Vállalatbiztonság

Dr. Michelberger Pál

Óbudai Egyetem, Keleti Károly Gazdasági Kar

Szervezési és Vezetési Intézet

michelberger.pal@kgk.uni-obuda.hu

Absztrakt: Számos tudományos cikk foglalkozik a felelős vállalati magatartással és gazdálkodó szervezetek etikus viselkedésével. Olyan értékelő és elemző modellek is születtek, amelyek révén a vállalatok minősíthetővé váltak. A megállapított pozitív eredmények azonban nem mindig hoznak kézzelfogható hasznot az érintett cégek számára. Sokszor csak a vezetők, tulajdonosok erkölcsi elkötelezettségét mutatják. Talán helyesebb lenne, ha a stratégiai célok megfogalmazásánál a „statikus" felelősségvállalás helyett, illetve mellett megjelenne a biztonságra és bizalomra való törekvés is. Ez utóbbiaknál talán hangsúlyosabb a „proaktív", kockázatelemzésen alapuló védelmi tevékenység. A biztonság – mint állapot – versenyképességi tényező is lehet és növelheti az üzleti bizalom mértékét. A tanulmány néhány modell, vizsgálati módszer és a szakirodalom elemzése alapján vizsgálja, hogyan lehet eljutni a kockázatoktól az üzleti partnerek által érzett bizalomig.

1 Bevezetés

A vállalatbiztonság olyan állapot, amelyben a gazdálkodó szervezet képes hosszútávon fenntartani a működőképességét és értékteremtő folyamatait, ill. nem várt események – akár katasztrófák – bekövetkezése után azokat a lehető legrövidebb idő alatt helyreállítani. A biztonság további kritériuma, hogy a vállalat jövője a stratégiai tervei alapján saját kezében van és a vállalat tevékenysége során nem veszélyezteti a környezetét, a külső és belső érintetteket. A vállalatbiztonság fenntartása holisztikus szemléletet kíván. Folyamatos kockázatelemzésen és az ez alapján meghatározott védelmi intézkedéseken alapszik.

A tanulmányban később tárgyalt szabványok és ajánlások szinte mindegyike folyamatorientált és egy-egy funkcionális vállalati területre vonatkoznak. „*A folyamat egy vagy több tevékenység, amely értéket növel úgy, hogy egy bemenetkészletet átalakít a kimenetek készletévé (javakká vagy szolgáltatásokká) egy más személy (a vevő, ill. felhasználó) számára, emberek, módszerek és eszközök kombinációjával.*" (Tenner –DeToro, 1998, p.75.)

A kockázatkezelés is vállalati folyamatokra (termékfejlesztés, értékesítés, beszerzés, termelés, szerviz, elosztás, stb.) irányul, és így elérhető a folyamatbiztonság, amely révén a folyamatokat végrehajtó szervezet az előírt időpontra megfelelő mennyiségű és minőségű kimenetet nyújt. Ha a vállalati – különösen az értékteremtő – folyamatok „biztonságosak", ill. elfogadott kockázati szint mellett üzemelnek, akkor az egész vállalat megfelelő „biztonsági állapotba" kerülhet (Michelberger – Lábodi, 2012, p. 285).

2 Vállalati kockázatkezelés

Egy vállalat számára kockázatot jelentenek azok a potenciálisan bekövetkező külső és belső események, zavarok, amelyek következtében veszélybe kerül a vevői igények kielégítése vagy bármely vállalati érintett (stake- és stockholder) biztonsága. Leegyszerűsítve a kockázat alatt bizonytalan események negatív hatásait értjük. Léteznek tiszta (csak káros következményt hozó) és ún. „spekulatív" (nyereséget és veszteséget egyaránt eredményező) kockázatok is (Horváth-Szlávik, 2011a).

A vállalati kockázatértékelés során megállapítjuk (sokszor csak megbecsüljük) a kárértéket és a negatív következmény valószínűségét (ISO 31000). Ha az ebből kijövő kockázati szint kellően alacsony, azaz az esemény bekövetkezésének valószínűsége és a káresemény „értéke" is alacsony akkor elfogadjuk, ill. együtt tudunk vele élni. Ellenkező esetben (lehetséges vagy majdnem biztos esemény, jelentős v. kritikus következménnyel) kockázatkezelésre kerül sor, amely rendszeres védelmi tevékenységet is jelenthet (Michelberger-Lábodi, 2012. p. 245). Kockázatkezelési mód lehet még az áthárítás (pl. biztosítás) vagy a kockázatot jelentő tevékenység megszüntetése (Horváth-Szlávik, 2011b.).

A kockázatkezelés szakszerű elvégzése előtt szükség lehet a kockázatok csoportosítására is. Beszélhetünk stratégiai, pénzügyi, piaci, jogi, működési és személyi, valamint környezeti kockázatokról. A kockázati kategóriák azonban gyakran összefüggnek egymással (Horváth-Szlávik, 2011a.), szétválasztásuk nem is mindig indokolt vagy lehetséges (pl. egy magasan kvalifikált, értékes munkaerő elvesztése…).

A kockázatok csoportosítására talán jobb a külső (piac, iparág, régió) és belső (folyamatok, erőforrások, szervezet, beruházások) környezetet alapul venni. A legfontosabb, hogy az értékelés minden lényeges kockázatra kiterjedjen.

3 Védelmi tevékenységet megalapozó szabványok és ajánlások

A vállalati biztonságért felelős vezetők a bőség zavarával küzdenek, amikor az üzletmenetet, ill. annak irányítását biztonsági szempontok alapján is szabályozni kívánják. Számos szabvány, ajánlás tárgyalja vagy érinti a vállalati biztonság egy-egy területét. A most −a teljesség igénye nélkül − felsorolt dokumentumok a biztonság több szempontú megközelíthetőségét mutatják

3.1 COSO ERM keretrendszer

A COSO (Comitte of Sponsoring Organisations of Treadway Comission) által a 90-es évek elején összeállított és folyamatosan fejlesztett vállalati kockázat kezelő (Enterprise Risk Management) keretrendszer a vállalat belső folyamataira, azok szabályozására és ellenőrzésére vonatkozik. Az üzleti stratégiát szem előtt tartva minden kockázattípusra alkalmazható, de elsősorban pénzügyi területeken alkalmazzák.

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, 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 (Racz et.al, 2010) 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.

3.2 MSZ ISO/IEC 27001

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 (MSZ 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 számos – önálló szabványként megjelenő − kiegészítő rész is (pl. információbiztonsági kockázat kezeléssel kapcsolatos előírások – ISO/IEC 27005); bevezetési útmutató – ISO/IEC 27003; szektorok közötti kommunikáció szabályozása információbiztonsági szempontból – ISO/IEC 27010; a telekommunikáció információbiztonsága – ISO/IEC 27011).

3.3 MSZ EN ISO 14001

A gazdálkodó szervezetek a működésükkel kapcsolatos környezetvédelmi feladataik ellátásának támogatására szabványosított környezetközpontú irányítási rendszert alkalmazhatnak (MSZ EN ISO 14001). A cél többek között a környezet terhelésének és működés környezeti hatásainak csökkentése, a vállalati image növelése, valamint a környezetet érintő viselkedés-kultúra elfogadtatása.

A környezetközpontú irányítási rendszer a szabványnak megfelelően foglalkozik a szervezet tevékenységeinek környezetet befolyásoló hatásaival, kockázatértékeléssel, a működéssel kapcsolatos jogi és egyéb biztonsági követelményeknek történő megfeleléssel és a még elfogadható környezetterhelés elérésével. Meghatározza a környezettudatos működéshez a szükséges erőforrásokat és képességeket, valamint a külső és belső kommunikáció formáit. Szabályozza a vészhelyzetekre történő felkészülést, a hibaelhárítást, az ellenőrzést és a megelőző tevékenységeket. A rendszerszabvány nem ad meg kibocsátásra vonatkozó konkrét követelményeket és ellenőrzési módszereket. Alkalmazása elsősorban etikai indíttatású, de egyre fontosabb szerepet játszanak a jogi és gazdasági követelmények is.

3.4 CObIT 4.1

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.

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:

1. tervezés és szervezés,
2. beszerzés és megvalósítás,
3. szolgáltatás és támogatás,
4. figyelemmel kísérés értékelés.

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

3.5 ISO/IEC 15504

Az ISO/IEC 15504-es szabványcsomag alapján a vállalati folyamatokat két dimenzió alapján lehet csoportosítani és értékelni, valamint fejleszteni. Mi az adott folyamat célja, várható eredménye és mit tudunk általa elérni (folyamatképesség)?

A folyamatképesség szintjei a következők (ISO/IEC 15504-2):

0. szint – hiányos folyamat (a folyamat célja nem biztos, hogy teljesül…),
1. szint – végrehajtott folyamat (a folyamat célja valamilyen szinten teljesül, van eredmény),
2. szint – irányított folyamat (és a folyamat eredménye is megfelelően kezelt),
3. szint – kialakított folyamat (a folyamat minta / szabvány alapján „megtervezett" és végrehajtott),
4. szint – kiszámítható folyamat (a folyamat mérhető és ellenőrizhető),
5. szint – optimalizáló folyamat (a folyamat fejleszthető és a megadott célok teljesülnek, itt már megjelenik a „visszacsatolás" is…).

A folyamatok értékelésével és kimeneteik minősítésével a kockázatértékelés irányába is elindulunk. A végrehajtott és az irányított folyamatok „közepes" és „magas" kockázatot hordoznak. A 3. és 4. szinthez (kialakított és kiszámítható folyamatok) már csak „közepes" és „alacsony" kockázati szint társul. Az optimalizáló folyamat pedig csak alacsony kockázatú lehet. A megállapított kockázati szint természetesen függ attól is, hogy a tényleges folyamat a valóságban mennyire tér(het) el az előre megadott képességszintjétől (Iványos – Roóz, 2010).

3.6 MSZ ISO 28001

A gazdálkodó szervezetek számára legfontosabb erőforrás a szakmailag felkészült, értékteremtő ember. A munkahelyi egészségvédelem és biztonság hatékony kezelését támogatja az MSZ 28001-es szabvány 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.

3.7 MSZ ISO/IEC 20000

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. 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. A szolgáltatás menedzsment tevékenységek a ma népszerű, a többi szabványban is alkalmazott „Plan-Do-Check-Act" 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:

- szolgáltatásbiztosítás (szolgáltatási szint, szolgáltatási jelentések, kapacitás, szolgáltatás folytonosság és rendelkezésre állás, információ biztonság, informatikai szolgáltatás költségtervezése és pénzügyi kezelése),
- szabályozási folyamatok (konfiguráció- és változás menedzsment),
- kiadási folyamatok (dokumentumok, működési leírások kiadás kezelése, a jóváhagyott változások dokumentálása),
- megoldási folyamatok (incidens- és problémakezelés),
- Kapcsolattartás (ügyfélszolgálat, üzleti- és szállítói kapcsolatok kezelése).

3.8 BS 25999

A brit üzletmenet folytonossággal 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 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 „Plan-Do-Check-Act" ciklus alapján fontos az irányítási rendszer dokumentálása és rendszeres vezetői átvizsgálása, valamint tesztelése és folyamatos fejlesztése is.

3.9 A SCOR és a CPFR Modell

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).

Az ellátási láncot alkotó szervezetek eredményei nem egyszerűen összeadódnak, hanem az erőforrás-allokációból adódóan a gazdálkodás különböző területein egymást felerősítő szinergikus hatások alakulnak ki. Ez azonban a kockázatokra is igaz. Az ellátási lánc menedzsmentje a vállalatok tudatos együttműködését jelenti. Elfogadják, hogy annak léte versenypozíciójuk javulását eredményezi. A lánc tagjai hajlandók lemondani rövid távú előnyöket hozó egyéni érdekeik érvényesítéséről a teljes lánc optimális működésének érdekében. Ez közös kockázatkezelést és komplex „ellátás" biztonságot eredményező védelmi tevékenységet is feltételez. Ennek szabályozásában nyújthat segítséget az **ISO 28000**-es szabványcsomag, amely az ellátási láncok biztonság irányítási rendszerére vonatkozó követelményeket is tartalmazza.

Az ellátási láncokban fontosabb a teljes hálózat hatékony működése, mint a tagvállalatok egyéni erőforrás felhasználási optimuma. Ez bevált CPFR (Collaborative Planning, Forecasting and Replenishment) folyamatmodell alapján arra készteti a vállalatokat, hogy együttműködjenek. 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. Ez az ellátásbiztonságot is javítja.

4 Érintettek, fenntartható fejlődés és vállalati felelősség

A vállalatbiztonság külső szemlélő részéről nehezen értékelhető, hiszen nem ismeri részletesen a vállalati kockázatokat, azok belső minősítését és az ezekre hozott védelmi intézkedéseket. Az üzleti partnereket sokszor a vállalat önmagáról kialakított – biztonsági elemeket is tartalmazó – képe is befolyásolja. Ebben az esetben a vállalatbiztonságot a nehezen mérhető üzleti bizalom is minősíti.

Edward R. Freeman vezette be az ún. stakeholder-szemléletet a nyolcvanas évek elején. Minden gazdálkodó szervezetnél találhatók olyan külső és belső csoportok (kormányzat, versenytársak, szakmai és civil szervezetek, alkalmazottak, fogyasztók, szolgáltatók, beszállítók, hitelezők stb.), akik érintettek a szervezet küldetésének teljesítésében (Freeman, 1984). Ezek a csoportok sokszor befolyással bírnak a vállalat erőforrásaira is. Az érintettekkel (stakeholderekkel) történő kapcsolattartás, a velük folytatott üzleti tranzakciók sikeressége és az ő érdekeik figyelembe vétele létfontosságú a vállalatbiztonság szempontjából. A kockázatok számbavétele és értékelése során tisztázni szükséges az érintettekkel való viszonyt, hatásukat a vállalati folyamatokra és kimenetekre, valamint az érintettek „erőterét”, azaz milyen irányban kívánják befolyásolni a vállalat működését és nem megfelelő kapcsolat esetén milyen veszélyt jelenthetnek a vállalati folyamatok végrehajtására. Az érintetteket a vállalati jövőkép kialakításába, a stratégiai tervezésbe is be lehet vonni. „Barátságos” környezetben, közös célok megfogalmazásával könnyebb a vállalati működést fenntartani, zavar esetén helyreállítani.

A vállalatok hosszú távú működése szempontjából egyre fontosabb a fenntarthatóság kérdése. A vállalat elfogadottságát növeli − főleg annak közvetlen környezetében, régiójában − ha nem zsákmányolja ki visszafordíthatatlanul az erőforrásait. Egy biztonságra törekvő vállalat esetében a célok között az erőforrások hosszútávon történő biztosítása is megjelenik, és ez alapvetően befolyásolja a saját régióban található stakeholderekkel való viszonyt. Akár a

versenytársakkal is kiegyeznek, ha a fenntarthatóság kerül veszélybe. Ez természetesen a vállalatbiztonság operatív (rövidtávú) és stratégiai bontását is igényelheti. Az erőforrás-függőség helyett / mellett a regionális fenntarthatóság – mint környezeti, társadalmi igény – is jelentkezik az alkalmazkodó vállalat biztonságpolitikájában és stratégiai terveiben. Az eddig költségalapon hozott üzleti döntésekben (vegyem vagy gyártsam?; ki legyen a beszállító?; honnan biztosítom a szükséges munkaerőt?; fejlesztek vagy know-how-t vásárolok?) szerepet kapnak a biztonság és a regionális fenntarthatóság szempontjai is. Olyan bizalmi légkörre lenne szükség, amelyben kialakulhat érdemi párbeszéd a régióban megtalálható, és erőforrásokat nyújtani tudó potenciális érintettekkel (Zsóka – Zilahy, 2011). A regionális fenntarthatóságot is szem előtt tartó vállalatoknak talán lehetőséget kellene kapni, hogy bemutassák, működési folyamataikat, innovációs tevékenységüket…

A vállalat-vezetés és a felelős vállalati magatartás (Corporate Social Responsibility - CSR) összekapcsolása értelmezhető úgy is, hogy a vállalatnak milyen a viszonya az érintettekkel (Zolnai et.al, 2005). A vállalati felelősség nem egyszerűen etikai kategória. Nyereséget kell termelni a tulajdonosoknak, ki kell elégíteni a vevőket és be kell tartani piacon elfogadott írott és íratlan szabályokat, valamint mérlegelni kell üzleti döntéseinknek rövid és hosszú távú hatásait a környezetre, a társadalomra, és az egyénre egyaránt.

Az Európai Bizottság definíciója szerint a CSR „*olyan koncepció, amely alapján a vállalatok a társadalmi és környezeti megfontolásokat üzleti folyamataikba és a stakeholderekkel folytatott interakcióikba integrálják, önkéntes alapon*." (EC, 2005)

Hogyan kapcsolódik ez a vállalatbiztonsághoz? A bizonyítottan „felelős vállalat" bizalmat ébreszt az érintettekben, amely így biztonságot is szolgáló üzleti tranzakciókat hozhat.

A bizonyítás alapja lehet valamilyen szabály szerint végrehajtott önértékelés[1] vagy külső fél által végzett felelős magatartást elemző vizsgálat. A vizsgálatok az alábbi szempontok szerint történhetnek (Angyal, 2008):

- jog- és szabálykövetés (pl. bírósági szakaszba került jogsértések száma),
- etikus magatartás (pl. rendelkezik-e a vállalat etikai kódex-szel) ,
- környezethez való viszony (pl. van-e ISO 14001-es környezetirányítási rendszer),
- érintettek elégedettsége (pl. vevői v. alkalmazotti elégedettség rendszeres mérése és értékelése),

1 Ilyen önértékelési modellek pl. az Európai Kiválósági Rendszer (European Foundation for Quality Management – EFQM; www.efqm.org) és az Általános Beszámoló (General Reporting Initiative – GRI; www.globalreporting.org)

- politikai illeszkedés (pl. együttműködés kormányzattal, önkormányzattal, civil szervezetekkel),
- társadalmilag hasznos, de nem profitorientált tevékenység (pl. mecenatúra),
- társadalmi problémákra való fogékonyság.

5 Irányítási és kontrollrendszerek létrehozása a vállalatbiztonság érdekében

A 2. fejezetben és az irodalomjegyzékben megadott számos szabvány és ajánlás nehéz helyzetbe hozza a stratégiai döntéshozókat. A nagyszámú lehetőség közül rendkívül nehéz kiválasztani az alkalmazandó útmutatásokat és kialakítandó irányítási rendszereket. Ennyi mindenre egyszerre felkészülni nem lehetséges. A „bürokrácia" és a folyamatok több-szempontú szabályozása felőrölheti a vállalati menedzsment erőforrásait. Egy idő után a szabályozott működés fontosabb lehet, mint a vállalat termék és / vagy szolgáltatás kibocsátása.

A megoldás az integrált irányítási és kontrollrendszerek alkalmazásában körvonalazódik.

Az ISO 9001 minőségirányítási, az ISO 14001 környezetirányítási és az ISO 27001 információbiztonsági szabványok közös jellemzője a folyamatközpontúság. Mindegyik az ISO 9001 felépítését követi. A szabványok végén található mellékletek a tartalomjegyzékek pontjait követve ezt a kapcsolatot részletesen bemutatják. A szabványalkotók egyik célja az volt, hogy a szabványok – a többszörös szabályozást elkerülve - integráltan is bevezethetők legyenek. A kialakított integrált irányítási rendszer „egyszeres" auditálása is megoldható.

A BPM-GOSPEL (Business Process Modelling for Governance SPICE and Internal Fianancial Control) konzorcium magyar szakemberek közreműködésével 2012-ben kidolgozta a „Felelős Vállalkozások Irányítási Modelljét, amely a COSO és CObIT ajánlásokon, valamint az ISO/IEC 15504-es szabványcsomagon alapszik. A vállalat a modell alkalmazásával képes lehet a fenntartható, szabályozott és ellenőrzött üzletmenet kialakítására, ami kiválthatja az érintettek – elsősorban az üzleti partnerek – bizalmát.

A COSO vállalati kockázatkezelési keretrendszer alapján megfogalmazott előírások gond nélkül beilleszthetők az ITIL és/vagy CObIT alapján kialakított keretrendszerbe (Wilder, 2008, p.12).

Az ISACA, az Információellenőrök Nemzetközi Szervezete 2009-ben olyan információbiztonsági üzleti modellt (Business Model for Information Security) dolgozott ki, amelybe számos területet érintő szabványt és ajánlást integrált.

2008-ban az IT Governance Institute és az Office of Government Commerce szervezetek olyan ajánlást publikáltak az ISACA honlapján, amelyben az információs rendszerek üzemeltetésének (ITIL ill. ISO/IEC 20000) és az információbiztonság irányításának (ISO/IEC 27002), valamint az információtechnológia irányításának és ellenőrzésének (CObIT) együttes alkalmazási lehetőségét dolgozták ki.

6 Biztonság szerepe a versenyképességben

„*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. A tartós működőképesség feltételezi, hogy a vállalat törekszik a biztonságra, a fizikai és emberi erőforrások, a vállalati folyamatok, az innováció, a piaci kereslet és a vállalat közvetlen környezete szempontjaiból egyaránt.

A vállalatok tőkéje, a termékek és szolgáltatások iránti kereslet, az üzleti bizalom (hiánya), a regionális érdekek és a vállalatfejlesztési elképzelések (piac, termék, technológia, szervezet) eredményessége mind-mind a versenyképesség fokmérője. A versenyképesség fenntartása a gazdálkodó szervezet stratégiai céljainak elérését is jelenti változó gazdasági, jogi, piaci és kulturális viszonyok között.

„*Az …üzleti bizalom alacsony szintje egyrészről beszűkíti valamennyi – a gazdaság működtetésében érdekelt – szereplő fennmaradási és fejlődési lehetőségeit, másrészről a bizalomhiányból fakadó kockázati felár (pl. magasabb kamatok, biztosítási díjak, behajtási költségek, stb. formájában) indokolatlanul megnöveli működési költségeket, ezzel csökkentve a hatékonyságot és a versenyképességet*." (Felelős Vállalkozások Irányítási Modellje, BPM-GOSPEL, 2012, p. 5.)

7 Következtetések

A vállalati biztonság menedzsment képes a vállalati kritikus folyamatokat és eszközöket úgy ellenőrzése alatt tartani, hogy teljesüljenek a stratégiai tervekből levezetett vállalati célok. Olyan folyamatos tervezési, szervezési, irányítási és

ellenőrzési, valamint koordinációs tevékenységeket jelent, amely a vállalat minden külső és belső érintettje számára megfelelő és fenntartható biztonsági szintet eredményez. A technikai kérdések helyett a szervezeti működés válik elsődlegessé. Lehetővé teszi a biztonsági célok elérésének mérését és folyamatos fejlesztését és optimalizálását (Carelli et.al, 2004, p. 14).

A vállalat biztonság tehát állapot. Ez azonban nem tekinthető statikusnak. Kockázatelemzésen és -kezelésen alapuló, állandó fejlesztést és ellenőrzést igénylő folyamatos védelmi tevékenység lehet csak eredményes a gazdálkodó szervezeteknél. A vállalati szakterületek biztonsági igényei mellett, után fontos szerepet kapnak a folyamatok és azok ügyviteli leképezése. Ez utóbbi munkakörök kialakítását, munkaköri feladatok meghatározását teszik szükségessé. A szervezetek legfőbb biztonsági kockázata az ember és a vállalat biztonság csak úgy érhető el, ha folyamatokban résztvevők munkáját szabályozzuk, ill. felkészítjük őket nem várt kockázati események kezelésére.

A vállalatbiztonság nem a végső cél. Ha ez a külső és belső érintettek számára elfogadható, akkor megjelenik a vállalat versenyképességében is, amely később nehezen számszerűsíthető, de nehezen is erodálható (szervezetek közötti) bizalmat fog eredményezni. Az üzleti bizalom visszahat a versenyképességre és azon keresztül a biztonságra is. A bizalom a vállalat üzleti környezetét is minősíti. A bizalommal viseltető érintettek segíthetnek a jobb vállalati teljesítmény elérésében.

Irodalom

[1] Angyal Ádám: Vállalatok társadalmi felelőssége. (Versenyben a Világgal 2007-2009, 51. műhelytanulmány). Versenyképesség Kutatások Műhelytanulmány-Sorozat, Budapesti Corvinus Egyetem, Vállalatgazdaságtan Intézet, 2008.

[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 Erzsébet – Zoltayné Paprika Zita: Vállalati versenyképesség a globalizálódó magyar gazdaságban. Akadémiai Kiadó, 2002.

[4] Freeman, R. Edward : Strategic Management. A Stakeholder Approach. Pitman Series in Business and Public Policy, 1984.

[5] Horváth Zsolt - Szlávik Péter: Vállalati integrált kockázatkezelés I-II.. Minőség és Megbízhatóság, 2011/3. szám pp. 124-130 és 2011/4. szám pp. 219-226.

[6] Iványos János – Rooz József: Új megközelítés a közszféra belső kontrollrendszereinek értékelésére. Pénzügyi Szemle, 2010/2. szám, pp. 364-379.

[7] Michelberger Pál – Lábodi Csaba: Vállalati információbiztonság szervezése. In Nagy Imre Zoltán (szerk.): Vállalkozásfejlesztés a XXI. században II. Tanulmánykötet, Óbudai Egyetem, 2012, pp. 241-302.

[8] 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.

[9] Wilder, Dan: The New Business Continuity Model. White paper, 2008, p 58. www.talkingbusinesscontinuity.com/downloads/pdf/The-New-Business-Continuity-Model.pdf (letöltés dátuma: 2013. 03.29.)

[10] Tenner, Arthur R. – DeToro, Irving J.: BPR, Vállalati folyamatok újraformálása. Műszaki Könyvkiadó, Budapest, 1998.

[11] Zolnai László - Győri Zsuzsanna - Kenyeres Annamária - Jorge Vidal: Vállalkozások társadalmi felelőssége az Európai Unióban és Magyarországon. MKIK, 2005.

[12] Zsóka Ágnes – Zilahy Gyula: A vállalatok szerepe a regionális fenntarthatósági kezdeményezésekben. In Csutora Mária – Hofmeister Tóth Ágnes (szerk.): Fenntartható fogyasztás? A fenntartható fogyasztás gazdasági kérdései. Szöveggyűjtemény, Budapesti Corvinus Egyetem, 2011, pp. 155-176.

[13] BPM-GOSPEL projekt konzorcium (Business Process Modelling for Governance SPICE and Internal Financial Control): Felelős Vállalkozások Irányítási Modellje. A Vállalkozások Irányítási Képességének Fejlesztéséhez, 2012. www.trusted.hu/attachments/article/46/Felel%C5%91s%20V%C3%A1llalkoz%C3%A1sok%20Ir%C3%A1ny%C3%ADt%C3%A1si%20Modellje.pdf (letöltés dátuma: 2013.03.04.)

[14] An Introduction to the Business Model for Information Security, ISACA, 2009.

www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf (letöltés dátuma: 2013.03.14.)

[15] Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, ISACA, 2008, A Management Briefing from IT Governance Institute & Office of Government Commerce
www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf (letöltés dátuma: 2013.02.25.)

[16] CObIT 4.1. verzió (magyar változat - Control Objectives for Information and related Technology (CObIT) 4.1 - Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések) IT Governance Institute, USA, 2007.
www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf
(letöltés dátuma: 2013. 03.29.)

[17] Collaborative Planning, Forecasting and Replenishment (CPFR). Overview, 2004, Voluntary Interindustry Commerce standards (VICS).
www.vics.org/docs/standards/CPFR_Overview_US-A4.pdf (letöltés dátuma: 2013.04.03.)

[18] 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: 2013.03.27.)

[19] Supply Chain Council. Supply-Chain Operations Reference (SCOR) Model. Overview. Version 10.0, 2010
http://supply-chain.org/f/Web-Scor-Overview (letöltés dátuma: 2013.04.03.)

[20] Sustainability Reporting Guidelines. Version 3.1, 2011
www.globalreporting.org/resourcelibrary/G3.1-Guidelines-Incl-Technical-Protocol.pdf (letöltés dátuma: 2013.04.03.)

[21] BS 25999-1:2006; Business Continuity Management, Code of Practice

[22] BS 25999-2:2007; Business Continuity Management, Specification

[23] ISO 28000:2007; Specification for security management systems for the supply chain

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

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

[26] ISO 31000:2009; Risk management – Principles and guidlines

[27] ISO 31010:2009; Risk management – Risk assessment techniques

[28] ISO/IEC 15504-1:2004 Information technology – Process assessment – Part 1: Concepts and vocabulary

[29] ISO/IEC 15504-2:2003 Information technology – Process assessment – Part 2: Performing an assessment

[30] ISO/IEC 15504-2:2003/Cor 1:2004

[31] ISO/IEC 15504-3:2004 Information technology – Process assessment – Part 3: Guidance on performing an assessment

[32] ISO/IEC 15504-4:2004 Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination

[33] ISO/IEC 15504-5:2012 Information technology − Process assessment − Part 5: An exemplar software life cycle process assessment model

[34] ISO/IEC TR 15504-6:2008 Information technology − Process assessment − Part 6: An exemplar system life cycle process assessment model

[35] ISO/IEC TR 15504-7:2008 Information technology − Process assessment − Part 7: Assessment of organizational maturity

[36] ISO/IEC TS 15504-8:2012 Information technology − Process assessment − Part 8: An exemplar process assessment model for IT service management

[37] ISO/IEC TS 15504-9:2011 Information technology − Process assessment − Part 9: Target process profiles

[38] ISO/IEC TS 15504-10:2011 Information technology − Process assessment − Part 10: Safety extension

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

[40] MSZ EN ISO 9001:2009; Minőségirányítási rendszerek. Követelmények (ISO 9001:2008)

[41] MSZ EN ISO 14001:2005; Környezetközpontú irányítási rendszerek. Követelmények és alkalmazási irányelvek (ISO 14001:2004)

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

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

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

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

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

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

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

[49] Opinion of the European Economic and Social Committee on Information and measurement instruments for corporate social responsibility (CSR) in a globalised economy, European Commission, 2005