempontjából lényeges megállapítás, hogy közepes vállalkozásnak tekinthető az a cég, amelynek az alkalmazotti létszáma nem haladja meg a 250 főt, éves nettó árbevétele kevesebb, mint 50 millió euró, valamint a mérleg-főösszeg maximum 43 millió euró. A tényleges magyarországi KKV szektorban - egyéni- és mikro-vállalkozásokat leszámítva - közel 30 ezer vállalkozás van. Számos hazai és nemzetközi felmérés bizonyítja, hogy a vállalatok nem foglalkoznak megfelelő súllyal az informatikai-, ill. információbiztonsággal.

A helyzet különösen a kis- és közepes vállalkozások (KKV) esetében lehangoló (Symantec SMB Disaster Preparedness 2011). Üzleti környezetük és a velük szemben támasztott elvárások gyorsan változnak, ráadásul az ilyen szervezetek méretükből adódóan rugalmasabbak, mint a nagyvállalatok. Az információvédelmi tevékenységük (ill. annak hiánya) kisebb kockázatú ugyan, de állandó felügyeletet és megújulást igényel. A fizikai biztonság, ill. védelem a

megfelelő környezet kialakítását jelenti, a szándékos vagy vétlen károkozás ellen, ill. katasztrófahelyzetben.

A logikai biztonság, ill. az ehhez kapcsolódó operatív védelem területei a következők:

- adatvédelem (személyes és üzleti adatok)
- alkalmazás szintű védelem (naplózás)
- hozzáférési és jogosultsági rendszerek
- mentési és archiválási rendszerek
- külső és belső hálózat közötti kapcsolat szabályozott működése
- az IT eszközök szoftveres védelme (pl. vírus ellenőrzés)
- vészforgatókönyvek katasztrófahelyzetekben

A fizikai és logikai kockázatok mellett ma már külön veszélyforrás lehet az ember is (ld. 9. fejezet). A humán biztonság kérdései az elmúlt időszakban felértékelődtek (pl. elbocsátott munkatársak megtorlásai, képzetlenségből adódó működési zavarok), de a KKV-k nem helyeznek megfelelő súlyt erre a területre. Az Európai Unió egy szakmai szervezetének (ENISA) „Hogyan növelhető az információbiztonsági tudatosság" című kiadványa kommunikációs segítséget ad a vállalatok számára. A dokumentum külön kitér a KKV-kat érintő akadályokra és az ilyen kiadványoknál megszokott kritikus sikertényezőket is megfogalmaz. Fontos megértetni az alkalmazottakkal, hogy az információbiztonság nemcsak a vállalati informatikusok felelőssége… A biztonságtudatosság kialakítása talán a legkevesebb pénzügyi erőforrást igényli, de nem egyszeri feladat, hanem folyamatos oktatást és „karbantartást" kíván.

Mit tehet egy KKV ha információbiztonságot szeretne és alig áll rendelkezésre ehhez szükséges erőforrás? Andy Horn javaslatainak átdolgozásával, kiegészítésével próbáljuk megadni a választ (Andy Horn, 2009)

1. Legyen a vállalatnál elfogadott információbiztonsági politika! Határozzuk meg, hogy milyen üzleti információk fontosak számunkra és kiknek, milyen módon kell ezeket elérni!
2. Vizsgáljuk át kockázati szempontból üzleti folyamatainkat! Jelöljünk ki szervezeti egységenként információbiztonsági felelősöket!
3. „Központosítsuk" a szoftverbeszerzést! Az alkalmazásokat használatba vétel előtt teszteljük és ellenőrizzük (ez különösen igaz az ingyenesen letölthető megoldásokra…)!
4. Legyen naprakész leltár az IT eszközökről és az adatbázisokról!

5. Tájékoztassuk – akár formális oktatás révén is - az alkalmazottakat az őket érintő információbiztonsági feladatokról és felelősségükről! Törekedjünk a „tiszta asztal, tiszta képernyő” szabály betartatására!
6. Alkossunk és vezessünk be információkezelési szabályokat, különösen a bizalmas személyes és üzleti adatok esetében!
7. Fordítsunk figyelmet a fizikai biztonságra, az IT eszközök tárolására és illetéktelen személyek hozzáférésének megakadályozására!
8. Biztosítsuk az üzletmenet folytonosságát krízis- vagy katasztrófa helyzetben is! Tároljuk a fontos üzleti adatokat és alkalmazásokat redundánsan, akár külső szolgáltató igénybevételével is!
9. Ismerjük meg és használjuk ki az alap- és alkalmazói szoftverek információvédelmi lehetőségeit (pl. naplózás, titkosítás)!
10. Védjük az IT-t és kommunikációs rendszereinket rosszindulatú szoftverek és illetéktelen behatolás ellen (pl. antivirus-, spamszűrő- és kémprogram elleni alkalmazások)!

9 Információbiztonság az ellátási láncokban

A vállalatok közötti üzleti tranzakció-, ill. információkezelés létfontosságú a hosszú távú együttműködés, a stratégiai partnerkapcsolat szempontjából. A résztvevők kommunikációs viselkedésének meghatározó jellemzői a minőség, az információ-megosztás és a részvétel. Az ellátási láncban közreműködő, önállóan gazdálkodó szervezetek hálózatot alkotnak, amelynek jellemzői az együttélés, az együttműködés, a kooperáció, a hosszú távú elkötelezettség, a közös értékrend, a kölcsönös egymásra hatás és a közreműködő gazdálkodó szervezetek folyamatos interakciója. A cégek információs rendszerei ezért átlépik a vállalati határokat, biztosítva az ellátási láncban stratégiai szövetséget kötő vállalatok együttműködését. A sajátos vállalati kultúrák, az ellátási láncban betöltött eltérő szerepek, a változó üzleti érdekek és a különböző információtechnológiák nehézzé tehetik a hatékony integrációt, ugyanakkor az információbiztonság alapvető fontosságú az ellátási lánc elemei között létrejövő kapcsolat létrehozásában és működésében.

Az ellátási lánc értékteremtő folyamatok és erőforrások összehangolt rendszerét jelenti, amely több vállalatot érintve az alapanyagok beszerzésével kezdődik és a végtermék fogyasztóhoz történő eljuttatásával fejeződik be. Részét képezik a beszállítók, a gyártók, logisztikai szolgáltatók, raktárak és a disztribúciós folyamatok egyéb szereplői is. Működését elsősorban a végső fogyasztók igényei határozzák meg, közös érdekeltséget teremtve a lánc résztvevői számára.

Az amerikai Supply Chain Council (**SCOR modell**) által megfogalmazott definíció alapján az ellátási lánc minden olyan tevékenységet magában foglal, amely a termék előállításával és kiszállításával kapcsolatos, a beszállító beszállítójától kezdve a végső fogyasztóig bezárólag.

Az 5 fő folyamat, amely meghatározza az ellátási láncot

1. tervezés (a kereslet-kínálat elemzése és a termékek, ill. szolgáltatások előállításának minőségi, mennyiségi és időrendi meghatározása)
2. beszerzés (alapanyag, alkatrész és kooperációs szolgáltatások)
3. gyártás (alkatrészgyártás és szerelés)
4. kiszállítás (készletezés, rendelés-feldolgozás, elosztás, valamint a végső fogyasztó kiszolgálása)
5. visszaszállítás (hibás, felesleges és karbantartandó termékek kezelése, ill. vevőszolgálati tevékenység)

A vevői igények kielégítésére hatással lehet, ha az ellátási láncot alkotók kellő hatékonyságú információkezelő rendszert alkalmaznak. Ennek eredményeként nem az egyedi szervezetek diszkrét eredményei összegződnek, hanem az erőforrás-allokációból adódóan a gazdálkodás különböző területein szinergikus hatások alakulnak ki. Az ellátási lánc menedzsmentje a vállalatok tudatos együttműködését jelenti. Elfogadják, hogy annak léte versenypozíciójuk javulását eredményezi. A lánc tagjai hajlandók lemondani saját, rövidtávú előnyeik érvényesítéséről a teljes lánc optimális működésének érdekében. A vállalatok belső logisztikai és információs rendszerei nélkülözhetetlenek a vállalatok közötti folyamatok koordinálásához (Mentzer et.al, 2001).

A vevői igények- és azok kielégítésében játszott szerepek ismerete, valamint a nem teljesítésből az ellátási lánc működésére vonatkoztathatóan származó hátrányok tudatosítása ugyanakkor hozzájárul az ellátási láncot alkotó gazdálkodó szervezetek elkötelezettségének kialakulásához. A folyamatosan változó gazdasági környezetben ma a gazdálkodó szervezetek számára rendkívüli jelentőséggel bír az, hogy egy értékalkotó hálózat részeként lehetőségük nyílik környezetük irányítási struktúráinak befolyásolására (Chikán-Gelei, 2005.).

Az ellátási láncok kialakítása és működtetése két lehetséges úton valósulhat meg. Az első esetben egy domináns vállalat képes irányítani az egész lánc tevékenységét. Itt a beszállítók kénytelenek elfogadni az erő pozíciójából diktált feltételeket. Igaz ez az információs rendszerek esetében is. A beszállítók előzetes minősítéséhez hozzátartozik a megfelelő IT infrastruktúra meglétének és alkalmazhatóságának ellenőrzése. A másik esetben egy tényleges stratégiai szövetség jön létre az „egyenlő” partnerek között. A résztvevők viszonylag hosszabb távon kívánnak együttműködni a kölcsönös előnyök érvényesítése érdekében, de nehezebben tudják az ellátási lánc működését optimalizálni a mégis megjelenő egyéni érdekek alapján.

9.1 Az információ megosztása az ellátási láncokban

Az ellátási láncok minimális szinten történő működéséhez néhány alapvető vállalati adatot mindenképpen szükséges a többi résztvevő számára biztosítani (készletszintek, értékesítési adatok és előrejelzések, vevői rendelések állapota, termelési és szállítási ütemezések, kapacitásadatok). Itt a vállalat által előírt belső információbiztonsági követelményekről világos, dokumentált tájékoztatást kell adni az ellátási lánc többi tagjának.

Az integráció egy magasabb szintjén már közös, integrált információs rendszereket is használnak. Az ellátási lánc tagjai „szabadon" hozzáférhetnek a termékek, vevők, beszállítók és piaci helyzetre vonatkozó információkhoz is. Sok esetben megismerhetik a társak belső vállalati folyamatait és korábban titkosnak tartott adatait (Lörincz, 2008). Empirikus felmérések alapján megállapítható, hogy az ellátási láncban szereplő vállalatok számának növekedésével és információtechnológiai integráció fokozódásával, valamint az információ megosztásával emelkedik az informatikai incidensek száma (Smith et.al. 2007). Ilyenkor közös információbiztonság irányítási rendszerek kialakítása sem elképzelhetetlen. Az ellátási láncok ma már nem működnek információtechnológia nélkül. A résztvevő vállalatok számára fontos, hogy a bemenő erőforrások milyen csatornákon (beszállítókon) keresztül milyen feltételekkel és költségekkel érkeznek, ill. mi történik a kimenő „termékekkel", milyen közvetítőkön keresztül jut el a végső fogyasztóig. Az az ellátási lánc lesz sikeres, amely gyorsabb, megbízhatóbb, karcsúbb és kisebb költségű, mint a versenytársai.

9.2 Az ellátási láncok kockázata

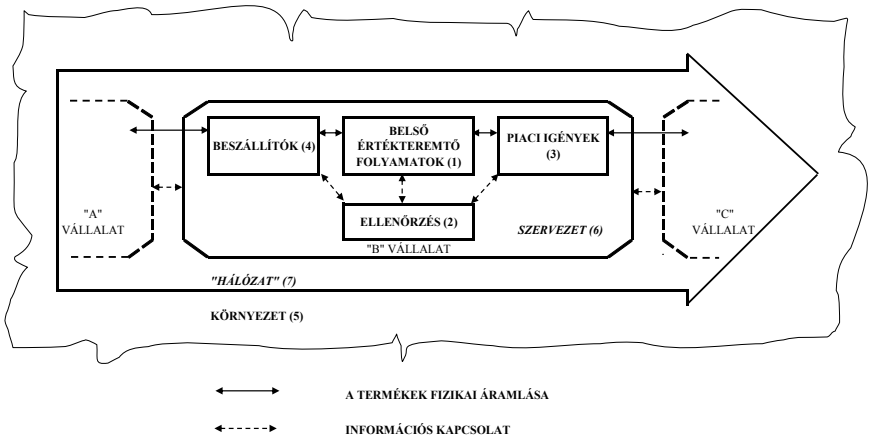
Az ellátási láncok kockázatát tekintve a szakirodalom egységes álláspontot képvisel. Az ellátási lánc kockázata olyan potenciális események, zavarok bekövetkezése az ellátási láncon belül és annak környezetében (akár piacán is…), amelynél veszélybe kerül a vevői igény kielégítése, vagy a vevő biztonsága is. A hagyományos kockázati megfontolás (a bekövetkező kockázati tényezőből származó kár nagysága és a kockázati esemény valószínűsége) helyett, ill. mellett bevezették a „sebezhetőség" fogalmát.

A kockázatokat, ill. az ellátási láncok sebezhetőségét eredetük alapján 5 csoportba lehet sorolni (Christopher Peck, 2004)

1. értékteremtő folyamatok zavarai (gyártás, beszerzés, raktározás, szállítás, ütemezés)
2. ellenőrzés (annak hiánya, ill. hibája)
3. piaci igények (információhiány, kiszámíthatatlanság, váratlan események)

4. beszállítók (megbízhatatlanság, kapacitáshiány, vis maior)
5. környezet (gazdasági-, politikai események, balesetek, természeti katasztrófák)

Ezt további két kockázat „forrás" egészíti ki. A belső vállalati szervezet (6) szintén sebezhető, ha az nem felel meg a kialakított értékteremtő folyamatoknak és nem jól használja az információs rendszereket. Az ellátási lánc tagjai között is előfordulhatnak együttműködési zavarok mind az információ-, mind az anyagáramlásban. A több önálló vállalatból álló hálózat (7) is kockázati tényezőt jelent (9. ábra – Smith et.al. 2007).



9. ábra
Az ellátási láncok kockázat-forrásai

Az ellátási láncok integrált információs rendszereinek kockázatkezelését információtechnológiai oldalról is megközelíthetjük. A fizikai védelem a megfelelő környezet és információtechnológiai infrastruktúra kialakítását jelenti a környezeti ártalmak és a szándékos, vagy véletlen károkozás ellen.

A logikai vagy „üzemeltetési" védelem kiterjed az összekötött hálózatokra, az alkalmazott alapszoftverekre (operációs rendszerek és adatbázis-kezelők), az alkalmazásokra (pl. ERP és EAM rendszerek) valamint a tárolt adatokra. Meghatározzák a munkavégzés módját (pl. naplózási szabályok, vírusfertőzés elleni tevékenység), megadják a felhasználók jogosultságát és illetékességét.

A szabályozási munka eredménye általában Üzletmenet Folytonossági Terv (Business Continuity Plan) és Katasztrófa-elhárítási Terv (Disaster Recovery Plan) lesz. Az előbbi az üzleti folyamatokat támogató informatikai erőforrások meghatározott időben és funkcionális szinten történő rendelkezésre állásának biztosítása, valamint váratlan esemény által okozott károk minimalizálásáról szól.

Az utóbbi helyettesítő megoldásokat ad meg súlyos károkat és az informatikai szolgáltatás meghiúsulását okozó események bekövetkezésére. A cél, hogy a negatív hatások minimalizálhatók legyenek és az eredeti állapot visszaállítása elfogadható költségek mellett, gyorsan megtörténhessen.

9.3 Logisztikai információs rendszerek

Az üzleti életben használt vállalati információs rendszerek csoportosítása a szakirodalomban már kikristályosodott (Laudon-Laudon, 2006). Ez a csoportosítás kisebb kiegészítéssel az ellátási láncok területén is alkalmazható.

A tranzakció kezelő rendszerek a vállalati és vállalat-közötti értékteremtő folyamatok során keletkező adatok rögzítésére, feldolgozására és tárolására szolgálnak (rendelés felvétel, raktárgazdálkodás, külső és belső szállítás, készletkövetés, termelésirányítás, beszerzés). A vezetői munkát a döntéstámogató és vezetői információs rendszerek támogatják, amelyek többek között a tranzakció kezelő rendszerekben tárolt adatokból nyújtanak operatív döntésekhez összesített információkat. Az anyagszükséglet- és gyártási erőforrás-tervező rendszereken túl megjelennek a különböző szállítási útvonal és rakomány optimalizációval foglalkozó alkalmazások és a strukturális döntésekhez segítséget nyújtó szimulációs megoldások is. Az ellátási láncokban fontosabb a teljes hálózat hatékony működése, mint a tagvállalatok egyéni erőforrás felhasználási optimuma. Ez esetenként közös információs rendszerek üzemeltetését is jelentheti… Erre készteti a vállalatokat a Voluntary Interindustry Commerce Standards Association által kifejlesztett ellátási láncok tagjai közötti együttműködést támogató „**Collaborative Planning, Forecasting and Replenishment" (CPFR) folyamatmodell** is. A szükséglettervezés alapja a végső fogyasztói igény. A modellt alkalmazása egy konszenzuson alapuló előrejelzést eredményez, amely azután meghatározza a disztribúció, a termelés és a beszerzés tagokra is lebontott terveit. Az ellátási lánc tagjai törekednek arra, hogy az előrejelzés alapját szolgáló adatok minél pontosabbak legyenek. A közös kockázatkezelés és a komplex „ellátás" biztonságot adó védelmi tevékenység szükségszerűség. Ennek szabályozásában nyújthat segítséget az **ISO 28000**-es szabványcsomag, amely az ellátási láncok biztonság-irányítási rendszerére vonatkozó követelményeket tartalmazza.

A taktikai és stratégiai döntésekhez szükséges múltbéli adatok sokszor olyan adatpiacokból vagy adattárházakból származnak, amelyek tisztított és redundancia-mentes adatbázisok. Ezek alapjai lehetnek a különböző üzleti intelligencia alkalmazások felhasználásának is.

Az ellátási láncok szempontjából kiemelt fontosságú a kommunikáció kérdésköre. A kommunikációs rendszer alapját az automatikus azonosító rendszerek képezik (vonalkód, szabványos áruazonosítás, rádiófrekvenciás azonosítás), de ide tartozik a tagok közötti kapcsolattartást megvalósító kommunikációs technikák is

(elektronikus adatcsere, értéknövelő hálózatok, Internet, globális helymeghatározó rendszerek) Ezek többnyire szabványokhoz és ajánlásokhoz kötött megoldások. Ezen belül kiemelt szerepet kapnak az ún. értéknövelő hálózatok. A különböző kommunikációs szabványok közös alkalmazása teljesítményjavulást hozhat az ellátási láncban, de a tagok eltérő szerepe, funkciója miatt sokszor a szabványosítás indokolatlan kötöttségeket is okozhat. Az értéknövelő hálózatok különböző szabványú, egymással nem kompatibilis tranzakciós üzeneteket „fordítanak le, ill. át" és továbbítják azokat az ellátási lánc többi tagja felé. (Gyakorlatilag értéknövelő hálózatnak tekinthető a külső, harmadik fél által üzemeltetett EDI rendszer is…)

Az ellátási lánc tagjai számára fejlesztett „egyéni" vállalati információs rendszerekben, ill. a teljes hálózat számára készülő integrált alkalmazásokban ilyen éles határt húzni a részrendszerek között nem lehet. A tranzakció kezelés, a döntéstámogatás és a kommunikáció egymástól elválaszthatatlan.

9.4 Az információbiztonság irányítása az ellátási láncok szereplőinél

A stratégiai üzleti partnerek kiválasztásánál ma legalább olyan fontos a stabil, megbízható IT alapokon nyugvó kapcsolattartási lehetőség, mint a megvásárolt termék v. szolgáltatás ára és minősége, valamint a leellenőrizhető referenciák megléte. Az ISO/IEC 27001-es szabvány célkitűzéseit, valamint az auditáláshoz szükséges gyakorlati útmutatót végig elemezve számos területen kell a kockázatokat kezelni.

Egy információs rendszerek kölcsönös, de természetesen korlátozott használatát is megengedő üzleti kapcsolatban alapvető, a partnerekkel egyetértésben megfogalmazott elvárások lehetnek a következők:

- a titoktartási nyilatkozat elkészítése és mindkét fél által történő elfogadása
- a fizikai beléptetés szabályozása (egyszeri vagy rendszeres lehetőség…, engedélyezés és visszavonás rendje)
- a megfelelő jogosultsági rendszer kialakítása (jelszavak kiadása és érvénytelenítése, a hozzáférés körének tisztázása)
- az információ továbbítás és hordozás szabályainak megállapítása (pl. másolatok készítése, a megsemmisítés kérdése…)
- az alárendelt szerződő partner felelősségvállalása a saját alkalmazottaiért (pl. hozzáférésre feljogosított személyek névsorának átadása…)
- csak a szükséges és elégséges adatok/információk biztosítása a partnerek számára

- informatikai outsourcing szabályozása (a szervezet egyes információfeldolgozási feladatait egy másik szervezet látja el, és emiatt hozzáfér hálózati elemekhez, adatbázisokhoz és szoftver-alkalmazásokhoz…)
- az együttműködés során bekövetkezett káros események (incidensek) tapasztalatainak leszűrése, a hibaelhárítás ráfordításainak számszerűsítése és a felelősség egyértelmű megállapítása
- formális eljárások lefolytatása, ha valamelyik fél alkalmazottai megsértik a megállapodásokat
- információs rendszer közös kialakítása esetén a fejlesztés során és a napi működésben használt IT eszközök egyértelmű elkülönítése
- az üzleti kapcsolat fenntartásában nélkülözhetetlen szoftverek szabályozott, írott megállapodások alapján történő átadása (pl. banki rendszerekkel történő kapcsolattartás)
- az elektronikus kereskedelem (EDI is…) és levelezés biztonságának szabályozása különös tekintettel az üzleti tranzakciós adatok, ill. az üzenetek hitelességére, titkosságára és sértetlenségére
- az elfogadott feltételek és követelmények írásba foglalása a későbbi jogviták elkerülése miatt…

Az információbiztonsági irányítási rendszer kiépítésének célja a partnerek elvárásainak, a vonatkozó hazai és nemzetközi előírásoknak megfelelő működés és az információbiztonság megteremtése, az adatok és információk sértetlenségének, bizalmasságának megőrzése, ezek rendelkezésre állásának biztosítása. Minimalizálható legyen az esetlegesen bekövetkező üzleti kár és biztosítani tudjuk az üzletmenet-folytonosságot.

Az információbiztonsági irányítás rendszer bevezetése az ellátási láncokban is projektszerűen történhet, amelynek lépéseit (információvédelmi átvilágítás, kockázatértékelés és elemzés, dokumentálás, a rendszer kialakítása és elindítása) az 5. és 6. fejezet részletesen tárgyalja.

10 Az információbiztonság emberi tényezői (információbiztonsági tudatosság)

A szervezeti információbiztonságot fenyegető kockázatok jelentős része emberi tényező. Ezeket teljes mértékben kiküszöbölni nem lehet, de jó humán erőforrás politikával csökkenthetők. A munkavállalók kiválasztásának, alkalmazásának és kilépésének szabályozásába információbiztonsági szempontokat is be lehet, ill.

kell építeni. Figyelembe vehető a korábban megszerzett informatikai képzettség, a megbízhatóság, az életkor és a munkakörnyezet valamint a folyamatos képzések elfogadási képessége.

10.1 A képzettség

Egy szervezet információs vagyonát általában nem a szándékos károkozás fenyegeti leginkább, hanem az információbiztonsági tudatosság hiánya (ENISA), a meggondolatlanság, a képzetlenségből adódó bizonytalanság és a betarthatatlannak tűnő vagy nem kellően ismert ügyviteli szabályozás.

A szabályozandó területek elsősorban az Internet munkahelyi használatát érintik:

- böngészés és letöltés (illegális tartalmak megjelenése a szervezeten belül)
- közösségi oldalak látogatása (bizalmas vállalati adatok publikussá tétele),
- elektronikus levelezés (címzett egyértelmű azonosításának hiánya)
- azonnali üzenetküldés (instant messaging services), ill. csevegés használata magáncélú kapcsolattartásra

Az informatikai képzettségi szintek különböző információbiztonsági kockázatokat hordoznak magukban.

A képzetlen felhasználó nem képes még a legegyszerűbb információtechnológiához kapcsolható feladatokat sem ellátni.

Az alapszintű informatikai ismeretekkel bíró munkavállaló előképzettséget nem igénylő irodai alkalmazásokat képes használni, de újszerű vagy összetett feladatok esetén gyakran bizonytalan és bizalmatlan.

A formális képzéseken (pl. ECDL, ERP) részt vett, „középszintű" ismeretekkel bíró felhasználó készségszinten használja az ő munkaterületét lefedő vállalati alkalmazásokat. Sokszor képes kisebb rendszerhibák elhárítására. A magabiztosság azonban kockázati tényezőt jelent, hiszen túlértékelheti saját képességeit (pl. indokolatlan adatbázis módosítás).

A kiemelt tudású felhasználó (sok szervezetnél ún. kulcsfelhasználó) részterülteken szinte rendszergazdai ismeretekkel bír, sokszor ismeri az alkalmazások alatt futó adatbázis-kezelő és operációs rendszerek működésének néhány elemét. Saját területén felismeri az alkalmazáshibákat és képes azokat önállóan kijavítani. Ennél a csoportnál a figyelmetlenség és a gondatlanság jelenti (pl. bizalmas vállalati információk hibás e-mail címre történő továbbítása, nem elfogadható jelszókezelés).

10.2 Generációs kérdések

Az információbiztonság emberi tényezői között nemcsak a képzettség, hanem a generációs különbségek is szerepet játszhatnak. A szociológusok és a marketing szakemberek szerint a mai munkavállalók születésük alapján három jellegzetes csoportba sorolhatók (Lancastar-Stillmann, 2005)

- ún. „baby boom"-osok (1946 és 1965 között születettek)
- X generáció (1965-1980 között jöttek a világra)
- Y generáció (1980 után születtek)

Bár nehéz általánosan elfogadott szabályokat megfogalmazni, de mindegyik korosztályra más-más információbiztonsági kockázat jellemző, más-más szabálysértéseket követnek el.

A „baby-boom"-osok demográfiai robbanás részesei, általában szeretik munkájukat és lojálisak cégükhöz. Kevésbé tudnak alkalmazkodni az információtechnológia fejlődéséhez, ezért technikai és tudásbeli hiányosságaik lehetnek.

Az X generáció tagjai szeretik a függetlenséget, azonban gyakran fásultak és cinikusak. Rosszindulatból is okozhatnak kárt. A biztonsági előírásokat gyakran figyelmen kívül hagyják a hatékonyabb munkavégzésre hivatkozva.

Az Y generáció, általában jóindulatú és fogékony az információtechnológia iránt, de eredménytelenség esetén türelmetlenné válhatnak. A munkahelyen leginkább ők keresnek fel kockázatosnak tűnő honlapokat. Gyakran saját mobil eszközökre töltenek le - természetesen titkosítás nélkül - bizalmas vállalati adatokat.

A generációs különbségeket, a korcsoportok sajátosságait tehát figyelembe kell venni az információvédelem szabályozása estén is (Kelemen, 2008).

10.3 Munkakörnyezet

A mobil eszközök mindennapos használata, az otthoni internetes kapcsolatot kihasználó munkavégzés vagy az ergonómiailag nem megfelelően kialakított munkahely számos biztonsági kockázatot is felvet.

Az elveszített/eltulajdonított eszközökön túl értékét tekintve sokkal jelentősebb veszteség lehet a tárolt adatok elvesztése vagy illetéktelen kezekbe kerülése.

A rossz munkakörülmények, figyelemmegosztó környezeti hatások rossz irányba befolyásolhatják a biztonsági intézkedések betartását és a pontos munkavégzést.

A munkavégzés befejezése után is gondoskodni kell a különböző alapú információhordozók megfelelő tárolásáról és azok hozzáféréséről. Gyakran előforduló probléma, hogy az egy helyiségben dolgozó kollégák egymás

jelszavával lépnek be a vállalati alkalmazásokba, férnek hozzá a vállalati adatbázisokhoz. A gyorsabb munkavégzés „érdekében" a közelebbi vagy éppen „szabadon lévő" hozzáférési pontot választják és nem „bajlódnak" a kilépés és a belépés jelszavakkal védett folyamatával.

Információbiztonsági kockázatot jelenthet a hagyományos telefonbeszélgetések lebonyolítása is. Nem megfelelő környezetben (zajterhelés, fokozott munkatempó) elmaradhat a hívó vagy hivott fél egyértelmű azonosítása.

10.4 Információtechnológiai és információbiztonsági képzések

Az informatikai beruházások leggyakrabban elmaradó része a felhasználók megfelelő „betanítása". Az oktatások gyakran nem veszik figyelembe a szervezeti egységek sajátosságait, a felhasználók eltérő alapképzettségét és a generációs sajátosságokat. A szakmailag kiválóan megfelelő rendszergazda nem biztos, hogy oktatás-módszertani kérdésekben is hasonlóan jól felkészült. Gyakran elmaradnak a napi rutin mellett megkopó információvédelmi tevékenységgel kapcsolatos „frissítő" képzések és szinte tabunak számit az elsajátított ismeretanyag számonkérése.

Az információtechnológiai változásokból adódó szabályozás-módosítások nem jutnak el azonnal az érintettekhez.

11 Egy folyamatszemléletű szervezeti biztonsági modell

A sikeres szervezeti működés alapja a tudatos kockázatvállalás és -kezelés. Az üzleti szervezeteknek olyan kockázatkezelési rendszerre (Enterprise Risk Management – ERM) van szükségük, amely

- azonosítja és kezeli a kockázati tényezőket
- az egész szervezetre és a befogadó környezetre is kiterjed
- révén a vezetők a teljes kockázati profilt átlátják
- segíti a stratégiai és operatív döntéshozatalt

Így megalapozható a vállalati (szervezeti) folyamatok védelme és elérhető a folyamatok biztonsága.

Folyamatbiztonság olyan állapotnak tekinthető, ahol az előírt bemenetek (folyamat végrehajtásához szükséges erőforrások) biztosítása után a folyamat tevékenységeit végrehajtó szervezeti egységek az előírt időben megfelelő mennyiségű és minőségű kimenetet (termék, szolgáltatás, információ) nyújtanak

és zavar esetén a folyamat normál működése a lehető legkisebb erőforrás ráfordítással és a legrövidebb idő alatt helyreállítható.

Az eddig tárgyalt szabványok és ajánlások többségükben folyamatközpontúak, de általában a gazdálkodó szervezetek egy-egy funkcionális területére vonatkoznak.

Minden szervezeti folyamat végrehajtásához erőforrásokra van szükség, amelyek közül kiemelkedik – az értékteremtő és kiszolgáló folyamatok egyik alapvető feltétele – a megfelelő időben és helyen, a jogosult személyek számára biztosított információ. Ezért lehet az alapja egy egész szervezetre vonatkozó biztonsági modellnek az információbiztonsági irányítási rendszer kialakítása. Az ügyvitel (workflow) szabályozásával – ill. működési zavar esetén annak helyreállításával – megteremthetjük a szervezet „virtuális működésének" biztonságát.

A vállalatok működésében kiemelt szerepet kaphat a virtuális vállalati modellt (vállalati információs rendszert – pl. ERP, EAM) alkalmazó felhasználó munkaköri feladatainak meghatározása. Milyen adatokat rögzíthet, módosíthat, törölhet, ill. kérhet le és milyen tranzakciókat kezdeményezhet… A felhasználók előre kialakított – biztonsági szempontokat is figyelembe vevő – pozíciókat töltenek be (Kern et. al, 2002.). Ennek kezelését (munkakör analízis, -tervezés, -irányítás és -karbantartás) hívja a szakirodalom ún. szerep életciklusnak (role life-cycle; ld. 12. fejezet).

Az információbiztonság – mint állapot – megteremtése után vagy mellett következhetnek a további „részterületek" (emberi erőforrás, környezet, termelés, belső logisztika, ellátási és értékesítési láncok, infrastruktúra, K+F) biztonsági szabályozása. Az ott értelmezett logikai, fizikai és szervezeti biztonság fogalma a többi területre is kiterjeszthető. A **logikai védelem** alatt az adatok integritásának biztosítását, a vírus- és számítógépes behatolás-védelmet és titkosítási eljárásokat értjük; a **fizikai védelem**hez többek között a beléptetést, szünetmentes energiaellátást, térfigyelést, tűz- és vízkár-elhárítást soroljuk; a **szervezeti, ill. adminisztratív védelem** a belső csalások, visszaélések, szándékos és vétlen károkozások megelőzését szolgálja. Ezek integrálása jelentősen csökkentheti a szervezetek biztonsági kockázatait.

További vállalati biztonsággal (is) foglalkozó – eddig nem tárgyalt – szabványok és ajánlások is figyelembe vehetők.

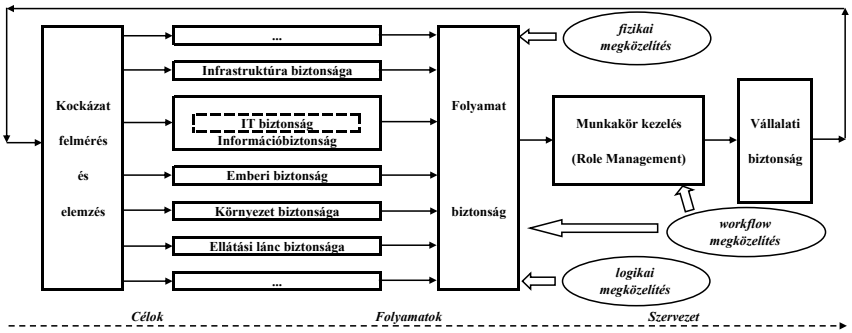
A brit **üzletmenet folytonosság**gal foglalkozó **BS 25999-1, -2** jelzetű szabványcsomag szintén egy vállalati működést szabályozó irányítási rendszer kialakítását teszi lehetővé. Minden szervezetre alkalmazható. A potenciális veszélyek és kockázati tényezők feltárása egy összetett hatáselemző munka eredménye (Business Impact Analysis, BIA). Megvizsgálják a vállalat kulcstermékeit, ill. annak előállítási lépéseit, a szolgáltatásokat támogató folyamatokat, az üzleti tevékenység megszakadásának maximálisan elfogadható időtartamát és a külső üzleti partnerektől való függőséget.

Az üzleti hatáselemzés alapján a vállalat olyan „kiterjesztett” üzletmenet folytonossági tervet alakít ki (Business Continuity Plan), amely segítségével a váratlan események sem okozhatnak gondot (katasztrófa helyzet, alapanyaghiány, közműzavarok, munkaerőhiány, technológiai berendezések meghibásodása, informatikai problémák, vevői reklamációk stb.). Megmarad a cég jó híre és képes folytatni az értékteremtő tevékenységeket, kiszolgálni az üzleti partnereket.

A vállalat minden kritikus anyagi és információs folyamata rendelkezik olyan helyettesítő megoldással, amely lehetővé teszi a rendkívüli helyzetben történő működést és az eredeti állapotba történő visszatérést.

A **COSO** (Comitte of Sponsoring Organisations of Treadway Comission) által összeállított **Enterprise Risk Management** nevű, 1992-től eredeztethető keretrendszer felsővezetőknek és döntéshozóknak szól. A vállalat belső üzleti folyamataira, azok szabályozására és ellenőrzésére fókuszál. Az üzleti stratégiát folyamatosan szem előtt tartva szinte minden kockázattípusra alkalmazható, de elsősorban pénzügyi területeken alkalmazzák.

A gazdálkodó szervezetek számára legfontosabb erőforrás a szakmailag felkészült, értékteremtő ember. A munkahelyi egészségvédelem és biztonság hatékony kezelését támogatja az **MSZ 28001**-es szabvány (BS OHSAS 18001) szerint felépíthető irányítási rendszer. Elsődleges célja azoknak a kockázati eseményeknek a meghatározása és kezelése, amelyek bekövetkezésük esetén károsan befolyásolhatja a munkavállalók teljesítményét, ill. balesetet, egészségkárosodást idézhetnek elő. Az irányítási rendszer kezeli a munkafolyamatok kockázatait, figyelembe veszi a releváns jogi környezetet és az adott szervezetnél jellemző biztonsági követelményeket, valamint az elérendő célokat. Szabályozza a munkaegészség fenntartásához kapcsolódó feladatokat. Segít a folyamatok megfigyelésében, értékelésében és az irányítási rendszer fenntartásához szükséges erőforrások és képességek meghatározásában. Előírja a bekövetkező kockázati események dokumentálását és utólagos értékelő vizsgálatát. Kiemelten kezeli a vészhelyzetekre történő reagálást és a helyesbítő és megelőző tevékenységeket. A rendszerszabvány nem ír elő konkrét követelményeket és ellenőrzési módszereket, azonban alkalmazása célorientált és folyamatszemléletű szervezeti működést biztosít. Alkalmazásával hozzájárulhatunk az emberi erőforrás jobb védelmét szolgáló munkakörnyezet kialakításához.



10. ábra
Vállalati biztonság elérése

A folyamatok biztonsága hozhatja meg a teljes vállalati biztonságot (10. ábra). A holisztikus biztonságszemlélet figyelembe veszi és kiemelten kezeli a szervezet stratégiai céljait, az értékteremtő folyamatokat és eszközöket, valamint az ezeket kiszolgáló információ technológiát. A szervezet vezetésének ezért közreműködnie kell a biztonsági célok kijelölésében, elérésében, valamint megvalósításuk ellenőrzésében és mérésében (Carelli et.al, 2004, pp. 14-22.).

12 Jogosultságtól a szerepkör- és személyazonosság kezelésig

A vállalati tranzakció kezelő és vezetői információs rendszerek (pl. ERP, CRM, EAM) támogatják, modellezik és sok esetben optimalizálják a vállalati értékteremtő és kiszolgáló folyamatok végrehajtását. A munkatársak (a felhasználók) az információtechnológiai erőforrásokhoz hozzáférve munkakörükből adódó „elemi" feladatokat látnak el. Adatokat rögzítenek, módosítanak, lekérdeznek, esetleg törölnek azért, hogy az információ – mint erőforrás – biztosítva legyen a különböző szintű vállalati döntéshozóknak.

Sok felhasználó és több, inhomogén információtechnológiai alapokon nyugvó információs rendszer esetén a felhasználók azonosítása és rendszer-eléréseik nyomon követése teljesen kaotikussá válhat. Rések és/vagy átfedések keletkezhetnek a hozzáféréseknél. A jogosultságot nem mindig a tényleges feladat- vagy munkakör alapján határozzák meg. Inkább informális szokásokat és vállalati hagyományokat vesznek figyelembe. Többszörös felhasználó-kezelés alakulhat ki az egymástól független vállalati információs rendszerekben. Változások alkalmával (áthelyezés, kilépés, új folyamatok, kiszervezés stb.) ad-

hoc módon végzik a jogosultsági kérdések - sok esetben utólagos - adminisztrációját.

A megoldás a vállalati folyamatok és szervezet elemzésén alapuló szerepkörök kialakítása lehet, ami azután összekapcsolódhat a szerepekbe bekerülő felhasználók személyazonosságának kezelésével.

12.1 A jogosultság

A felhasználó a vállalati folyamatok végrehajtásából adódó feladatainak elvégzéséhez vállalati információtechnológiai eszközöket is alkalmaz. Természetesen nincs szüksége minden IT erőforrásra és minden tárolt adatra. A jogosultság korlátozza a felhasználó közreműködését, optimális esetben csak a munkaköréből adódó tényleges információkezelési feladatok elvégzését teszi lehetővé, de azt viszont teljes körűen. Meghatározásának alapja az üzleti folyamat(ok), azok céljai , a szervezeti felépítés és az informatikai infrastruktúra. Szerepet játszanak benne az információbiztonsági kockázatok is (értékes vállalati információk elvesztése v. illetéktelen kezekbe kerülése). A tényleges jogosultsági rendszer kialakítására hatással van a szervezeti és egyéni tudás, a vállalati kultúra, valamint a munkakörhöz rendelt felelősség.

A jogosultság formálisan is nyilvántartható és nyilvántartandó (kiadható, beállítható, ellenőrizhető, jóváhagyható, elutasítható, szüneteltethető, elvehető). Fontos a munkahelyi vezető és az adott terület adatbiztonságáért felelős hozzájárulása. A felhasználó egyszerűbb esetben felhasználói nevet (login) és jelszót (password) kap. Ez magasabb biztonsági igények esetén kiegészíthető vagy helyettesíthető biometrikus „azonosítókkal" (pl. ujjlenyomat, írisz, fülcimpa) vagy kiegészítő hardver eszközökkel. Ezeket rendeljük −a vállalati folyamatoknak és üzleti céloknak megfelelően −az információs rendszerek, üzleti alkalmazások moduljaihoz, menüihez, menüpontjaihoz, képernyőihez és adatmezőihez valamint adatbázis lekérdezési lehetőségeihez. A jogosultság a felhasználókon túl köthető alkalmazási helyhez és időszakhoz is.

A jelszó, mint védelmi tényező önmagában nem képes az illetéktelen hozzáférések megakadályozására (Keszthelyi, 2011). Elvárás a felhasználóktól, hogy saját jelszavaikat titkosan és felelősségteljesen kezeljék. Másnak átadni, más által hozzáférhető helyen hagyni tilos!

A jó jelszó ismérvei:

- 8 karakternél hosszabb
- kis- és nagybetű mellett tartalmaz számokat és egyéb írásjeleket is
- a kívülálló számára nem értelmes
- a felhasználó számára megjegyezhető

- rendszeres időközönként (pl. havonta) változtatják

12.2 A szerepkörök

Nagyobb létszámú, több telephelyes „szabványosított" folyamatokat végrehajtó vállalatok esetén megfontolandó szerepkörök kialakítása. Ugyanabban a szerepkörben dolgozó felhasználók azonos jogosultságot kapnak. A szerepkör nem csak egy informatikai alkalmazáshoz kötődhet. Így a jogosultságok beállítása automatizálható és nagy számban egyszerre változtatható. A felesleges hozzáférések kiszűrhetők és az egyéni jogosultságok száma csökkenthető. A szerepkörök száma tehát kevesebb lesz, mint a felhasználók száma.

A szerepkörök köthetők folyamatokhoz (folyamat elemekhez) és szervezeti egységekhez. Az előbbi a vállalat üzleti tevékenységének funkcionális kiszolgálását teszi lehetővé, az utóbbi pedig a szervezeti működést és döntéshozatalt támogatja. A szerepkörök „állandóak", az információtechnológia fejlődése vagy új folyamatok változtathatják csak meg. A felhasználói fluktuáció így kevésbé van hatással a vállalati információs rendszerek működésére. A legtöbb IT kereskedelemben kapható, tranzakció-kezelésen alapuló megoldás már használja az ún. szerepkör-alapú hozzáférés ellenőrzést (Role Based Acces Control). A szerepkörök kialakításának kezdetén a tényleges vállalati folyamatokon és szervezeten alapuló üzleti szerepelvárás általában nem egyezik meg az informatikai megoldások által biztosított információkezelési lehetőségekkel. A szerepkör kialakítás egyik fontos célja tehát az információtechnológia és az üzleti követelmények összhangba hozása (Klarl, et. al, 2009).

A szerepkörök kialakításának gyakorlata többféle lehet:

a. Fentről lefele (top-down) történő megközelítés… Alapjában véve figyelmen kívül hagyjuk a már meglévő szerepköröket, ill. jogosultságokat. A szervezeti felépítésből és a folyamatok elemzéséből kiindulva a felhasználók feladatai alapján alakítjuk ki az új szerepköröket, ill. szerepkör csoportokat. A felhasználók közvetlen megkérdezésével írjuk le az ügyviteli folyamatokat. Minden lehetséges szerepkört, ill. ehhez tartozó jogosultságot meg kell határozni, akár több információs rendszert is figyelembe véve. A munka az egész szervezetet felöleli, tehát idő- és erőforrás-igényes lehet (role engineering). Nehezen automatizálható

b. Lentről felfele (bottom-up) történő megközelítés… Megvizsgáljuk a már meglévő összes jogosultságot és esetleg meglévő szerepkört (role-mining). Megállapítjuk a jogosultságok egymáshoz való viszonyát, átfedéseket és réseket. Megpróbálunk ez alapján minimálisan szükséges számú új szerepkört kialakítani. Azokat a szerepköröket, amelyekhez

kevés felhasználó tartozna, megpróbáljuk törölni és a vállalati folyamatok kiszolgálását úgy (workflow) átszervezni, hogy az a maradó szerepkörökkel kiszolgálható legyen. A vezetők ellenőrzik az új jogosultságokat és szerepköröket

c. „Hibrid" szerepkörfejlesztés esetén a két előbbi megközelítést közösen alkalmazzuk, egy gyorsabb és olcsóbb szerepkörfejlesztés érdekében

A szerepkörök „életciklusát" négy fázisra oszthatjuk, ami egy többszörösen összetett szabályozási kört (11. ábra) eredményez (Kern, et.al, 2002):

1. Analízis

Azonosítjuk a szerepeket - lehetőség szerint hibrid szerepkörfejlesztéssel - a vállalati információs rendszerekben a szervezeti pozíciók és munkaköri feladatok alapján. Ehhez vállalati folyamatokat és az informatikai alkalmazásokat egyaránt ismerő szakemberekre van szükség.

2. Tervezés

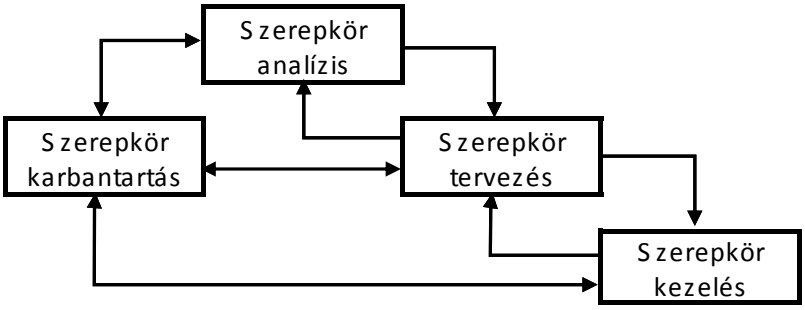
Meghatározzuk az információs rendszerekben egy-egy szerepkörhöz tartozó tényleges felhasználói feladatokat (role-mapping) és előírjuk az ehhez kapcsolódó adminisztrációs kötelezettségeket (workflow). Gyakorlatilag az analízis és a tervezés fázisa tekinthető a szerepkör kialakításnak.

3. Kezelés

Ebben a fázisban a működő szerepkörök adminisztrációját, ellenőrzését végezzük figyelembe véve a folyamatok és a szervezet kisebb változásait is. Itt történik a felhasználók és szerepkörök összekapcsolása (pl. új belépés) és szétválasztása (pl. elbocsátás). Vizsgálat tárgya lehet az is, hogy felhasználó kihasználja-e a szerepköréből adódó jogosultságokat.

4. Karbantartás

A vállalati folyamatok és szervezet nagyobb méretű változásokat is elszenvedhetnek (összeolvadás, üzletág eladása, új telephely kialakítása, BPR). Ez természetesen a szerepköröket sem hagyja érintetlenül. Ebben a fázisban elképzelhető szerepkörök egyesítése és szétválasztása.



11. ábra
Szerepkör életciklus (Kern, et. al, 2002)

12.3 Személyazonosság kezelés

A személyazonosság kezelés révén azonosíthatjuk a munkatársakat és üzleti partnereket egy vagy több vállalati információs rendszerben. Így szabályozhatjuk hozzáférésüket a különböző információtechnológiai erőforrásokhoz. Összeköti a felhasználói jogosultságokat és tiltásokat a rendszerekben meglévő információkezelési feladatokkal (2. táblázat). Ez akkor válik különösen fontossá, amikor a vállalatnak több, egymással kapcsolatban álló, eltérő információtechnológiai infrastruktúrán alapuló információs és kommunikációs rendszere is van. Nem feladata a felhasználói hozzáférés hitelesítése (authentication) és új jogosultság (authorisation) létrehozása. Végigköveti a felhasználói életciklust egyénenként (pl. belépést, munkakör bővülést, átszervezésből adódó pozíció változást, hosszabb fizetés nélküli szabadságot vagy a kilépést).

A személyazonosság formális kezelése (esetleg ilyen célra készült informatikai megoldás vállalati használata) több területen hozhat eredményeket:

a. Költségcsökkenés

Kevesebb teher jut az információs rendszereket üzemeltető (help-desk) szakemberekre. Az azonosításból adódó problémák (pl. elveszett jelszó pótlása) kezelési ideje csökken. Az ügyviteli folyamatok szabályozása átláthatóbbá válik és egyszerűbben vezethetők be új alkalmazások. Tanulmányok foglalkoznak ilyen ún. IDM rendszerek (Royer, 2008), ill. információbiztonsági folyamat-fejlesztések (Purser, 2004) megtérülésével. A vállalati folyamatok üzleti célok szerinti szabályozása (ebbe bele tartozik az információbiztonságon belül a személyazonosság kezelés is) nemcsak

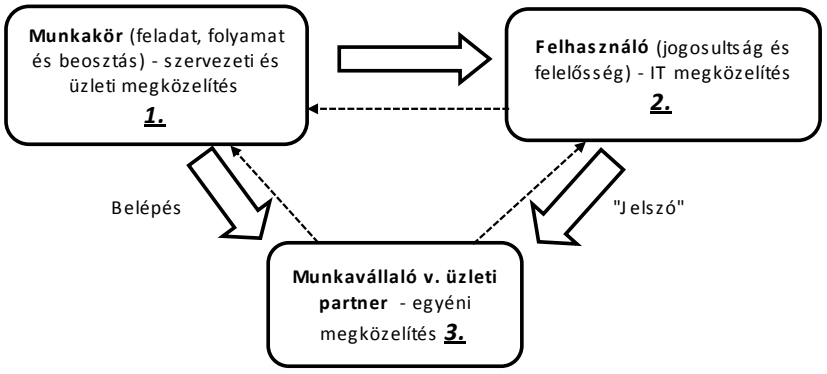
kockázatcsökkenést eredményez, hanem – esetenként számszerűsíthető – költségmegtakarítást is.

b. Rugalmasság

A változó folyamatok és új üzleti informatikai megoldások gyorsabban bevezethetők. Új munkatárs belépését követően a szükséges jogosultság szinte azonnal kiadható. A felhasználók jelezhetik igényüket eddig nem használt erőforrásokra. Az üzleti célok és döntések határozzák meg az információtechnológia használatát és nem fordítva (12. ábra).

c. Biztonság és megfelelőség

A jogosultságok gyorsan visszavonhatók a kilépett dolgozónál. A jelszavakat egy helyen kezelik. A felhasználók csak ahhoz kapnak hozzáférést, ami a munkájuk elvégzéséhez feltétlenül szükséges. Az egymást átfedő jogosultságok könnyebben kimutathatók. Lekérdezhető nyilvántartás készül arról, hogy melyik felhasználó mikor, milyen hozzáférést kapott és azt ki engedélyezte.



12. ábra
Tevékenységalapú személyazonosság kezelés

Feladatok	Felhasználók (alkalmazott , üzleti partner)	Vezetők	Üzemeltetők (IT - rendszergazda, biztonsági vezető)
Belépés és jogosultság igénylés	**K**	**V**	**I**
Jogosultság kiosztás és jóváhagyás	**I**	**K**	**V**
Felhasználói regisztráció	**K,I**	**I**	**V**
Szerepkör illesztés (új folyamat, BPR, szervezet változás)	**I**	**K,V**	**V**
Szerepkör változás (előléptetés, áthelyezés)	**K**	**V**	**I,V**
Jogosultsági problémák (pl. elfelejtett jelszó)	**K**	**I**	**V**
Hozzáférés ellenőrzés, felügyelet (időszakos és eseti jelentések, naplóelemzés)	**I**	**K, I**	**V**
Jogosultság megszüntetés (pl. kilépés)	**I**	**K**	**V**
Jelmagyarázat	**K**; kezdeményezés	**V**; végrehajtás	**I**; informálódás

2. táblázat
Személyazonosság kezelés feladatai

Irodalom

[1] van Bon, Jan – Verheijen, Tieneke – IT Service Management Forum: Frameworks for IT Management, Van Haren Publishing, 2006

[2] Carelli, Richard A. – Allen, Julia H. – Stevens, James F. – Willke, Bradford J. – Wilson, William R.: Managing for Enterprise Security, Networked Systems Survivability Program, Carnegie Mellon University, 2004, p.55 (CMU/SEI-2004-TN-046)

[3] Chikán Attila – Czakó Erzébet – Zoltayné Paprika Zita: Vállalati versenyképesség a globalizálódó magyar gazdaságban, Akadémiai Kiadó, Budapest, 2002

[4] Chikán Attila – Gelei Andrea: Az ellátási láncok és menedzsmentjük, Harvard Business Manager (Magyar Kiadás), 2005. január, pp. 35-44

[5] Christopher, Martin – Peck, Helen: Building the resilient supply chain, International Journal of Logistics Management, Vol. 15, No. 2, 2004, pp. 1-13

[6] van der Aalst, Wil – van Hee, Kees: Workflow Management – Models, Methods, and Systems, MIT Press, Cambridge MA, 2004, p. 384, ISBN 978-0-262-72046-5

[7] Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve, Complex Kiadó. 2008

[8] Gelei Andrea – Kétszeri Dávid: Logisztikai információs rendszerek felépítése és fejlődési tendenciái, Műhelytanulmány, Corvinus Egyetem, Budapest, Vállalatgazdaságtan Intézet, 2007. június

[9] Godányi Géza: Katasztrófavédelem és üzletmenet-folytonosság az információtechnológiában (A DR/BC tervezés alapjai), Híradástechnika, LIX évf. 2004/4. pp. 47-52

[10] Hangbae Chang – Jungduk Kim – Sungjun Lim: Information Security Management System for SMB in Ubiquitous Computing, Lecture Notes in Computer Science, Volume 3983/2006, May 2006, p. 707-715

[11] Horn, Andy: Information Security – More Than An IT Challenge for SME, www.freshbusinessthinking.com/business_advice.php?CID=3&AID=2629 &PGID3 (letöltés dátuma: 2009.11.25.)

[12] Klarl, Heiko – Molitorisz, Korbinian – Emig, Christian – Klinger, Karsten – Abeck, Sebastian: Extending Role-based Access Controll for Business Usage, SECURWARE'09, The Third International Conference on Emerging Security Information Systems and Technologies, Athens/Glyfada, Creece, June 18-23., 2009, pp. 136-141, ISBN 978-0-7695-3668-2

[13] Káté István: Kis és közepes vállalkozások információbiztonsági rendszerének kialakítása és integrálásuk lehetőségei, Diplomamunka, Óbudai Egyetem, Keleti Károly Gazdasági Kar, Vállalkozásfejlesztés mesterszak, 2010

[14] Kelemen László: Nem sztereotípiák, IT-business, 2008. szeptember 28, VI évf. 37. sz. 32. oldal

[15] Keszthelyi András: Password Strength and Memorability, FIKUSZ 2011, Symposium for Young Researchers, Óbuda University, Budapest, Hungary, November 11., 2011, pp. 23-29., ISBN 978-615-5018-25-1

[16] Kern, Axel – Kuhlmann, Martin – Schaad, Andreas – Moffett, Jonathan: Observations on the Role Life-Cycle in the Context of Enterprise Security Management, SACMAT'02 Proceedings of the 7th ACM Symposium on Acces Control Models and Technologies, Monterey, CA, USA, June 3-4., 2002, pp. 43-51., ISBN 1-58113-496-7

[17] Ködmön István (szerk.): Hétpecsétes történetek (Információbiztonság az ISO 27001 tükrében), Hétpecsét Információbiztonsági Egyesület, Budapest, 2008

[18] Lancaster, Lynne C. – Stillman, David: When generations collide, New York, First Collins Business Edition, 2005

[19] Laudon, Kenneth C. – Laudon, Jane P.: Management Information Systems: Managing the Digital Firm, Prentice Hall, 9-th edition, 2006

[20] Lábodi Csaba – Nahlik Gábor: Gazdálkodó szervezetek versenyképességének fokozása integrált irányítási rendszerek alkalmazásával, 6. Menedzsement, vállalkozás és benchmarking konferencia – Budapest, BMF, KGK, 2008. május 31., pp. 263-273

[21] Lőrincz Péter: Az ellátási láncok sajátosságai menedzsment és informatikai szempontból, MEB 2008, 6th International Conference on Management Enterprise and Benchmarking, May 30-31. 2008, Budapest, pp. 239-249

[22] Mentzer, John T. – DeWitt, William – Keebler, James S. – Min, Soonhong – Nix, Nancy W. – Carlo D. Smith – Zacharia, Zach G.: Defining Supply Chain Management, Journal of Business Logistics, Vol. 22, No. 2, January 2001, pp. 1-25

[23] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve, Verlag-Dashöfer, Budapest, 2000-

[24] Muha Lajos – Bodlaki Ákos: Az informatikai biztonság, Pro-Sec Kft., Budapest, 2003

[25] Ji-Yeu Park – Robles, Rosslin John - Chang-Hwa Hong – Sang-Soo Yeo – Tai-hoon Kim: IT Security Strategies for SME's, International Journal of Software Engineering and its Applications, Vol. 2. No. 3., July. 2008, pp. 91-98

[26] Purser, Steve A. : Improving the ROI of the security management process, Computers & Security, vol. 6, no. 23. 2004., pp. 542-546, ISSN 0167-4048

[27] Racz, Nicolas – Weippl, Edgar - Seufert, Andreas: A frame of reference for research of integrated Governance, Risk & Compliance (GRC), In: Bart De Decker, Ingrid Schaumüller-Bichl (Eds.), Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings, Berlin: Springer, pp. 106-117

[28] Royer, Denis: Enterprise Identity Management – What's in for Organisations, The Future of Identity int he Information Society (IFIP International Federation For Information Processing, Volume 262, 2008, Springer, pp. 433-446, ISBN 978-0-387-79025-1

[29] Smith, Gregory E. – Watson, Kevin J. – Baker, Wade H. – Pokorski, Jay: A critical balance: collaboration and security in the IT-enabled supply chain, International Journal of Production Research, Vol. 45, No. 11, pp. 2595-2613

[30] László Szerb – József Ulbert: The Examination of the Competitiveness in the Hungarian SME Sector: A Firm Level Analysis, Acta Polytechnica Hungarica, Vol.6, No.3, 2009. pp.105-123

[31] Tawileh, Anas – Hilton, Jeremy – McIntosh, Stephen: Managing Information Security in small and Medium Sized Enterprises: A Holistic Approach. Highlights of the Information Security Solutions Europe, SECURE 2007 Conference, Warsaw, 24-27.09.2007 (ISSE/SECURE 2007 Securing Electronic Business Processes, p. 331-339)

[32] Tóth Tibor (szerk.): Minőségmenedzsment és informatika, Műszaki Könyvkiadó – Magyar Minőség Társaság, Budapest, 1999

[33] Vadász István – Lábodi Csaba – Ulrich Anikó: Az első magyarországi integrált minőség- és információvédelmi irányítási rendszer kiépítése és tanúsíttatása, ISO 9000 Fórum, Dunaújváros, 2003., Konferencia-kiadvány

[34] Vasvári György: Vállalati biztonságirányítás (Informatikai biztonságmenedzsment), Time-Clock Kft., 2007

[35] Vágó Balázs: Kis- és középvállalkozások információbiztonsági tudatosságának költséghatékony növelése, Diplomamunka, Óbudai Egyetem, Keleti Károly Gazdasági Kar, Vállalkozásfejlesztés mesterszak, 2011

[36] Hogyan növelhető az információbiztonsági tudatosság (Felhasználói útmutató), ENISA (European Network and Information Security Agency), 2006. június., www.enisa.europa.eu/act/ar/deliverables/2006/ar-guide/hu (letöltés dátuma: 2009.11.25)

[37] Collaborative Planning, Forecasting and Replenishment (CPFR), Overview, 2004, Voluntary Interindustry Commerce standards (VICS), www.vics.org

[38] Control Objectives for Information and Related Technology (CObIT – Information systems Audit and Control Association, 4th edition, USA, 2005)

[39] www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf (letöltés dátuma: 2011.05.05)

[40] Enterprise Risk Management - Integrated Framework Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission, September, 2004 (www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf letöltés dátuma: 2011.10.06)

[41] Symantec 2011 SMB Disaster Preparedness Survey, Global Results, January 2011, www.symantec.com (letöltés dátuma: 2011.05.03)

[42] Outpacing change, Ernst & Young's 12th annual global information security survey (2009)

www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf (letöltés dátuma: 2009.12.01)

[43] Supply Chain Council, Supply-Chain Operations Reference (SCOR) Model, Overview, Version 9.0, 2008 (www.supply-chain.org)

[44] www.commoncriteriaportal.org (letöltés folyamatos)

[45] www.hetpecset.hu (letöltés folyamatos)

[46] www.itsmfi.org (letöltés folyamatos)

[47] An Introductory Overview of ITIL V3. IT Service Management Forum, 2007 (www.itsmfi.org – letöltés dátuma: 2011. október 6)

[48] www.iso27001security.com (letöltés folyamatos)

[49] ISO27k Toolkit, Version 3.8, 2009, Prepared by the international community of ISO27k implementers, at www.ISO27001security.com www.ISO27001security.com/ISO27k_Toolkit_overview_and_contents_3v8.rtf (letöltés dátuma: 2009.01.04)

[50] www.iso27001certificates.com (letöltés folyamatos)

[51] www.itgi.org/cobit (letöltés folyamatos)

[52] BS 25999-1:2006 Business Continuity Management, Code of Practice (Üzletmenet-folytonosság menedzsment, Gyakorlati útmutató)

[53] BS 25999-2:2007 Business Continuity Management, Specification (Üzletmentet-folytonosság menedzsment, Specifikáció) ISO 28000:2007 Specification for security management systems for the supply chain

[54] ISO 28001:2007 Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance

[55] ISO 28002:2011 Security management systems for the supply chain - Development of resilience in the supply chain - Requirements with guidance for use

[56] ISO/IEC 38500:2008 Corporate governance of information technology

[57] MSZ EN ISO 14001:2005 Környezetközpontú irányítási rendszerek, Követelmények és alkalmazási irányelvek (ISO 14001:2004)

[58] MSZ EN ISO 14004:2010 Környezetközpontú irányítási rendszerek, Az elvek, a rendszerek és a megvalósítást segítő módszerek általános irányelvei (ISO 14004:2004; angolnyelvű)

[59] MSZ ISO/IEC 17799:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2005)

[60] MSZ ISO/IEC 20000-1:2007 Informatika. Szolgáltatásirányítás. 1. rész: Előírás

[61] MSZ ISO/IEC 20000-2:2007 Informatika. Szolgáltatásirányítás. 2. rész: Alkalmazási útmutató

[62] MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

[63] MSZ 28001:2008 A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR), Követelmények (BS OHSAS 18001:2007)

[64] MSZ 28002:2009 A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR), Útmutató az MSZ 28001:2008 bevezetéséhez (BS OHSAS 18002:2008)

Mellékletek

1. melléklet – Szervezeti információk osztályozása információbiztonsági szempontból

2. melléklet – Információkezelési szabályok

3. melléklet – Információbiztonságért felelős személyek és feladatai

4. melléklet – Üzletmenetet befolyásoló fenyegetettségek

A most következő mellékletek Káté István diplomadolgozata alapján kerültek összeállításra. Alkalmazásukat mintapéldaszerűen javaslom. Nem tekinthetők teljes körű felsorolásoknak, inkább gondolatébresztésre alkalmasak. Ettől eltérő csoportosítások és meghatározások is jó eredményeket hozhatnak.

1. melléklet – Szervezeti információk osztályozása információbiztonsági szempontból

Nyilvános (public): Az az információ - adathordozótól függetlenül -, amit mindenki számára hozzáférhetővé kívánnak tenni és amit egy erre feljogosított szervezeti egység vezetője publikusnak, közérdekűnek minősített (pl. nyilvános honlapok tartalma, sajtónyilatkozatok)

Belső használatra… (internal): Minden olyan dokumentum, amely a többi kategóriába nem sorolható, ill. még nincs eldöntve, hogy melyik csoportba kerül. A „címzettek" köre előre nem meghatározott, de szervezeten belüli tagok. Ezeknek az információknak a nyilvánosságra, ill. illetéktelen kezekbe kerülése elhanyagolható versenyhátrányt és információbiztonság csökkenést okoz.

Bizalmas (confidental): Olyan információk (és hordozóik), amely egy előre meghatározott csoportnak (jellemzően vezetőknek) és az általuk bevont alkalmazotti körnek szólnak. Külső, illetéktelen fél kezébe kerülése esetén érezhető versenyhátrány, kimutatható pénzügyi veszteséget vagy jogi következményeket okozhat. Elősegítheti külső „támadások" megvalósítását (pl. szerződések, technológiák, IT rendszer dokumentációja, árkalkulációk, vezetőknek szánt helyzetértékelések, fizetési listák, személyes adatok, katasztrófa elhárítási tervek).

Szigorúan bizalmas (high confidental): Előre meghatározott, szűk körnek (szervezet felső vezetőinek és adatgazdáknak) szánt olyan információk, ill. dokumentumok, amelyek nyilvánosságra kerülésük esetén

- jelentős károkat
- súlyosan elmarasztaló jogi következményeket
- az információvédelmi rendszer súlyos sérülését
- jelentős fennakadásokat
- és munkamegtagadást okozhat (pl. felsővezetői döntés-előkészítő anyagok, nagy értékű szerződések, jelszavak, titkosító rendszerek dokumentációja, személyes kulcsokat tartalmazó tanúsítványok)

2. melléklet – Információkezelési szabályok

Eszközök, adathordozók	Információk osztályozása		
	Belső használatra	Bizalmas	Szigorúan bizalmas
Telefon	Nincs korlátozás.	Bizalmas információ csak a hívó, vagy hivott fél kétséget kizáró azonosítása után közölhető.	Bizalmas információ csak a hívó, vagy hivott fél kétséget kizáró azonosítása után közölhető biztonságosnak tartott távközlési csatornán.
Fax	Nincs korlátozás.	Csak akkor engedélyezhető, ha a küldő fél meggyőződött, hogy a vételi oldalon a címzett személyesesn is jelen van.	Csak akkor engedélyezhető, ha a küldő fél meggyőződött, hogy a vételi oldalon a címzett személyesesn is jelen van és a távközlési csatorna biztonságosnak tartott.
Papíralapú dokumentumok	Belső továbbítás irattartóban, külső továbbítás zárt borítékban...	A szállítás csak zárt borítékban, a címzettet név szerint megadva személyes átadással történhet. Használat után a dokumentumot zárható helyen kell tárolni. A borítékon a bizalmasságot TILOS jelölni!	A szállítás csak zárt borítékban, a címzettet név szerint megadva személyes átadással történhet. Használat után a dokumentumot páncélszekrényben kell tárolni. A borítékon a bizalmasságot TILOS jelölni. Ellenőrizni kell a személyes átvételt!
E-mail	Belső levél esetén nincs korlátozás, külső felek részére küldött elektronikus üzenetek esetén jogi következményeket tartalmazó záradék szerepeltetése indokolt.	Csak titkosítva továbbítható!	Csak titkosítva továbbítható! Elosztási listák használata TILOS! Minden címzett külön megnevezendő!
Intranet	Nincs korlátozás.	Titkosítás kötelező! A jogosult felhasználók felhasználói névvel és jelszóval férhetnek hozzá a tárolt adatokhoz.	Titkosítás kötelező! A jogosult felhasználók felhasználói névvel és jelszóval férhetnek hozzá a tárolt adatokhoz.
Internet	Internetes publikáció TILOS!	Internetes publikáció TILOS!	Internetes publikáció TILOS!
Mobil adathordozók (CD, DVD, pen drive, lap-top)	Nincs korlátozás.	Az eszközöket használaton kívül zárt helyen kell tárolni! A hordozható gépek lemezmeghajtóit titkosítani kell! Egyéb mobil adathordozókra az információk titkosított formában kerüljenek fel!	Az eszközöket használaton kívül zárt helyen kell tárolni! A hordozható gépek lemezmeghajtóit titkosítani kell! Egyéb mobil adathordozókra az információk titkosított formában kerüljenek fel!
Nyomtatás	Nincs korlátozás, hibás nyomtatásból származó dokumentumokat iratmegsemmísitővel kell megsemmisíteni.	A nyomtatás csak az adatgazda engedélyével történhet, kizárólag személyesen. A nyomtatást TILOS a nyomtató memóriájában tárolni! A kiinyomtatott dokumentumon szerepelni kell a "Bizalmas" jelölésnek! A hibás dokumentum iratmegsemmísitővel megsemmisítendő!	A nyomtatás csak az adatgazda engedélyével történhet, kizárólag személyesen. A nyomtatást TILOS a nyomtató memóriájában tárolni! A kiinyomtatott dokumentumon szerepelni kell a "Szigorúan bizalmas" jelölésnek! A hibás dokumentum iratmegsemmísitővel megsemmisítendő!
Irodai számítógépek	Nincs korlátozás, de a kész elektronikus dokumentumokat előírt helyen ajánlott tárolni (file server).	A használaton kívüli dokumentumokat a megfelelő jogosultági hátteret biztosító helyen, dokumentumtárban kell tárolni!	A használaton kívüli dokumentumokat a megfelelő jogosultági hátteret biztosító helyen, dokumentumtárban kell tárolni!
Archivum	Titkosítás nélkül...	Titkosítás nélkül kell archíválni! Az adathordozó tárolása során biztosítani kell az adatok visszaolvashatóságát, öregedés esetén új másolat készítését! Az archívumot tartalmazó adathordozót zárható helyen kell tárolni! A hozzáférésekről jegyzőkönyv készül.	Titkosítás nélkül kell archíválni! Az adathordozó tárolása során biztosítani kell az adatok visszaolvashatóságát, öregedés esetén új másolat készítését! Az archívumot tartalmazó adathordozót páncélszekrényben kell tárolni! A hozzáférésekről jegyzőkönyv készül. A hozzáférés csak előre meghatározott kör számára lehetséges.
Szóbeli kommunikáció	Szervezeten belül nincs korlátozás, külső féllel történő szerződés esetén titoktartásra vonatkozó pont szerepeltetése indokolt.	A fül- és szemtanút tájékoztatni kell a közlés bizalmasságáról! Külső fél esetében titoktartási megállapodás megkötése indokolt. Ellenőrizendő, hogy illetéktelen személy nem hallgatja ki a beszélgetést!	A fül- és szemtanút tájékoztatni kell a közlés bizalmasságáról! Külső fél esetében titoktartási megállapodás megkötése indokolt. Gondosan ellenőrizendő, hogy illetéktelen személy nem hallgatja ki a beszélgetést és hang- vagy képfelvétel nem készül-e róla...

3. melléklet – Információbiztonságért felelős személyek és feladataik

Ügyvezető (elsőszámú vezetője a szervezetnek…)

- információbiztonsági célok és politika megfogalmazása
- az információbiztonsági szabályozás / szabályzat jóváhagyása és jogszabályi megfelelésének figyelembevétele
- felelősségi körök definiálása
- erőforrás-biztosítás elfogadható kockázati szintek megadásával
- külső és belső auditok támogatása
- vezetői átvizsgálások elvégzése

Információbiztonsági vezető

- az információbiztonsági szabályzat karbantartása
- a szabályzatban foglaltak betartásának ellenőrzése az egész szervezetre kiterjedően
- információvédelmi oktatás szakmai követelményeinek összeállítása, a képzések szakmai irányítása
- biztonsági események megelőzése, a megtörtént esetek nyilvántartása és értékelése
- védelmi intézkedések kezdeményezése
- javaslatok szankciók foganatosítására
- kockázatelemzések irányítása
- kármegelőzés, -elhárítás és -mérséklés feladatainak és eredményességének elemzése
- együttműködés a szervezet többi vezetőivel a információbiztonság továbbfejlesztése érdekében
- informatikai biztonság fejlesztésének irányítása
- informatikai rendszerek üzemeltetésének biztonsági ellenőrzése
- minősítési és osztályba sorolási tevékenység

Informatikai vezető

- az információbiztonsági szabályzat érvényre juttatása

- a rendszergazdák biztonsággal kapcsolatos tevékenységének időszakos és eseti ellenőrzése
- biztonsági események naplózása és közreműködés a kivizsgálásban
- a biztonsági osztályba sorolás követelményeinek megfelelő rendszerek és eszközök adaptálása
- az információs rendszerek biztonsági tanúsítási és minősítési eljárásrendszerének kidolgozása
- biztonsági rendszerek tervezése, fejlesztése vagy átalakítása új technológiák bevezetésekor
- szervezet szintű információvédelmi rendszerek beruházásának előkészítése, lebonyolítása és rendszerbe állítása
- informatikai projektek erőforrás-szükségletének meghatározása az információbiztonsági szempontok figyelembevételével
- elektronikusan feldolgozott adatok tárolása, megőrzése és selejtezése, valamint adatbázisok, adattárházak üzemeltetése
- információs rendszerek kockázatarányos védelmének biztosítása és védelmi szabályok betartásának ellenőrzése
- információ technológiai eszközök (adathordozók is) rendszerből történő kivonásának és selejtezésnek információvédelmi szabályozásnak megfelelő lebonyolítása

Rendszergazda

- információs rendszerek üzemeltetése
- jogosultsági rendszerek létrehozása, nyilvántartása és módosítása
- informatikai eszközök beállítási dokumentációjának kezelése
- informatikai eszközök biztonsági beállításainak elvégzése
- szoftverek telepítése
- szoftverek és adatok biztonsági másolatainak elkészítése, archíválása
- hiba esetén részt vesz az információs rendszer helyreállításában és tesztelésében
- felelős a víruskereső rendszer naprakész működéséért
- biztonsági események jelentése az informatikai vezetőnek
- segítségnyújtás a felhasználóknak

Felhasználó

- köteles az információvédelmi szabályzatban rá vonatkozó részeket megismerni és betartani
- számára rendelkezésre bocsájtott informatikai eszközöket megóvni és felelősen használni (nem rendeltetésszerű használat→ kártérítési kötelezettség)
- informatikai eszközök illetéktelen hozzáférési kockázatának csökkentése
- illetékes vezető tájékoztatása az előforduló hibákról vagy biztonsági eseményekről
- együttműködő magatartás az eseti és a rendszeres biztonsági ellenőrzéseknél
- jelszó, ill. jogosultsági adatok megőrzése
- részvétel információbiztonsági képzéseken

4. melléklet – Üzletmenetet befolyásoló fenyegetettségek

Függés	Fenyegetettség	Hatás	Megelőzés
Közüzemek	Áramszünet	Korlátozott szolgáltatás ellátás	Csak indokolt fogyasztók táplálása szünetmentes áramforrásokról
	Távközlési zavarok	Összeköttetés megszakadása telephelyek között és partnerek felé	Szolgáltató-független redundáns kapcsolatok fenntartása
	Gázellátási zavarok	Munkavállalók kényszerű munkahely elhagyása	Alternatív fűtési rendszer biztosítása
Környezet	Viharok	Villámcsapás miatt villamos és távközlési infrastrúktura sérülése	Villámhárító rendszer beüzemelése
	Földrengés	Infrastrúktura, ingatlanok részleges vagy teljes megsemmisülése	Földrengésbiztos építési módok alkalmazása
	Áradás	Elektromos zárlatok	Áradásveszélyes területek mellőzése
	Tűzvész	Infrastrúktura részleges v. teljes megsemmisülése, adatvesztés	Tüzoltó, tüzvédelmi rendszer telepítése
Információ technológia	Szoftverhibák	Alkalmazások hibás funkcionalítása	Szoftverfejlesztési ciklusok és tesztelési előírások betartása
	Szoftver frissítés és verzióváltás	Operációs rendszerek, adatbáziskezelők és alkalmazások hibás funkcionalítása	Frissítések tesztelése éles üzleti környezetben történő használat előtt
	Hardver hibák	Szolgáltatás kiesés	Redundanciák biztosítása
	Hálózati aktív és passzív elemek meghibásodása	Hálózati forgalom akadozása, megbénulása	Redundanciák biztosítása
	Informatikai szállító kiesése	Szolgáltatási szint csökkenés	Előzetes szállítói minősítés, többes IT beszállítói kör kialakítása
	Adatvesztés	Szolgáltatás sérülés	Adat redundanciák használata, többszörös adat-tárolás
	Vírustámadás	Adatvesztés, információ technológia korlátozott működő képessége, hálózati terhelés növekedés	Naprakész virusdefinicós adatbázisok és víruskeresők alkalmazása
	Hibás beszerzés politika	Szolgáltatási szint csökkenés	Szakértői támogatás a beszerzések lebonyolításához
	Illetéktelen hozzáférés	Információk szivárgása	erős felhasználó azonosító eszközök alkalmazása
Infrastruktúra	Szerverszoba klimatizálásának leállása	Szerver leállás	Rendszeres megelőző karbantartás
	Fűtési rendszer leállása	Munkavállalók munkaképességnek csökkenése	Alternatív lokális fűtési megoldások biztosítása
	Vízvezeték sérülése	Villamos zárlatok, szolgáltatás kiesés	Megelőző karbantartás, védett és szegmentált villamos hálózat
Emberi tényezők	Kulcsemberek kiesése	Szolgáltatási szint csökkenés	Azonos képességű, helyettesítő munkaerő képzése
	Belső visszaélés, csalás, megveszegetés	Szolgáltatás sérülés	Információbiztonsági szabályozás
	Járványok	Szolgáltatás sérülés	Egészségvédelmi orvosi tanácsadás
	Bosszúállás	Szolgáltatás sérülés	Információbiztonsági szabályozás
	Szakképzetlenség	Szolgáltatás sérülés	Oktatás, képzés, számonkérés
	Fizikai rongálás	Szolgáltatás kiesés	Őrzés-védelem
	Illegális szoftverek használata	Szolgáltatás kiesés	Információbiztonsági szabályozás
	Dokumentálatlanság	Szolgáltatás sérülés	Oktatás, képzés, számonkérés
	Szakszerütlen IT tervezés és üzemeltetés	Szolgáltatás sérülés	Oktatás, képzés, számonkérés
	Sztrájk	Szolgáltatás kiesés	Minimális szolgáltatási szint megadása
	Adatlopás	Üzleti információk szivárgása	Információbiztonsági szabályozás
	Betörés	Üzleti információk szivárgása	Őrzés-védelem
	Szabotázs	Szolgáltatás sérülés	Részleges v. teljes helyettesítő megoldások fenntartása