International Journal of Engineering and Management Sciences (IJEMS) Vol. 2. (2017). No. 4.
DOI: 10.21791/IJEMS.2017.4.28.

Biztonságorientált folyamatmenedzsment
Security Oriented Process Management

MICHELBERGER PÁL, HORVÁTH ZSOLT

Óbudai Egyetem, Keleti Károly Gazdasági Kar, Szervezési és Vezetési Intézet, michelberger.pal@kgk.uni-obuda.hu
Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Gépészeti és Biztonságtudományi Intézet, horvath.zsolt@bgk.uni-obuda.hu

Absztrakt. A vállalati kockázatmenedzsment elméleti háttere az ISO 31000-es szabványcsomaggal és a COSO ajánlással megalapozottnak tekinthető. Vállalati körben történő alkalmazásuk azonban „helyismeretet" és szakmai tapasztalatokat igényel. A kockázatmenedzsment napjainkban jellemzően még mindig funkcionális területekhez, ill. szervezeti egységekhez kötődik (pl. logisztika, pénzügy, minőségirányítás, emberi erőforrás, IT). Ez a szemlélet a szerzők véleménye szerint gyakran párhuzamos, többszörös szabályozást eredményez a kockázatmenedzsment területén. Holisztikus szemlélettel és a vállalati folyamatok kockázati szempontú elemzésével ez elkerülhető. A tanulmány megírásának hármas célja volt;

- *a folyamat- és kockázatmenedzsment alapjainak áttekintése,*
- *a folyamatok kockázatkezelésénél alkalmazható ötlet szakmai felvetése (Van-e lehetőség a folyamatokhoz rendelt erőforrások rendelkezésre állásának elemzésével az üzleti kockázat csökkentésére?),*
- *a folyamatok kockázatkezelésben alkalmazható szabványok és ajánlások összegyűjtése.*

Abstract. Theoretical background of enterprise risk management can be considered as founded by the ISO 31000 standard family and the COSO recommendation. However, their application in a given company domain requires knowledge of the local environment, and professional experience. Nowadays risk management is still anchored to functional fields, or organisational units (logistics, finance, quality management, HR, IT, e.g.). According to the view of the authors, this approach could results in parallel, multiple regulations of risk management. This could be avoided by a holistic view, and a risk based analysis of company processes. Writing this study is aimed at three major goals:

- *providing an overview of the bases of process and risk management,*
- *proposing a professional idea to be used at risk management of processes (Is it possible to reduce business risk by analysing availability of resources assigned to processes?),*
- *providing a review of standards and recommendations which can be used in process risk management.*

Bevezetés

Bár a folyamatmenedzsmentben több kockázatkezelésre alkalmas elem is van (folyamat-kontrolling és folyamatköltségek vizsgálata), de az ilyen témájú szakirodalomban a „kockázat" szó nagyon ritkán jelenik csak meg. Indokolt lehet a mára letisztult kockázatmenedzsment eszközöket a folyamatszervezés és végrehajtás szolgálatába állítani.

DOI: 10.21791/IJEMS.2017.4.28.

1. Kockázatmenedzsment

1.1. Kockázat fogalma

Egy vállalat, szervezet számára kockázatot jelentenek azok a potenciálisan bekövetkező külső és belső események, zavarok, amelyek következtében veszélybe kerül a vevői, ügyfél 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 [9].

A szakirodalomban egyre gyakrabban kerül középpontba a „pozitív" kockázatok vizsgálata [20]. Ez a folyamatmenedzsment esetében két dolgot jelenthet; jobb (folyamat)-minőséget és alacsonyabb (folyamat)-költségeket. Egy folyamat vagy tevékenység előírtnál gyorsabb végrehajtása egy vállalat számára nem mindig hordoz pozitív hatást a folyamat kimenetei szempontjából (pl. egy rögzített időpontra megrendelt szállítmány korábbi beérkezése a logisztikai rendszer működését megzavarhatja, amely ugyanolyan negatív kockázatot jelent(het), mint a szállítmány késése…).

A vállalatok a kockázatmenedzsment fogalma alatt jellemzően a kockázatok lehetséges negatív hatásai elleni védekezést értik, és azokat a módszereket alkalmazzák. A cikk további részében a kockázatok alatt mi is csak a negatív kockázatokat értjük, és azok menedzsmentjével kapcsolatos állításokat mutatunk be [10].

A szervezeti működéssel kapcsolatba hozható incidensek, események 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. A hagyományos kockázati megközelítés mellett – pontosan meghatározható kockázati adatok hiányában – beszélhetünk „sebezhetőségről" is, amelyek a szervezeti folyamatokat fenyegető veszélyek eredetét mutatja.

1.2. Kockázatok típusai, csoportosítása

A kockázatokat különböző szempontok szerint lehet csoportosítani. A tradicionális menedzsment irodalomhoz igazodva megkülönböztethetünk külső- és belső kockázatokat. A külső kockázatok a szervezet tevékenységétől, döntéseitől függetlenek (pl. jogszabályi változások, katasztrófa helyzetek, beszállítói piac változása). A belső kockázatok a szervezet működésével, folyamataival vannak összefüggésben (pl. vezetői hibák, pénzügyi döntések, nem megfelelő marketing tevékenység) [9]. A kategorizálás megkönnyítheti a kockázatok felismerését és kezelését és segít felelősöket találni az általában funkcionális felépítésű szervezetekben.

A kockázatkezelés jellemző szakmai (védelmi) területei a következők [5]:

- vagyon-,
- személy-,

DOI: 10.21791/IJEMS.2017.4.28.

- információ-,
- környezet-,
- munkahelyi egészségvédelem (munkabiztonság is…),
- valamint az informatikai rendszerek és az üzleti folyamatok, kapcsolatok védelme.

Egy másik lehetséges csoportosítás [6]:

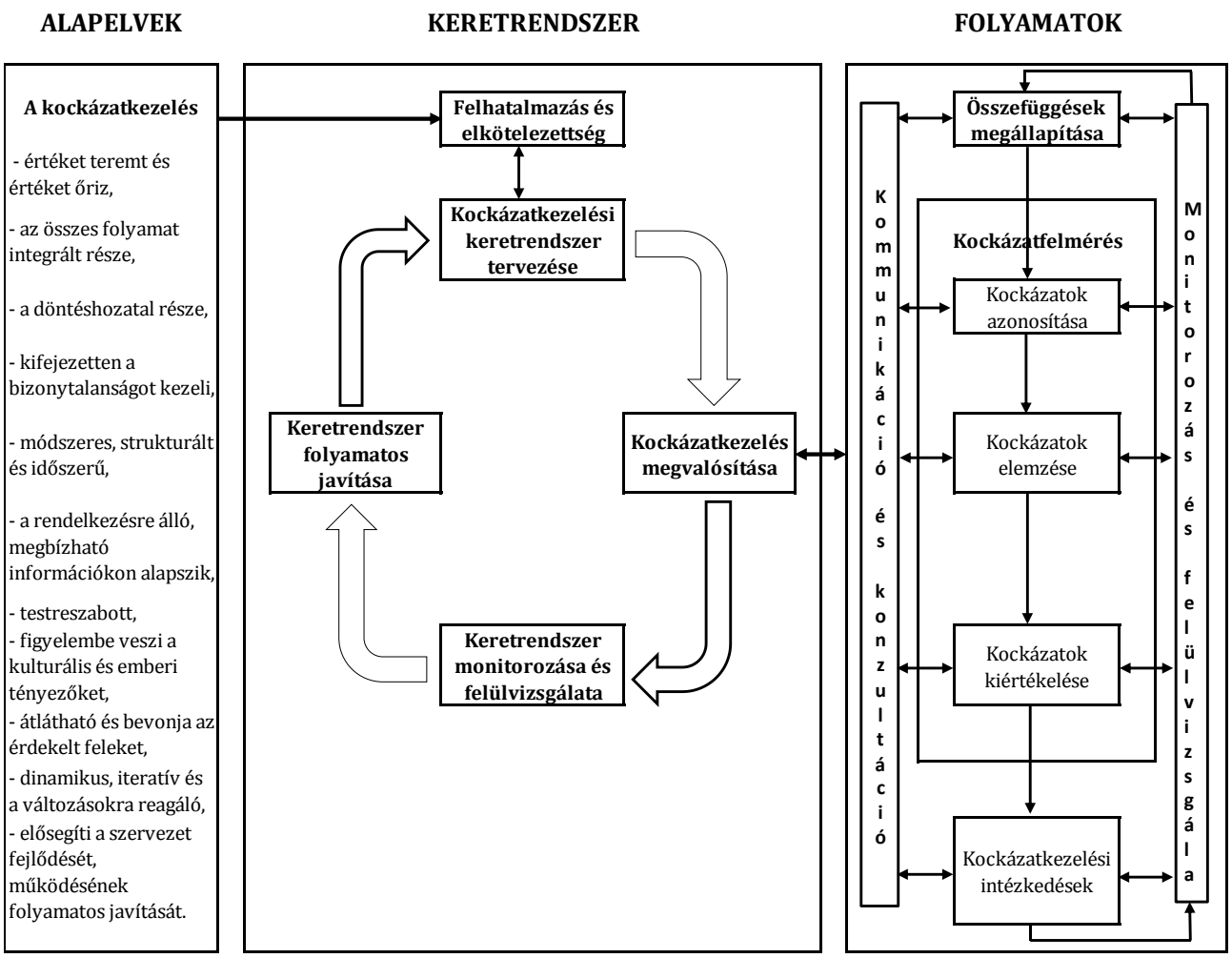
- pénzügyi és finanszírozási kockázatok (pl. árfolyamváltozás, jegybanki alapkamat, alapanyagárak alakulása, kinnlevőségek),
- stratégiai kockázatok (szabályozási v. politikai környezet megváltozása, vevők és beszállítók hosszútávra szóló döntései, a szervezet megítélése és annak változása),
- működési kockázatok (humán erőforrás, információs és kommunikációs technológia, termelő eszközök működőképessége),
- projektkockázatok (a szervezet életében nem ismétlődő projektek – beruházások, innovációk – már említett kockázatai).

Számos területnek (pl. információbiztonság, minőségmenedzsment, környezetirányítás, munkahelyi egészségvédelem, karbantartás, pénzügy, termelés) sajátos, olykor tradíciókon alapuló kockázatkezelési gyakorlata van, ami sok esetben egymástól független és a gazdálkodó szervezet működését többszörösen megterheli, érinti a vállalat (szervezet) külső és belső környezetét egyaránt. Indokolt lehet tehát a kockázatok kezelésének holisztikus és integrált megközelítése [13]. A kockázati kategóriák azonban gyakran összefüggnek egymással, szétválasztásuk nem is mindig indokolt vagy lehetséges (pl. egy magasan képzett, értékes munkaerő elvesztése…). A legfontosabb az, hogy minden szervezetet és annak működését érintő lényeges kockázatot azonosítsunk.

1.3. Kockázatok azonosítása, elemzése, értékelése és kezelése

A vállalati kockázatértékelés során megállapítjuk (sokszor csak megbecsüljük) a kárértéket és a negatív következmény valószínűségét [38]. 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. Kockázatkezelési mód lehet még az áthárítás v. megosztás (pl. biztosítás) vagy a kockázatot jelentő tevékenység megszüntetése. A kockázatmenedzsment a jól ismert PDCA ciklushoz hasonlóan körfolyamat [2]. Kockázatok azonosítása után elemezni kell a kockázatokat, majd értékelni és súlyuknak megfelelően rangsorolni kell. Ha lehetőség van rá, akkor próbáljuk meg minimalizálni ezeket, és tartsuk a kockázatokat folyamatos felügyelet alatt, amely újabb kockázatok azonosításhoz vezet(het). Az ISO 31000-es szabvány [66] tartalmazza a kockázatmenedzsment alapelveit, folyamatát és annak felügyeletét (ld. 1. ábra).

DOI: 10.21791/IJEMS.2017.4.28.



1. ábra Az ISO 31000:2009 szabvány felépítése [38]

1.4. Kockázatmenedzsmenttel (is) foglalkozó szabványok és ajánlások

A felelős vezetők a bőség zavarával küzdenek, mert számos szabvány, ajánlás tárgyalja a vállalati biztonsági állapot eléréséhez szükséges feladatokat. Ezek a dokumentumok foglalkoznak kockázatmenedzsmenttel is.

A következő felsorolás nem a teljesség igényével készült. A szerző által fontosnak tartott és a kockázatmenedzsmentben használható szabványokat, ajánlásokat és modelleket tartalmazza. Szerepük és rövid leírásuk korábbi forrásokban megtalálhatók (ld. hivatkozások);

- MSZ ISO 14001 Környezetközpontú irányítási rendszerek. Követelmények és alkalmazási irányelvek [18, 59],
- MSZ 28001 (BS OHSAS 18001) A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR). Követelmények [18, 57, 58],
- MSZ EN ISO 9001 Minőségirányítási rendszerek. Követelmények [1, 17, 61],
- FMEA (Failure Mode and Effect Analysis) Hibamód- és hibahatás elemzés a minőségirányításban [4].

DOI: 10.21791/IJEMS.2017.4.28.

- BS 25999-1 Business Continuity Management, Code of Practice és BS 25999-2 Business Continuity Management, Specification - brit eredetű, üzletmenet folytonossággal foglalkozó szabványcsomag (ld. még ISO 22301)[18, 29, 30, 34],
- ALARP alapelv – As Low As Reasonable Practicable – a lehető legkisebb, még ésszerűen megvalósítható kockázati szint elérésére történő törekvés [16, 24],
- COSO (Comitte of Sponsoring Organisations of Treadway Comission) vállalati kockázat kezelő (Enterprise Risk Management) keretrendszer [18, 19, 23, 33],
- MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények [18, 64],
- ISO/IEC 27005 Information technology - Security techniques - Information security risk management [17, 47],
- CObIT 4.1. verzió (Control Objectives for Information and related Technology magyar változata - Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések) [18, 31],
- MSZ ISO/IEC 20000-1 Informatika. Szolgáltatásirányítás. 1. rész. Előírás [18, 62],
- MSZ ISO/IEC 20000-2 Informatika. Szolgáltatásirányítás. 2. rész: Alkalmazási útmutató [18, 63],
- ISO/IEC 15504 Information technology - Process assessment – többrészes szabványcsomag a folyamatok értékelési lehetőségeiről folyamatcélok és várható eredmények tekintetében [12, 14, 18, 40, 41, 42, 43],
- CRAMM modell (CCTA Risk Analysis and Management Method) – elsősorban információbiztonsági kockázatok elemzésére és kezelésére szolgáló modell [27],
- ISO/IEC 38500 – Corporate governance of information technology – keretrendszer az információs és kommunikációs technológiák vállalaton belüli irányításához [23, 51],
- SCOR – Supply Chain Operations Reference – modell, ellátási láncok működésére vonatkozó folyamatszervezési ajánlás [19, 67],
- CPFR - Collaborative Planning, Forecasting and Replenishment – folyamatmodell, amely az ellátási láncok tagjainak együttműködésén és az igények előrejelzésén alapul [19, 32],

1.5. 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 [35, 36, 37]. A hagyományos kockázati megfontolás (a bekövetkező kockázati tényezőből származó kár nagysága és a kockázati esemény valószínűsége) helyett, ill. mellett bevezették a „sebezhetőségek" fogalmát, amelyek 5 + 2 csoportba sorolhatók [3, 25]:

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),

DOI: 10.21791/IJEMS.2017.4.28.

6. belső vállalati szervezet (szervezet-folyamat összehangolatlansága),
7. önálló vállalatok hálózata (együttműködési zavarok).

2. Üzletmenet-folytonossági és katasztrófa-elhárítási tervek

2.1. Az üzletmenet-folytonosság és a katasztrófa-elhárítás fogalma és jelentősége

Nagyon alapos és megfontolt kockázatmenedzsment alkalmazása mellett is tudomásul kell vennünk, hogy 100 %-os biztonság nincs. Bármilyen kockázatmenedzsmentet is használ egy vállalat, hibák illetve előre nem látható események bekövetkezhetnek mindig, amelyek különböző negatív hatással lehetnek a vállalat működésére, eredményeire. Előfordulhatnak olyan (jellemzően nagyon ritkán bekövetkező) események is, amelyek hatására egy vállalat működőképessége rövidebb vagy hosszabb ideig leáll. Hosszabb idejű leállások a vállalatoknak anyagi veszteséget okoznak, amelyek egy szint felett visszafordíthatatlan károkat is jelenthetnek, és akár a vállalat csődjéhez vezethetnek. Az ilyen helyzeteket nevezzük a vállalat számára katasztrófa- vagy krízis-helyzeteknek.

Katasztrófahelyzet előállhat, ha egy vállalat egy vagy több fő üzleti tevékenységét bizonyos időn túl nem tudja végezni, vagyis bizonyos üzleti funkciókat biztosító folyamatai (ún. kritikus folyamatai) egy adott határidőnél hosszabb időre leállnak, nem vagy nem kellő mértékben működnek. A vállalat számára egy kritikus folyamat leállásának vagy nem megfelelő működésének a jellemző oka általában az adott folyamat valamely fontos erőforrásának vagy erőforrásainak (humán, pénzügyi, infrastrukturális, információs, stb…) kiesése vagy meghibásodása, vagy valamely kötelező input feltételének hiánya. (Ennek egy speciális esete, amikor valamely folyamat az informatikai erőforrások kiesése, a támogató informatika infrastruktúra hibája, nem megfelelő működése vagy megszűnése miatt áll le vagy nem működik megfelelően. Ekkor az informatikai infrastruktúra megfelelő működésének visszaállításakor az információtechnológia (IT) üzemmenet folytonosságról, vagy az IT katasztrófa utáni visszaállításról beszélünk. Ezek a tevékenységek az informatikai üzemeltetés eljárásrendjének részét képezik, a megfelelő módszerek megtalálhatóak az IT üzemeltetés – információbiztonsági - jó gyakorlatai között.)

Számtalan lehetséges külső és belső veszélyforrásra visszavezethetők a katasztrófa-helyzetek kialakulása.

Külső tényezők:

- környezeti tényezők (vihar, villámcsapás, árvíz, földrengés, …),
- balesetek (repülő, vonat, gépkocsi, veszélyes anyagok, …),
- közmű kimaradások (elektromos áram, telefon, ...),
- erőszakos cselekmények (polgári elégedetlenség, sztrájk, terrortámadás, rendszerbetörés, …).

Belső tényezők:

- infrastruktúra hibák (szerver, adattárház, …),

DOI: 10.21791/IJEMS.2017.4.28.

- balesetek (tűz, vízkár, elektromos hiba, …),
- rosszindulatú cselekmények (elégedetlen alkalmazott, vállalati szabotázs, …).

Ezekre mind megfelelő kockázatkezelési intézkedéssel felkészülni szinte lehetetlen, különösen azért is, mert ezek bekövetkezési valószínűsége sokszor nagyon kicsi. Ugyanakkor az esetleges, nagyon ritka bekövetkezés esetén a kár nagyon nagy, akár végzetes is lehet, tehát semmiképp sem szabad figyelmen kívül hagyni. A vállalatoknak tehát készülni kell az ún. katasztrófa helyzetekre. Ez nemcsak saját érdekükben elvárás, de több területen jogszabályi kötelezettség, továbbá számos nagyvállalat kötelezően elvárja ezt a beszállítóitól is.

Az ilyen katasztrófahelyzetekre való felkészülés módja az ún. „üzletmenet folytonossági tervek" és a „katasztrófa-elhárítási tervek" készítése, bevezetése, gyakorlása és szükség esetén alkalmazása.

Ahhoz, hogy ezeket tisztán láthassuk, először a fogalmakat szükséges definiálni:

- Katasztrófa-helyzet vagy súlyos vészhelyzet az, amikor az a fontos üzleti folyamat normális működésében olyan hosszú ideig fennakadás van, aminek hatására a vállalat számára helyreállíthatatlan, elviselhetetlen károk keletkezhetnek.
- Informatikai katasztrófa-helyzet vagy súlyos vészhelyzet az, amikor a támogató informatikai rendszer kiesése vagy hibás működése miatt a fontos üzleti folyamat normális működésében olyan hosszú ideig fennakadás van, aminek hatására a vállalat számára helyreállíthatatlan, elviselhetetlen károk keletkezhetnek.
- Üzletmenet-folytonossági terv (Business Continuity Plan, BCP). Azon intézkedések rendszerezett, tervezett együttese, amelyekkel a vállalat, a katasztrófa bekövetkezése után a lehető leghamarabb az üzleti folyamatok leglényegesebb elemeit újra működtetni tudja.
- Katasztrófa-elhárítási terv (Disaster Recovery Plan, DRP). Azon intézkedések rendszerezett, tervezett együttese, amelyekkel a vállalat, a katasztrófa bekövetkezése utáni szűkített üzleti folyamatok működésből az eredeti, teljes működést visszaállíthatja.
- Sebezhetőségi ablak. Az az időintervallum, ameddig a vállalat a fontos üzleti folyamatai leállását helyrehozhatatlan, elviselhetetlen következmények nélkül tolerálni képes.

2.2. Az üzletmenet-folytonosság és a katasztrófa-elhárítás működése

Az üzletmenet-folytonosság és katasztrófa-elhárítás (jobb név a katasztrófa utáni visszaállítás) működésére a katasztrófahelyzetek bekövetkezése után van szükség. Az előző fejezetben meghatározott definíciókból látszik, hogy más és más az üzletmenet-folytonosság fenntartásának és a katasztrófa utáni visszaállításnak a szerepe [7].

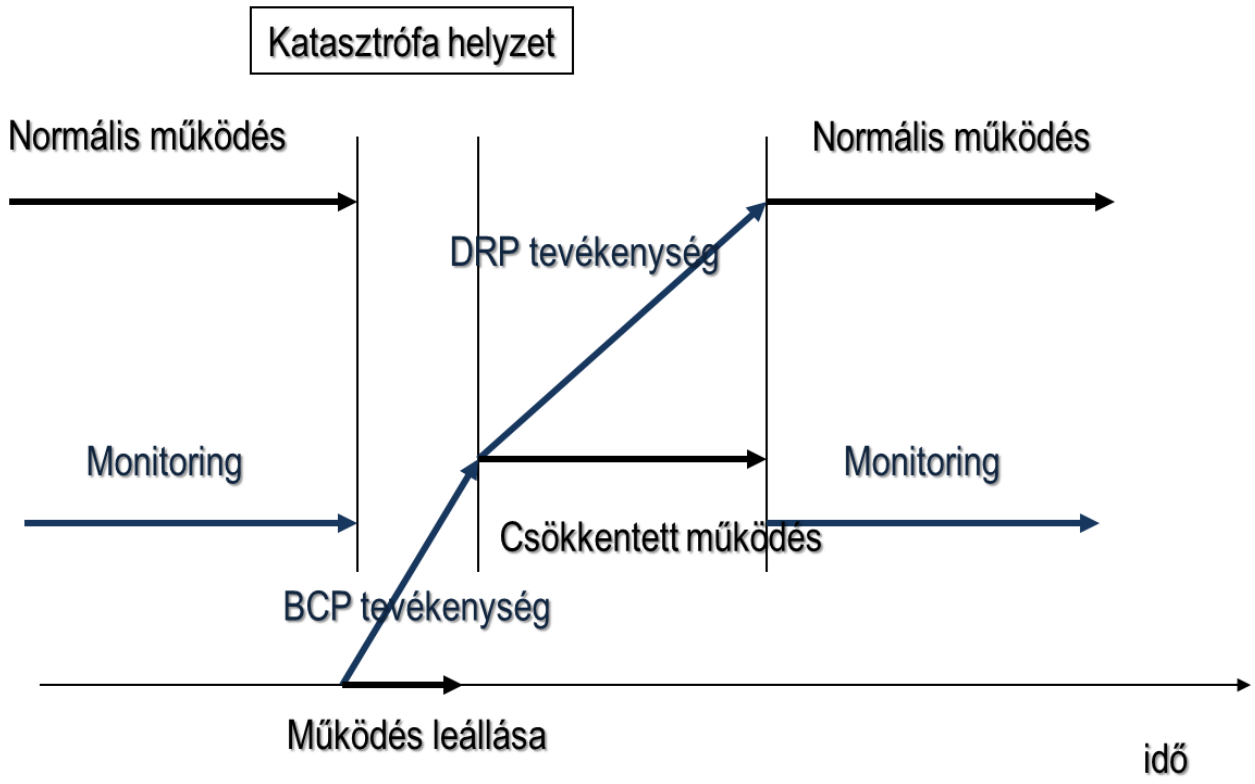
Az üzletmenet-folytonosságnak az elsődleges célja a vállalat veszteségének minimalizálása, a lehetséges csőd (vagy csőd-közeli állapot) elkerülése azáltal, hogy a vállalat fennmaradásához szükséges tevékenységeket, szolgáltatásokat – legalább egy szükséges minimum-szinten – a vállalat minél hamarább biztosítani tudja. Ha a vállalat egy alapvető létfontosságú tevékenysége ellehetetlenül, akkor annak minimális szinten való működését igyekezzen minél rövidebb időn (az ún. sérülékenységi ablakon) belül, akár tartalék eszközökkel, vagy erőforrás átcsoportosítással, vagy akár másféle alternatív tevékenységgel való kiváltással, de biztosítani.

DOI: 10.21791/IJEMS.2017.4.28.

A katasztrófa utáni helyreállítás célja az okozott károk felszámolása, és az eredeti normális működés teljes visszaállítása. Könnyen belátható, hogy ez a cél nem minden esetben oldható meg gyorsan, hiszen nincs mindig elegendő idő akár a hiba-okok elemzésére és megállapítására, akár a szükséges javítások vagy új beszerzések kivitelezésére. Ezért is szükséges a minimálisan szükséges folyamatos működéshez szükséges feltételeket az üzletmenet-folytonosság biztosítása tevékenységeken belül nagyon gyorsan biztosítani, majd utána a kellő időt rászánva kell a hibákat, a hiba-okokat meghatározni és a visszaállítás menetét megtervezni, majd azokat a katasztrófa utáni visszaállítás keretében végrehajtani.

Ezek a tevékenységek akkor hajthatók katasztrófa-helyzetben (vészhelyzetben) gyorsan és hatékonyan végre, hogyha az egyes lehetséges esetekre kidolgozott forgatókönyvek vannak, amelyeket az érintettek ismernek, kipróbáltak, megtanultak, azaz tudják használni. Ezeknek a terveknek a neve, megfelelve a tervezendő tevékenységeknek: Üzletmenet-folytonossági terv (BCP), illetve Katasztrófa-elhárítási terv (DRP).

Az üzletmenet-folytonosság és a katasztrófa-elhárítás működésének lépéseit 4 szakaszra bonthatjuk (2. ábra):



2. ábra: Üzletmenet-folytonosság és a katasztrófa-elhárítás működésének lépései

a. Felkészülési szakasz (a normál működés szakasza)

- a katasztrófa-helyzet bekövetkezése előtti szakasz,

DOI: 10.21791/IJEMS.2017.4.28.

- a vállalat folyamatainak normális működése,
- folyamatos monitoring tevékenységek,
- felkészülés a katasztrófa-helyzetre, „Felkészülési terv" alapján.

b. Válaszadási szakasz

- a katasztrófa-helyzet közvetlen bekövetkezése után a helyzet stabilizálásáig terjedő időszak,
- azon tevékenységek végrehajtása, amivel a vállalat eljuthat a minimális vagy csökkentett működés biztosításáig (BCP terv tevékenységei),
- a végrehajtás során alapvetően az ún. „Cselekvési terv" lépéseinek a betartásával.

c. Átmeneti (csökkentett) működés szakasza

- • minimális üzleti szolgáltatások működnek, a fő vállalati funkciók megvannak, de lehetséges, hogy csak csökkentett kapacitással és funkcionalitással. (rendkívüli üzemeltetés időszaka),
- • azon tevékenységek végrehajtása, amelyekkel a vállalat visszaállíthatja az eredeti működést (DRP tevékenységek),
- • a végrehajtás az ún. „visszatérési terv" lépéseinek a betartásával.

d. Normális működés (újból…)

- a vállalat folyamatainak normális, helyreállított működése,
- folyamatos monitoring tevékenységek.

A BCP és DRP tervekben meghatározott tevékenységek katasztrófa-helyzet bekövetkeztekor csak akkor hajthatók végre pontosan és szervezetten, hogyha azok egyrészt ismertek, kipróbáltak és működőképesek, továbbá az adott katasztrófa-helyzetben mindenki azonnal tudja, mi a tennivalója. Ehhez nem csak a konkrét tevékenységeket kell tudni, de megfelelő szervezés is szükséges, amelyeket az ún. Felkészülési terv, Cselekvési terv és Visszatérési terv is biztosítanak. Ezeknek a terveknek a fő feladatai (mintegy lépései) a következők:

Felkészülési terv

- hibák észlelése, elhárítása,
- kockázatok csökkentése (megelőző védelmi intézkedések),
- rendkívüli helyzet kezeléséhez szükséges feltételek biztosítása,
- munkatársak éberségének fenntartása (oktatás).

Cselekvési terv – átállás a rendkívüli működésre

- riadóterv,
- válságkezelési terv (válságstáb, rendkívüli feladatok és felelősségek),
- kommunikációs terv,
- kárfelmérési terv,
- mozgósítási terv (alternatív tevékenységek gyors elrendelése, elindítása, életbe léptetése).

Visszatérési terv

DOI: 10.21791/IJEMS.2017.4.28.

- tartalék infrastruktúra megtervezése, kialakítása lépéseinek megtervezése,
- szükséges erőforrások meglétének, beszerzésének megtervezése,
- biztonsági intézkedések kidolgozása az átálláshoz,
- átállás tevékenységeinek, végrehajtásának megtervezése.

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. Kiemelt feladat a felelős vezetők és a beosztott munkatársak folyamatos oktatása továbbképzése.

Az üzletmenet-folytonosság és katasztrófa-elhárítás elsősorban az információbiztonsággal foglalkozó szabványokban és ajánlásokban jelennek meg [7]. Az információbiztonsági és információtechnológiai megközelítés – ahogy ezt itt bemutattuk, – kiterjeszthető bármilyen más vállalati folyamat feltételeinek biztosítására, annak előírásszerű végrehajtására vagy zavar esetén normál működésének helyreállítására.

3. Folyamatmenedzsment alapjai

3.1. Folyamat definiciója

A folyamatot többféleképpen lehet definiálni. Az 1984-ben az Akadémiai Kiadó által megjelentetett Műszaki Lexikon 1. kötetében az alábbiakat olvashatjuk; „… valamely fizikai, kémiai, műszaki (technológiai), gazdasági v. biológiai rendszer egymással összefüggő jellemzőinek időfüggvénye.” [21; p. 872]

Kocsis József és Seregi Ferenc termelésirányítással foglalkozó Budapesti Műszaki Egyetemen, múlt században kiadott jegyzetükben már adott, korábban létrehozott (termelő) rendszer állapotváltozásait eredményező folyamatokat említenek. „Folyamaton… a rendszerben térben és időben lejátszódó célszerű tevékenységek meghatározott láncolatát értjük, amelyek az előre kitűzött cél megvalósítására irányulnak.” [15; p. 19]

Tenner és De Toro a vállalati technológiai és gazdasági (üzleti) folyamatok átalakításának menedzsmentjével foglalkozó könyvükben a fentieknél egy pontosabb, szakterületet jobban lehatároló meghatározást adtak meg. „A folyamat egy vagy több tevékenység, amely értéket növel úgy, hogy egy bemenetkészletet átalakít kimenetek készletévé (javakká vagy szolgáltatásokká) egy más személy (a vevő, ill. felhasználó) számára, emberek, módszerek és eszközök kombinációjával.” [26; p. 75]

3.2. Folyamatok alkotóelemei

A vállalatoknál zajló (üzleti) folyamatok megtervezéséhez és kialakításához a folyamat definiálása nem elég. A folyamatnak vannak alkotóelemei (feltételei, erőforrásai és eredményei):

- input (lehet információ, folyamatot kiváltó esemény, ill. valamilyen erőforrás),

DOI: 10.21791/IJEMS.2017.4.28.

- output (termék és / vagy szolgáltatás),
- tevékenység (ill. ezek láncolata; a folyamat tovább bontható folyamatelemekre, műveletekre),
- végrehajtásért felelős szervezeti egység vagy személy és a végrehajtó(k) akár folyamatelemenként is megadva,
- a folyamat végrehajtásához szükséges információkat hordozó elektronikus vagy papíralapú bizonylatok.
- adatok (külső és vállalati adatbázisok),
- A tevékenységek, ill. a folyamatelemek végrehajtásának logikai (párhuzamos vagy szekvenciális) rendje.

3.3. Folyamatok csoportosítása

A vállalatnál zajló folyamatokat leginkább a felhasznált erőforrások szerint csoportosíthatjuk;

a) anyagi folyamatok (anyagi erőforrások fizikai és kémiai tulajdonságainak, valamint térbeli pozíciójuk megváltozása, megváltoztatása).

b) irányítási folyamatok (gyakorlatilag információfeldolgozás és továbbítás, itt elsősorban a folyamat végrehajtásához szükséges információk átadása és átalakítása megy végbe, szorosan kapcsolódva az anyagi folyamatokhoz).

c) értékfolyamatok (a vállalat és környezete határán…).

Kategóriákba sorolhatjuk a folyamatokat a vállalati működésben betöltött szerepük alapján is;

- alap-, fő vagy értékteremtő folyamatok (ahol a vállalat inputokból outputokat állít elő külső érintettek, elsősorban vevők számára; termelés, logisztika, értékesítés, marketing, termékfejlesztés, stb.),
- támogató- vagy mellékfolyamatok (amelyek elsősorban az értékteremtő folyamatokat szolgálják ki; beszerzés, technológiai fejlesztés, emberi erőforrás biztosítása, információtechnológia, kontrolling),
- irányítási (vezetési) folyamatok (meghatározzák a többi folyamat működését; stratégiai tervezés, különböző irányítási rendszerek).

3.4. Folyamatok értékelése

Az üzleti folyamatok javítása, fejlesztése esetén sem kerülhetjük meg a csoportosítást. A folyamatok végrehajtásához szükséges idők is csoportokba sorolhatók [26; pp. 127-129]:

- RVA - Real Value Added; valóságos értéket termelő folyamatelemek végrehajtási ideje (pl. termékfejlesztés, gyártás, csomagolás, anyagbeszerzés, kiszállítás, szerelés, szervízszolgáltatás),
- BVA = Business Value Added; üzleti hozzáadott értéket termelő elemek ideje (pl. ütemezés, számlázás, munkaerő felvétel, könyvvizsgálat, értékesítés, marketing, nyilvántartások vezetése),
- NVA = Non-Value Added; hozzáadott értéket nem termelő elemek ideje (pl. várakozások, újra-megmunkálás, raktározás, felesleges vizsgálatok, túlzott adminisztrálás).

Az idők típusainak megállapításával és megmérésével meghatározható a hatékonyság (Tn).

DOI: 10.21791/IJEMS.2017.4.28.

$$T_n = RVA / T \qquad (1)$$

ahol

$$T = RVA + BVA + NVA \qquad (2)$$

Az egyszerű képlet alapján belátható, hogy a különböző időknél más és más irányelvet kell követni.

Küszöböljünk ki minden, hozzáadott értéket nem termelő (NVA) tevékenységet!

Minimalizáljuk az üzleti hozzáadott értéket termelő (BVA) tevékenységeket!

Optimalizáljuk a valóságos hozzáadott értéket termelő (RVA) tevékenységeket!

Az előzőek miatt is fontos vállalati feladat a folyamatok mérése és értékelése. A kvalitatív (nem vagy nehezen mérhető) és kvantitatív (jól mérhető, számszerűsíthető) KPI-k (Key Performance Indicator – Kulcs Teljesítmény Mutató) megadásával a folyamatok jól kézben tarthatók.

(A kvalitatív KPI lehet például vevői és dolgozói elégedettség, ugyanakkor a kvantitatívaknál több lehetőségünk van (pl. átfutási idő, selejt gyakorisága, beszállítói hibaszázalék, szállítási késések, reklamációk száma, kontrolling terv és tény adatai, költség adatok, kapacitáskihasználás, egy dolgozóra eső kibocsájtás), de pontos mérésük idő- és munkaigényesebb lehet.

3.5. Folyamatok kialakítása

A folyamatok tervezéséhez, elemzéséhez és kezeléséhez érdemes valamilyen folyamat hierarchiát kialakítani [11]. (Erre nem lehet általános szabályt megadni, mivel a vállalat különböző területein zajló folyamatok strukturáltságukban jelentősen eltérhetnek.);

- folyamat szint,
- részfolyamat szint,
- tevékenység szint (folyamat elem),
- művelet szint,
- mozdulat szint.

A folyamatok tervezése és működtetése a hagyományos (lineáris, funkcionális, törzsegységi, divizionális és mátrix szervezeti) formák változatlan megtartása mellett nehéz. A folyamatmenedzsment új szereplőket is igényel.

A folyamat-felelős ismeri a folyamatokat alkotó részfolyamatokat és a folyamat céljait. Ellenőrzi a folyamat teljesítmény mutatóit. Koordinálja a folyamat végrehajtásához szükséges erőforrásokat, kapcsolatot tart a többi folyamatfelelőssel és a vállalat hagyományos szervezeti vezetőivel. Fejlesztési javaslatokat fogalmaz meg a folyamat javítására.

DOI: 10.21791/IJEMS.2017.4.28.

A folyamat szponzora általában egy vállalatot (erőforrások, termék, piac, technológia) jól ismerő felső vezető, aki képes a folyamatorientált szemléletet és a hagyományos szervezeti működést szintetizálni. Hatalma, szervezetben betöltött szerepe segít elfogadtatni a folyamatorientált irányítást.

A (funkcionális) szervezeti egységek vezetői elvégzik (elvégeztetik) a folyamat-felelős által kért részfeladatokat. Teljesítményüket előre kidolgozott teljesítmény-mutatószám rendszerrel mérik.

Az üzleti folyamatokra jó példa lehet a vállalatirányítási információs rendszerekben (ERP) is modellezett értékesítés folyamata;

- ajánlatkérés fogadása,
- ajánlatadás,
- megrendelés fogadása,
- megrendelés visszaigazolása (kapcsolódó gyártási és beszerzési folyamatok elindítása),
- áru készáru raktárba helyezése,
- vevő kiértesítése,
- kivételezési jegy, szállítólevél kiállítása,
- visszaérkező szállítólevél alapján a számla elkészítése,
- számla ellenértékének fogadása,
- megrendelés lezárása.

3.6. Folyamatmenedzsment feladatai

A folyamatmenedzsment biztosítja a kitűzött vállalati célok teljesítését az üzleti és technológia folyamatok állandó mérésével, elemzésével és javításával. Figyelembe veszi és közvetíti a végrehajtók felé a vállalati tervekben bekövetkező változásokat. Gyakorlatilag a folyamatelemek végrehajtását jelentő szakmai (funkcionális) feladatok szétosztását és egy felelősségi rendszer kialakítását jelenti. Javít(hat)ja a vállalat napi operatív működését.

A folyamat menedzsment feladatai:

- új folyamatok és ebben a folyamat-hierarchia megtervezése,
- folyamatokhoz illő szervezet, hatás- és felelősségi körök kialakítása.
- teljesítménymutatók megfogalmazása, mérési módszereik kidolgozása,
- működő folyamatok elemzése, teljesítmény mérése,
- folyamat-szabályozás (kontrolling) bevezetése és működtetése,

4. Folyamatbiztonság és a vállalati működés biztonsága

Napjainkban a vállalatok üzletmenet-folytonosságát növekvő számú és egyre nehezebben átlátható veszély fenyegeti. Minden üzleti folyamatot (pénzügyi, működési, stratégiai és projekt-) és kapcsolódó

DOI: 10.21791/IJEMS.2017.4.28.

erőforrást (ember, IT, berendezések, infrastruktúra, energia, üzleti partnerek) kockázatfelmérésnek és -kezelésnek kell(ene) alávetni [38, 39].

A folyamat-centrikus vállalati működés múlt századi elterjedését többek között Porter értéklánc modellje is megalapozta [16, 22].

A nyereségesség mellett legalább olyan fontos a biztonságos – környezet által is elfogadott – működés valamint az üzletment folytonosság információtechnológián túl történő kiterjesztése.

A kockázatfelmérés és -kezelés is a 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 működése is megfelelő stabil, azaz „biztonsági állapotba" kerülhet.

A vállalat működés biztonsága 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 kockázatfelmérésen és az ez alapján meghatározott védelmi intézkedéseken alapszik.

5. Folyamatok erőforrás-alapú kockázatkezelése

A folyamatcentrikus, ill. folyamatmenedzsmentet alkalmazó vállalatok a folyamatok modellezésére folyamat modelleket kezelő szoftvereket alkalmaznak. Itt a folyamatok szöveges leírása mellett ún. „folyamatrácsok" is megjelennek. Ezek olyan táblázatok, amelyekben részfolyamatok megnevezése és sorrendje mellett megtalálhatók a végrehajtó szervezeti egységek, a folyamat felelőse, és a végrehajtáshoz szükséges információk és információhordozók, a részfolyamatok esetleges további bontása [11].

Projektmenedzsmentben is gyakran használt RACI mátrix a folyamat elemek (tevékenységek) emberi erőforrás-szükségletét hivatott tisztázni. A folyamatelemeknél különböző szerepköröket definiálunk, amelyekhez szereplőket kell jelölni a végrehajtás előtt, úgy hogy ne az emberi erőforrás legyen a szűk keresztmetszet és a további folyamat elemek is végrehajthatók legyenek [65].

Az üzleti folyamatoknál is kialakítható szerepkörök a következők:

R - responsible vagy felelős, aktív szereplő, végrehajtó, akár több személy is lehet egyszerre…,

A – accountable vagy elszámoltatható, az igazi irányító, aki a végrehajtásért ténylegesen felel, általában egy személyben (!)…,

C – consulted vagy konzultáló, aki nincs a folyamat elem (tevékenység) esetében döntési helyzetben, tájékoztatni szükséges és véleményét meg kell hallgatni a folyamat-elem végrehajtása előtt és után is,

DOI: 10.21791/IJEMS.2017.4.28.

I – informed vagy informálandó, érintett a folyamat-elem eredményében, tájékoztatni feltétlenül szükséges…

A RACI mátrix további funkciókkal is kiegészíthető, de ezek kezelése a szakirodalomban nem egységes. Felvehető a támogatói (support - hozzájárul a felelős munkájához, bizonyos részfeladatokat ő végez) és a kihagyandó (out of the loop – aki nincs benne a folyamatban (projektben), nem kell sem bevonni, sem egyeztetni vele) szerepkör is.

A táblázatok könnyen kiegészíthetők olyan további oszlopokkal, amelyekben a (rész)folyamatok végrehajtásához szükséges erőforrások rendelkezésre állásának „kockázati szintjét" adjuk meg, becslésen alapuló, 3-as osztályozással (alacsony, közepes, magas). Mélyebb értékelésük a nagyszámú folyamat és részfolyamat valamint a folyamatok különbözősége miatt általában nehézkes.

Az erőforrások kockázatalapú vizsgálata azért is indokolt, mert a folyamat-menedzsmentet támogató alkalmazások, szoftverek erőforrásigényt nyilvántarthatnak, de az anyagszükséglet- és gyártási erőforrás tervezésben (MRP I-II.) megszokott rendelkezésre állást, ill. diszpozíciós szükségletszámítást általában már nem végzik el. Az MRP-t alkalmazó vállalatirányítási információs rendszerek (ERP) folyamatorientáltak ugyan, de termékek anyag- és kapacitásszükségletét vizsgálják csak [8]. Egy üzleti vagy termelési folyamat végrehajtása azonban más jellegű erőforrások hiánya miatt is megakadhat. Az erőforrások csoportokba sorolhatók;

- anyag,
- munkaerő,
- információ,
- pénzügyi forrás,
- infrastrukturális erőforrások (pl. energia, gépi kapacitás).

A folyamat elem végrehajtásához szükséges erőforrás mennyiség arányos is lehet a folyamat outputtal (pl. alapanyag), de elképzelhető, hogy az csak a folyamat elindítástól függ (pl. információ).

A folyamat-kockázatok legalább évente egyszeri felülvizsgálata javasolt. Amennyiben egy részfolyamat esetében van egy magas kockázatú erőforráscsoport, vagy legalább kettő olyan, amely közepes kockázatot hordoz és várhatóan nem fog elfogadható módon rendelkezésre állni; akkor indokolt a kockázatkezelésnél és üzletmenet-folytonosságnál a már említett módon helyettesítő, vagy alternatív folyamatot / folyamatokat kialakítani. Ez természetesen nem jelenti azt, hogy a helyettesítő folyamat költségben, átfutási időben és minőségben teljesen megfelel az eredeti folyamatnak.

A helyettesítésnél is alakítsunk ki hierarchiát!

Váltsuk ki, ill. helyettesítsük a kockázatos erőforrás(oka)t! (Kockázatos beszállítók esetén a gyártók több forrásból is be tudják szerezni ugyanazt az elemet, alkatrészt…) Ha ez nem megoldható, dolgozzunk ki új tevékenységeket, esetleg új (rész)folyamatokat!

Példaként hozható fel a termelési folyamatok zavarai, ill. gyártókapacitások túlterhelése, kiesése esetén hagyományos „kockázatkezelési" eljárás, amely gyakorlatilag a lehetőségek számbavételét és rangsorolását jelenti;

DOI: 10.21791/IJEMS.2017.4.28.

1. a gyártási feladatok végrehajtása más technológiai lépésekkel, ún. alternatív technológia választása, ami várhatóan drágább és/vagy lassabb, mint az eredeti…,
2. lehetőség van az ún. időalapok növelésére (túlóra v. további műszakok elrendelése),
3. gyártás kihelyezése megfelelő erőforrással bíró külső partnerhez (kooperáció),
4. konstrukciós változtatás (a termék áttervezése),
5. kapacitásbővítés (termelő eszköz beszerzése és/vagy munkaerő felvétel).

A folyamatokhoz, folyamatelemekhez rendelt erőforrások egyszerre több folyamathoz is szükségesek lehetnek. Elégséges lehet a folyamatok kockázatkezelésére a folyamatelemek és a hozzájuk szükséges erőforrások egymáshoz rendelése után az erőforrások időbeli, mennyiségi és minőségi rendelkezésre állását vizsgáljuk, elemezzük.

Összefoglalás

A kockázat- és folyamatmenedzsment összekapcsolható. A folyamatorientált szervezetek üzleti folyamataik tervezése, végrehajtása és ellenőrzése során figyelmet fordítanak a különböző kockázatok megállapítására és kezelésére. Ez sok esetben nem tudatos, sokszor vállalati hagyományokon és üzleti tapasztalatokon alapszik. A két területnek eltérő módszertani háttere van (ld. hivatkozások), amelynek integrálása még várat magára. A dokumentált vállalati gyakorlat kialakítása és az esettanulmányokon (is) alapuló módszertani vizsgálata (szabványok, módszertanok alkalmazhatósága) számos alkalmazott kutatási kérdést vet fel.

A vállalat üzleti termelési folyamatainak végrehajtásához, a vállalati outputok kibocsájtásához az erőforrások rendelkezésre állása szükséges a kellő időben és helyen. Bármilyen okból bekövetkező hiányuk, nem elégséges mennyiségük vagy nem megfelelő minőségük üzleti kockázatot jelent és a vállalat eredményességének romlásához vezet. A folyamatmenedzsmentben a kockázatok csökkentésére alkalmazható lehet két másik menedzsment területen alkalmazott eszköz is;

A gyártási erőforrás tervezésnél alkalmazott (Manufacturing Resources Planning – MRP II.) kapacitásokra és anyagi erőforrásokra alkalmazott erőforrás-termék (mátrix) kapcsolat és az ehhez kapcsolható lineáris programozás. Az üzleti folyamatoknál termékek helyett folyamatelemeket adhatunk meg és az erőforrások köre is jelentősen bővül.

Információbiztonság és információtechnológiai rendszerek üzemeltetése területén alkalmazott és nemzetközi szabványokkal támogatott üzletmenet-folytonosság menedzsment (Business Continuity Management – BCM) kiterjesztése segíthet a helyettesítő folyamat-erőforrások előrelátó meghatározásában és zavar esetén az eredeti folyamat helyreállítási idejének becslésében.

Hivatkozások

[1] Avanesov, Evgeny: Risk Management in ISO 9000 Series Standards. International conference on Risk Assessment and Management, 24-25. November 2009, Geneva.

DOI: 10.21791/IJEMS.2017.4.28.

www.fr.com/files/uploads/attachments/RISC/Report_Avanesov.pdf (letöltés dátuma: 2013.10.21.)

[2] Balogh Albert: Kockázatmenedzsment és kockázatértékelés. Magyar Minőség XX. évf. 3. szám, 2011. március pp.6-14.

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

[4] Czeglédi László: Minőségmenedzsment, FMEA (6.3.11-es alfejezet). Tankönyvtár. Eszterházy Károly Főiskola, 2011. www.tankonyvtar.hu/hu/tartalom/tamop425/0005_42_minosegmenedzsment_scorm_06/6311_fmea.html (letöltés dátuma: 2015. 11.06.)

[5] Farkas Szilveszter – Szabó József: A vállalati kockázatkezelés kézikönyve. Dialóg Campus Kiadó, Budapest – Pécs, 2005.

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

[7] Fekete István: Folyamat alapú működési kockázatfelmérés – kockázatelemzés alapú belső ellenőrzés. Egészségügyi Szemle 2009/6. szám pp. 5-10.

[8] Homonnay Gábor: Alkalmazási rendszerek. Műszaki Könyvkiadó, Budapest. 2003.

[9] 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.

[10] Horváth Zsolt: A kockázatkezelés alkalmazási területei. Magyar Minőség XX. évf. 3. szám, 2011. március pp.15-25.

[11] IFUA Horváth & Partners: Folyamatmenedzsment a gyakorlatban. IFUA Horváth & Partners Vezetési és informatikai Tanácsadó Kft., 2006.

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

[13] Iványos János (szerk; Trusted Business Partners Kft.): Kockázatkezelési Kézikönyv (Irányítási forgatókönyvek alkalmazása az integrált vállalati kockázatkezelés megvalósítására). v. 2.1, 2014.

[14] Iványos, János – Roóz, József – Messnarz, Richard: Governance Capability Assessment. Using ISO/IEC 15504 for Internal Finacial Controls and IT management. Proceedings of the MONTIFIC Project at the Conference of "The Current Financial Crisis and Competences to Address Problems on the European Market". Budapest Business School together with European Qualification and Certification Association, Budapest, 30 September - 1 October 2010, pp.17-47. http://training.ia-manager.org/file.php/1/The_MONTIFIC_Book.pdf#! (letöltés dátuma: 2014. január 10.)

[15] Kocsis József - Seregi Ferenc: Termelésirányítás I. (Alapelvek és alapszámítások) Budapesti Műszaki Egyetem, Gépészmérnöki Kar - egyetemi jegyzet, Tankönyvkiadó, Budapest, 1987.

DOI: 10.21791/IJEMS.2017.4.28.

[16] Dombora Sándor - Michelberger Pál: Információbiztonság szerepe az üzleti folyamatokban.International Journal of Engineering and Management Sciences, Műszaki és Menedzsment Tudományi Közlemények, Debreceni Egyetem 1:(1) p. &. 11 p. (2016)

[17] Michelberger, Pál: Risk Management for Business Trust. In: Management, Enterprise and Benchmarking in the 21st Century. 413 p. Budapest: Óbudai Egyetem Keleti Károly Gazdasági Kar, 2014. (szerk. Michelberger Pál) pp. 401-413.

[18] Michelberger Pál: Vállalatbiztonság. in „Vállalkozásfejlesztés a XXI. században III." 2013. Óbudai Egyetem, Keleti Károly Gazdasági Kar (szerk. Nagy Imre Zoltán), pp. 35-47.

[19] Michelberger Pál - Lábodi Csaba: Vállalati információbiztonság szervezése. in „Vállalkozásfejlesztés a XXI. században II." 2012. Óbudai Egyetem, Keleti Károly Gazdasági Kar, (szerk. Nagy Imre Zoltán), pp. 241-302.

[20] Nordal, Y. Ayse B.: Modelling Risks – Limitations anf Challenges. XII. International May Conference on Strategic Management - IMKSM2016, May 28 – 30, 2016, Bor, Serbia. pp.11-24.

[21] Polinszky Károly (főszerk.): Műszaki Lexikon. 1. kötet. Akadémiai Kiadó, Budapest, 1984.

[22] Porter, Michael, E: Versenystratégia. Akadémiai Kiadó, 2006.

[23] 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.

[24] Redmill, Felix: ALARP Explored. University of Newcastle upon Tyne: Computing Science, 2010. Computing Science, Technical Report Series, No. CS-TR-1197 http://www.scsc.org.uk/pubs/Alarp%20explored.pdf (letöltés dátuma: 2015.12.19)

[25] 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.

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

[27] Yazar, Zeki: A Qualitative Risk Analysis and Management Tool - CRAMM. SANS Institute (InfoSec Reading Room), 2002. www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 (letöltés dátuma: 2016.11.21.)

[28] AS/NZS 4360:2004 Risk Management. Australian / New Zealand Standard

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

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

[31] CObIT 4.1. verzió (magyar változat - Control Objectives for Information and related Technology - Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések) IT Governance

DOI: 10.21791/IJEMS.2017.4.28.

Institute, USA, 2007. www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf (letöltés dátuma: 2013. 03.29.)

[32] 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.)

[33] 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.)

[34] ISO 22301:2012; Societal security - Business continuity management systems – Requirements

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

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

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

[38] MSZ ISO 31000:2015. Kockázatfelmérés és -kezelés. Alap- és irányelvek

[39] ISO 31010:2009. Risk management – Risk Assessment Techniques

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

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

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

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

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

[45] ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls

[46] ISO/IEC 27003:2010. Information technology - Security techniques - Information security management system implementation guidance

[47] ISO/IEC 27005:2011; Information technology - Security techniques - Information security risk management

[48] ISO/IEC 27010:2012. Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications

DOI: 10.21791/IJEMS.2017.4.28.

[49] ISO/IEC 27011:2008. Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

[50] ISO/IEC 33002:2015. Information technology - Process assessment - Requirements for performing process assessment

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

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

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

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

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

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

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

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

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

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

[61] MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények

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

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

[64] MSZ ISO/IEC 27001:2014. Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

[65] Project Management Institute: Projektmenedzsment útmutató (Project Management Body of Knowledge - PMBOK Guide). Akadémiai Kiadó, 2006

[66] RIMS Executive Report. The Risk Perspective (An Overview of Widely Used Risk Management Standards and Guidelines). Risk and Insurance Management Society Inc., 2011. www.rims.org/resources/ERM/Documents/RIMS Executive Report on Widely Used Standards and Guidelines March 2010.pdf (letöltés dátuma: 2013.10.24.)

DOI: 10.21791/IJEMS.2017.4.28.

[67] 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.)