DOI: https://doi.org/10.12700/btsz.2025.7.1.25

INTEGRATED ENTERPRISE RISK MANAGEMENT - OPPORTUNITIES AND THREATS IN THE LIGHT OF STANDARDS AND RECOMMENDATIONS

INTEGRÁLT VÁLLALATI KOCKÁZATMENEDZSMENT - LEHETŐSÉGEK ÉS VESZÉLYEK A SZABVÁNYOK ÉS AJÁNLÁSOK TÜKRÉBEN

MICHELBERGER Pál[1]

Abstract

What are the problems of an integrated corporate risk management system? The study draws attention to some of the pitfalls of the integrated corporate risk management system affecting the implementation and effectiveness of business- and technological processes, and to the possibilities of its design and operation. The methodological separation of the specific risk management of functional enterprise sub-areas due to tradition could be a serious threats. Corporate management cannot afford to deal with the effects of the resulting risk events only in detail. Risk management based on an unified basis must now be present in all areas of the operation of companies. One of the aims of the study was to review some of the major Hungarian publications related to integrated risk management in the past two decades. The bibliographical data of more than a dozen easily accessible, relevant journal articles from Hungarian authors can be found in the bibliography.

Keywords

risk level, process risk, FMEA, ISO 31000, ISO/IEC 27005

Absztrakt

Milyen problémák lehetnek egy integrált vállalati kockázatmenedzsment rendszerrel kapcsolatban? A tanulmány felhívja a figyelmet az üzleti- és technológiai folyamatok végrehajtását és eredményességét befolyásoló teljeskörű és integrált vállalati kockázatmenedzsment rendszer néhány buktatójára és kialakításának és működtetésének lehetőségeire. Komoly veszély a funkcionális vállalati részterületek sajátos kockázatértékelésének és -kezelésének hagyományok miatti módszertani elkülönülése. A vállalati vezetés nem engedheti meg magának, hogy a bekövetkező kockázati események hatásai csak részleteiben legyenek kezelve. Az egységes alapokon nyugvó kockázatmenedzsmentnek ma már a cégek működésének minden területén meg kell(ene) jelennie. A tanulmány egyik célja volt az elmúlt két évtized néhány jelentős, integrált kockázatmenedzsmenthez köthető, magyarnyelvű publikációjának áttekintése is. Az irodalomjegyzékben több mint egy tucat, könnyen elérhető, releváns, magyar szerzőktől származó folyóiratcikk bibliográfiai adatai találhatók meg.

Kulcsszavak

kockázati szint, folyamatkockázat, FMEA, ISO 31000, ISO/IEC 27005

[1] michelberger.pal@bgk.uni-obuda.hu | ORCID: 0000-0001-5752-0224 | professor, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ELŐZMÉNYEK

Frank H. Knight az Egyesült Államokban 1921-ben már elkülönítette a „kockázat" és a „bizonytalanság" fogalmát és talán elsőként foglalkozott művében az üzleti kockázatok jelentőségével [12] [21]. Martin Kenneth Starr 1972-ben írt átfogó termelésmenedzsment témájú könyvében még külön-külön foglalkozik a minőség-ellenőrzés és a beruházások (pénzügyi) kockázataival [19]. A kockázatelemzés tudományos megalapozása az 1980-as években volt megfigyelhető [18] [3]. Ennek folytatása volt a kockázatmenedzsment követelményeket leíró szabványok és ajánlások, illetve a kockázatelemzés, -értékelés és -kezelés gyakorlatát, módszertani hátterét bemutató szakmai dokumentumok megjelenése [41], amelyek napjainkban is folyamatosan fejlődnek, bővülnek. A később említett kockázatmenedzsment szabványok közül a COSO ERM ajánlás [36] [38] már 2004-ben is megvolt. Az ISO/IEC 31000-es szabvány korábbi változata már 2009-ben megjelent. Jelenlegi formájában 2018-ban adta ki a nemzetközi szabványügyi testület és az iso.org tanúsága szerint már fejlesztik az ISO/WD 31000-es új változatot is.

A holisztikus megközelítést, az egész vállalatra vonatkozó integrált kockázatmenedzsmentet a vezetők és az üzleti partnerek egyre jobban igénylik. A vállalatok sokszor ezért látszatintézkedéseket tesznek. A kockázatelemzéssel és -értékeléssel megbízott szakmai kör kialakít egy formális, általában írott szabályrendszert a tulajdonosi vagy üzleti partneri elvárások alapján. A kockázatkezelési szabályzat elkészül, de az láthatóan nem kényszeríti a szervezetet működése megváltoztatására, javítására. Általában kevesen és elszigetelten használják. Nincs meg a folyamatos felülvizsgálat [6]. A kockázatmenedzsment módszerek pedig nem illeszkednek a vállalati stratégiákhoz [11]. A kockázatok számbavétele, elemzése és értékelése nem folyamatos, hanem kampányszerű vagy periodikus, esetleg egy-egy nagyobb kockázati esemény bekövetkezése utáni pótcselekvés.

Vannak olyan gazdálkodási területek, ahol korábban is volt erős kockázatmenedzsment szabályozás (pl. vállalati pénzügyek, vagyonbiztosítások, minőségirányítás). Ezek azonban inkább elszigetelődnek, mintsem a saját szintjükre emelik fel a többi funkcionális szervezeti egység, vagy üzleti és technológiai folyamat kockázatmenedzsmentjét. Az sem segít, hogy számtalan kockázatmenedzsment szabvány és ajánlás közül lehet választani és a bőség zavara módszertani segédanyagoknál is jelentkezik. Mielőtt az integráció útjára lépünk, tehát választani kell a lehetőségek közül és ez változásra / változtatásra, valamint tanulásra kényszeríthet sok szervezeti egységet. A kockázatmenedzsment irányítási rendszert pedig a bevezetés után is folyamatosan tesztelni, használni és fejleszteni szükséges.

EGYSÉGES VÁLLALATI KOCKÁZATMENEDZSMENT RENDSZER HIÁNYA

A kockázatmenedzsment vállalati keretének kialakításához és magának a kockázatelemzéshez és -kezeléshez sok támogatást szabvány és ajánlás elérhető [10]. A most felsorolásra kerülő dokumentumok nem felelnek meg a teljesség igényének és inkább csak azok kerültek ide, amelynek fő profilja a funkcionális vagy a teljes szervezeti működést átfogó kockázat-menedzsment.

- ISO/IEC 310XX-es szabványcsalád [24] [28],
- ISO/IEC 27005-ös információbiztonsági kockázatok kezelésére készült útmutató [23],

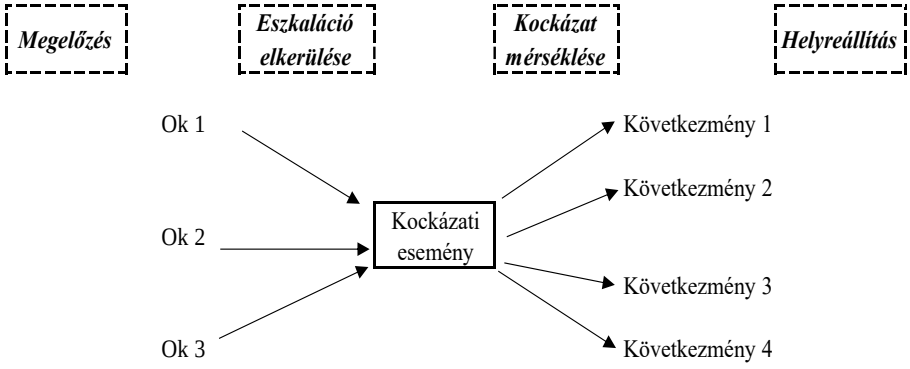
- ALARP alapelv (As Low As Reasonable Practicable a lehető legkisebb, még észszerűen megvalósítható kockázati szint elérésére történő törekvés) [39],
- COSO ERM (Comitte of Sponsoring Organisations of Treadway Comission) vállalati kockázatkezelő (Enterprise Risk Management) keretrendszer, amely a Governance-Risk-Complience (GRC) modellen alapszik [2] [16] [20] [36] [38],
- MIL-STD 882E amerikai katonai szabvány a kockázatmenedzsmentre [34],
- CRAMM modell (CCTA Risk Analysis and Management Method) elsősorban információbiztonsági kockázatok elemzésére és kezelésére szolgáló modell [14] [22],
- FMEA (Failure Mode and Effect Analysis) Hibamód és hibahatás elemzés elsősorban a minőségirányításban [13] [35].

Ezek általában nem kötelező jelleggel szabják meg, hogy milyen kockázatelemzési és -kezelési módszertani hátteret használ egy vállalat. Így azok gyakran nem integráltak és nem egységesek (ráadásul a kockázat értékelés eltérő mérési skálákon történik…).

Az integrált kockázatkezelés szükségességét az 1. ábra alapján is igazolhatjuk. A kockázatkezelés jellemző szakmai területeinek (következményeinek) egy lehetséges felosztása a következő [5]:

- pénzügyi és finanszírozási kockázatok (pl. árfolyamváltozás, alapanyagárak, vevők likviditásának romlása, jegybanki alapkamat változás),
- stratégiai kockázatok (pl. szabályozási vagy politikai környezet megváltozása, vevők ás beszállítók hosszútávú döntései, szervezet külső megítélése),
- működési kockázatok (humán erőforrás, Információs és kommunikációs technológia, termelőeszközök működőképessége),
- projektkockázatok (beruházások és innovációk kockázatai).

Számos ok hozhatja el adott kockázati esemény bekövetkezését, ami azután több szakmai területen is egymást erősítő következményt eredményez.



1. Ábra: Kockázati esemény okai és „nem kívánt" következményei („bow tie" diagram ISO/IEC 31010 szabvány alapján) [24]

Példaként vegyük kockázati eseménynek az elkészült és leszállított termékre vonatkozó számla kibocsátás megakadását. Ennek lehet információtechnológiai oka (a számlázó program nem működik, nem tud a vevő és az adóhatóság által elfogadott, sorszámozott, megfelelő adat-tartalmú bizonylatot előállítani. Ok lehet még a nem megfelelő teljesítés (a

vevő mennyiségi és minőségi átvétele hibát és / vagy hiányosságot észlelt). Elképzelhető okként egy kalkulációs probléma, amely a számla végösszegét kérdőjelezi meg. A következmények több vállalati területet is érinthetnek; romlik a cég reputációja és csökken a vevői bizalom, elmaradó vagy késő bevétel likviditási problémákat okoz. A számlázó program verzió-váltása után a becsült kockázati szint nőhet.

A szervezeten belüli, egy-egy területet izoláltan érintő kockázat elemzés, -értékelés és -kezelés nem fogja a kívánt mértékben emelni a vállalat biztonsági szintjét [9].

Az ISO/IEC 27005-ös szabvány [23] „A" melléklete például számos mintapéldát ad kvalitatív kockázatelemzéshez (a valószínűségek és a kockázati következmények, valamint a kockázatkezelést eldöntő kockázat nagyságának osztályba sorolásához). De ugyanitt találhatunk olyan értékelési mintákat (szempontokat), amelyek a kvantitatív elemzés irányába mutatnak (pl. kockázati események bekövetkezésének várható gyakorisága vagy az angol fontban (£), sávosan kifejezett kockázati következmények, károk osztályai.

Az 1. táblázat az ISO/IEC 27005-ös szabvány mellékletében javasolt (!) kvalitatív kockázati szint mátrixot mutatja. Öt valószínűségi szintből és a lehetséges öt következményből öt kockázati szint jöhet ki (nagyon magas – very high, magas – high, közepes – medium, alacsony – low és nagyon alacsony – very low…).

	Következmény				
Valószínűség	Katasztrófális	Kritikus	Súlyos	Jelentős	Mérsékelt
Majdnem biztos	Nagyon magas	Nagyon magas	Magas	Magas	Közepes
Nagyon valószínű	Nagyon magas	Magas	Magas	Közepes	Alacsony
Valószínű	Magas	Magas	Közepes	Alacsony	Alacsony
Kissé valószínűtlen	Közepes	Közepes	Alacsony	Alacsony	Nagyon alacsony
Valószínűtlen	Alacsony	Alacsony	Alacsony	Nagyon alacsony	Nagyon alacsony

1. Táblázat: Ajánlás kockázati szint mátrixra ISO/IEC 27005 szabvány „A" melléklete alapján [23]

A MIL-STD-882-E amerikai szabvány [34] egy hasonló mátrixot ad meg, amelyet katonai kockázatelemzés során „kötelező" használni. A 2. táblázatban azonban hat valószínűségi szint van és négy következmény alapján kapjuk meg az ötféle lehetséges kockázati szintet (elhanyagolható – eliminated, alacsony - low, közepes - medium, súlyos - serious, magas – high).

	Következmények súlyossága			
Valószínűség	1 - Katasztrofális	2 - Kritikus	3 - Nem jelentős	4 - Elhanyagolható
A - Gyakori	Magas	Magas	Súlyos	Közepes
B - Valószínű	Magas	Magas	Súlyos	Közepes
C - Alkalmi	Magas	Súlyos	Közepes	Alacsony
D - Csekély	Súlyos	Közepes	Közepes	Alacsony
E - Valószínűtlen	Közepes	Közepes	Közepes	Alacsony
F - Lehetetlen	Elhanyagolható	Elhanyagolható	Elhanyagolható	Elhanyagolható

2. Táblázat: Kockázati szint mátrix a MIL-STD-882E szabvány alapján [34]

A 2. táblázat tanúsága szerint B3 mező ugyanolyan kockázati szintet mutat, mint az D1 mező. A kockázati szint megállapítása után a valószínűségnek és a következmények súlyosságának továbbra is szerepet kellene játszani a kockázatkezelés módjának meghatározásában (elfogadás, kockázati szint csökkentése, megosztás, áthárítás vagy kockázatkerülés). Példánkban a D1 mezőbe eső kockázati eseménynél a következmények súlyosságát

javaslom preventív módon csökkenteni (D1 => D2), míg az B3 mezőbe kerülő kockázati eseménynél a valószínűség mérséklése lehet a preferált (B3 => C3).

A széles körben elterjedt FMEA módszer (Failure Mode and Effect Analysis; Hibamód- és Hibahatás Elemzés) három tényezőt vizsgál [13] [35];

- kárérték, súlyosság foka (Effect, 1 – alig észrevehető hiba, 10 – nagyon súlyos kár),
- bekövetkezés valószínűsége (Occurance, 1 – nagyon kis valószínűség, 10 – biztosan várható a hiba előfordulása),
- felderíthetőség (hiba esetén milyen gyorsan válik az felismerhetővé; Detection, 1 – jó hatásfokkal jelezhető a hiba, 10 – a hiba nem észrevehető, csak a későbbi káresemény jelzi…).

Ebből a három tényezőből számolunk egy „kockázat-prioritási számot" (RPN – Ratio Priority Number), ami valójában egy kockázati szintet mutat.

$$RPN = súlyosság\ foka \times bekövetkezési\ valószínűség \times felderíthetőség$$

Az RPN tehát egy 1-től 1000-ig terjedő diszkrét skálán mozoghat. A hibajavítás (és kockázat értékelés valamint -kezelés célja a magas RPN értékek csökkentése. Ilyenkor a 3 tényező közül a legnagyobbat javasolt kockázatkezeléssel lejjebb vinni. Az FMEA termelő és szolgáltató cégeknél nagyon elterjedt és konstrukciós tervezés hibáinak kiküszöbölése mellett használják technológiai folyamatoknál, infrastruktúrákhoz köthető rendszer-üzemeltetésben (pl. épületgépészet) és szervíztevékenységek kockázatkezelésében is.

A kockázatok, kockázati események (bekövetkezési valószínűség x következmények súlyossága) összegyűjtése és feldolgozása nehezen megvalósítható egy integrált kockázatmenedzsment rendszerben. Vannak olyan területek, amelyekben a valószínűség és a következmény majdnem pontosan meghatározható vagy kiszámolható esetleg mérhető (pl. árfolyam-ingadozás), más esetekben (pl. korábban nem tapasztalt természeti katasztrófák bekövetkezése, ill. azok következményei) ezek a paraméterek inkább csak becsülhetők. Integrált rendszerekben tehát az előbb bemutatott kvalitatív, osztályba soroláson alapuló kockázati esemény-minősítés lehet a végcél. Természetesen, ameddig lehetséges próbáljunk meg a számszerűsíthető, kiszámolható adatoknál maradni. Kvantitatív elemzés számszerű eredményeiből könnyebb kvalitatív kockázati szinteket meghatározni, mint fordítva…

Számos olyan szabvány és ajánlás van, amely érinti a kockázatmenedzsmentet és ösztönzi alkalmazását, de nem ez a fő profiljuk (Horváth – Szlávik, 2011a). Néhány a teljesség igénye nélkül;

- MSZ ISO 14001 Környezetközpontú irányítási rendszerek. Követelmények és alkalmazási irányelvek [32],
- MSZ 28001 (BS OHSAS 18001) A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR). Követelmények [27],
- MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Információbiztonság irányítási rendszerek. Követelmények [17],
- CObIT 5 verzió (Control Objectives for Information and related Technology magyar változata Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések) [14] [37],
- MSZ ISO/IEC 20000-1 Informatika. Szolgáltatásirányítás. 1. rész. Előírás [29],

- MSZ ISO/IEC 20000-2 Informatika. Szolgáltatásirányítás. 2. rész: Alkalmazási útmutató [30],
- MSZ ISO 22301 Üzletmenetfolytonossági irányítási rendszerek. Követelmények [33],
- MSZ EN ISO 9001 Minőségirányítási rendszerek. Követelmények [31],
- ISO/IEC 3300X Többrészes szabványcsomag a folyamatok értékelési lehetőségeiről folyamatcélok és várható eredmények tekintetében [25],
- ISO/IEC 38500 Corporate Governance of Information Technology IT vállalaton belüli irányítását szolgáló keretrendszer [26],
- SCOR Supply Chain Operations Reference modell, ellátási láncok működésére vonatkozó folyamatszervezési ajánlás [42],
- Project Management Body of Knowledge (Projektmenedzsment Útmutató) [40].

Az integrált vállalati kockázatmenedzsment (ERM – Enterprise Risk Management) kialakítása és működtetése jelentős lépés lehet egy szervezet életében. A hagyományos, szigetszerű kockázatkezelés töredezett, egymástól független intézkedéseket hozhat, amelyeknél nem ismerik fel kockázati esemény következményeinek összefüggéseit [6]. Az ERM ezzel szemben egy holisztikus megközelítés, amely integrálja kockázatkezelési gyakorlatot az egész szervezetre kiterjedően. Az üzleti és technológiai környezet állandó változása és bonyolultsága igényli a kockázatok átfogó, folyamatos azonosítását, elemzését és kezelését (mérséklését) [15].

Az ISO/IEC 31010-es szabvány [24] több mint 30 kockázatértékelésben és kezelésben alkalmazható eszközt és technikát sorol fel és értékeli használhatóságukat a Monte-Carlo módszertől, a hiba-fa analízisen át egészen a költség-haszon elemzésig. Természetesen egy integrált vállalati üzleti és technológiai folyamatokra fokuszáló kockázatmenedzsment rendszer esetében össze kell válogatni azokat, amelyek együttesen alkalmasak a kockázatok azonosítására, elemzésére, értékelésére és kockázatkezelés támogatására [1].

FOLYAMATOK KOCKÁZATKEZELÉSE

A kockázati események bekövetkezésének szervezeti működésre gyakorolt hatásának elemzése gyakran elmarad. A kockázatelemzés (akár előzetes, akár utólagos) a lokális káreseményre és annak nagyságára fókuszál az üzletmenetfolytonosság biztosítása helyett [20]. Nagyon ritka a vállalat számára előnyös „pozitív” kockázati események számbavétele [4].

Az ISO/IEC 33004-es (korábban ISO/IEC 15504) folyamat-felméréssel foglalkozó szabvány bevezetett hat „folyamatképességi szintet” [25];

0. hiányos folyamat (incomplete process; a folyamat célja nem, vagy csak részben teljesül),
1. végrehajtott folyamat (performed process; a folyamat célja teljesül, de időt és erőforrásigényt nem vizsgálunk…),
2. irányított folyamat (managed process; a folyamat és eredménye is megfelelően kézben tartott…),
3. kialakított folyamat (established process; a folyamat minta és/vagy szabvány alapján megtervezett és végrehajtott),

4. kiszámítható folyamat (predictable process; a folyamat végrehajtása mérhető és ellenőrizhető),
5. optimalizáló folyamat (optimizing process; a folyamatot folyamatosan fejlesztik az előre meghatározott üzleti célok elérése érdekében, megjelenik a visszacsatolás is…).

A folyamatok értékelésével és kimeneteik minősítésével a kockázatértékelést is érintjük [43]. A „végrehajtott" és az „irányított" folyamatok magas és közepes kockázatot hordozhatnak, míg a „kialakított" (3. szint) és a „kiszámítható" (4. szint) folyamatokhoz közepes és alacsony kockázati szint társulhat. Az „optimalizáló" folyamat csak alacsony kockázatú lehet. A megállapított kockázati szint természetesen függ attól is, hogy a tényleges folyamat a valóságban mennyire tér el az előre megadott / besorolt képességszinttől.

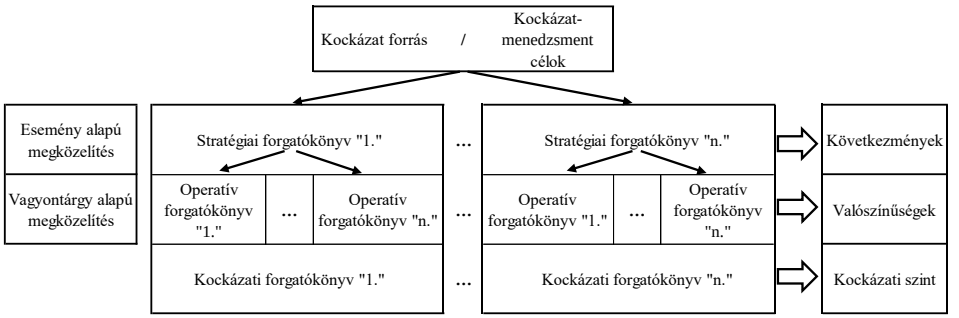
A folyamatok kockázatelemzése a kockázati források (fenyegetések) összegyűjtésén és azok hatásainak elemző vizsgálatát kívánják. Ebben a vizsgálatban szempont lehet folyamatelemek pontos meghatározása, a végrehajtásukhoz szükséges erőforrások rendelkezésre-állása. Gyakorlatilag a folyamatok sebezhetőségeinek strukturált gyűjteménye [7].

BIZONYTALANSÁG A KOCKÁZATELEMZÉSBEN

Ismeretek és tapasztalatok hiányában nem megoldott a korábban még nem bekövetkezett kockázati események kockázat becslése és kezelése. A kockázat leltárban megfogalmazott kockázati események helyett gyakran csak veszélyeket, fenyegetettségeket, gyengeségeket, bizonytalanságokat vagy biztonsági problémákat nevezünk meg bekövetkezési valószínűség és a kár nagyságának megadása, mérése vagy becslése nélkül. A bizonytalanság információhiányt is jelent és a kockázat nem létezik bizonytalanság nélkül [4].

A kockázatelemzés vagyontárgy- (A.2.4) és eseményalapú (A.2.5) az ISO/IEC 27005-ös szabvány szerint [23]. A vagyontárgy alapú megközelítés a jelentős értékű, vagy más szempontból fontos vagyontárgyak sérülékenyégeit, ill. az ezt kihasználni képes fenyegetéseket veszi számba. Az esemény alapú megközelítés a kockázatok forrásából indul ki (elsősorban szándékos károkozók motiváció és az általuk elérni kívánt célok). Előbbi valószínűségeket is tartalmazó operatív forgatókönyveket (operational scenario), míg utóbbiak következményeket megadó stratégiai forgatókönyveket (strategic scenario) eredményeznek. Minden operatív forgatókönyv összeköthető legalább egy stratégiai forgatókönyvvel, ill. egy stratégia forgatókönyvhöz tartozhat több operatív forgatókönyv (2. ábra). Ezeknek a kapcsolatoknak a folyománya a kockázat szintjét (risk level) is meghatározó kockázati forgatókönyv (risk scenario). Kétségtelen, hogy ha stratégiai forgatókönyvekhez nem tudunk minden fontos operatív forgatókönyvet hozzárendelni, akkor a kockázatelemzésünk hiányos lehet.

A szervezet, vállalat dolgozói és vezetői, üzleti partnerei gyakran szubjektív módon látják a várható kockázati eseményeket. Ezek sokszor befolyásolják a folyamatos, „együttfutó" csoportos kockázatértékelés eredményét. Nevezzük ezeket a kockázatokat „érzékelt" kockázatnak. A kockázatmenedzsmentben járatos szakemberek által, a folyamatok indítása előtt elvégzett tapasztalat alapú kockázatelemzés adja az „azonosított" kockázatokat. A két halmaz nem mindig fedi egymást, sőt általában nem egyezik a nem mindig feltárt „valós" kockázatokkal. A kockázat-érzékelés alapvetően meghatározhatja a szervezet tagjainak tevékenységeit és viselkedését is [21].



2. Ábra: Kockázati forgatókönyveken alapuló kockázatértékelés (ISO/IEC 27005 szabvány„A" melléklete alapján) [23]

KÖVETKEZTETÉSEK

Egységes, azonos mérési skálán történő kockázatértékelés javasolt minden üzleti- és technológiai folyamatot figyelembe véve [6].

A „funkcionális", részterületekre fókuszáló kockázatmenedzsment helyett alkalmazott integrált, folyamatalapú kockázat elemzés és -kezelés növelheti vállalati biztonsági szintjét [8].

Jó, ha az integrált kockázatmenedzsment a szervezeti erőforrások rendelkezésre állásán, annak elemző és előrejelző vizsgálatán (is) alapszik. Fontos a kockázatmenedzsment rendszer kialakításakor, hogy az ide vonatkozó ajánlások és szabványok közül melyeket akarjuk alkalmazni (mit vár el a környezetünk?), azokat hangoljuk össze a szervezet új, integrált kockázatkezelési gyakorlatával.

FELHASZNÁLT IRODALOM

[1] A. Balogh, Kockázatmenedzsment és kockázatértékelés. *Magyar Minőség*, XX. évf. 03. szám, 2011., pp. 6-25.

[2] H. Cendrowski and W.C. Mair, *Enterprise risk management and COSO. A Guide for Directors, Executives and Practitioners.* New York, John Wiley & Sons, 2009.

[3] Sz. Farkas és J. Szabó, *A vállalati kockázatkezelés kézikönyve.* Dialog Campus Kiadó, Budapest – Pécs, 2005.

[4] I. Fekete, Integrált kockázatmenedzsment a gyakorlatban. *Vezetéstudomány*, XLVI. évf., 1. szám, 2015., pp. 33-46.

[5] I. Fekete, Folyamat alapú működési kockázatfelmérés - kockázatelemzés alapú belső ellenőrzés. *Egészségügyi Gazdasági Szemle*, 2009/6., pp. 5-10.

[6] Zs. Horváth, A kockázatkezelés alkalmazási területei. Magyar Minőség, XX. évf., 03. szám, 2011., pp.15-24.

[7] Zs. Horváth, Kockázatmenedzsment a vállalati sikeresség érdekében. *Magyar Minőség*, XXVI. évf. 01. szám, 2017., pp. 16-24.

[8] Zs. Horváth és P. Szlávik, Vállalati integrált kockázatkezelés I. *Magyar Minőség,* 2011/3., pp. 124-129.

[9] Zs. Horváth és P. Szlávik, Vállalati integrált kockázatkezelés II. *Magyar Minőség*, 2011/4., pp. 219-226.

[10] T. Jenei, Leggyakrabban használt kockázatkezelési modellek összehasonlítása. *International Journal of Engineering and Management Sciences*, Évf. 1., 1. szám, 2016., p.11, doi: 10.21791/IJEMS.2016.1.22
[11] Á. Kemendi, Integrált kockázatkezelés. *Biztonságtudományi Szemle*, IV. évf., 1. szám, 2022., pp. 43-61.
[12] F.H. Knight, *Risk, Uncertainty, and Profit*, Boston and New York, Houghton Mifflin Co., The Riverside Press. 1921. [on-line] Elérhető: www.econlib.org/library/Knight/knRUP.html?chapter_num=9#book-reader
[13] A. Koncz and L. Pokorádi and Gy. Szabó, Failure Mode and Effect Analysis and Its Extension Possibilities. *Repüléstudományi Közlemények*, 30. évf., 1. szám, 2018., pp. 247-254.
[14] Tné. Mógor és Z. Rajnai, Elektronikus adatkezelő rendszerek kockázatelemzése, kockázati módszerek bemutatása. *Bolyai Szemle*, XXIII. évf. 2. szám, 2014., pp. 43-59.
[15] M. N. Mupa and F. R. Chiganze and T. I. Mpofu and R. M. Mubvuta, The Role of Enterprise Risk Management (ERM) in Supporting Strategic Decision-Making Processes in the Energy Sector. *IConic Research and Engineering Journals*. Vol.8. Issue 2., 2024., pp. 826-848.
[16] N. Racz and E. Weippl and A. Seufert, A process model for integrated IT governance, risk, and compliance management. Proceedings of the Ninth Baltic Conference on Databases and Information Systems, 2010., p.15.
[17] S. Répás és I. Dalicsek, Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében. *Pro Publico Bono - Public Administration*. Vol. 3 No. 4, 2015., pp. 22-33.
[18] K. S. Shrader-Frechette, Kristin, *Risk analysis and scientific method*. D. Reidel Publishing Company, 1985., p.232.
[19] M. K. Starr, Rendszerszemléletű termelésvezetés, termelésszervezés. Közgazdasági és Jogi Könyvkiadó, 1976., p. 619.
[20] S. Takács and A. Tóth, Folyamatmenedzsment a fizikai biztonság területén. *Magyar Rendészet*. 2024/2. pp.105-120. doi:10.32577/mr.2024.2.6
[21] T. Vasvári Tamás, Kockázat, kockázatészlelés, kockázatkezelés - szakirodalmi áttekintés. *Pénzügyi Szemle.* 2015/1. pp.29-48.
[22] Z. Yazar, A Qualitative Risk Analysis and Management Tool - CRAMM. Global Information Assurance Certification Paper Version 1.3. SANS Institute (InfoSec Reading Room), 2000-2005. p.14. [on-line], Elérhető: https://www.giac.org/paper/gsec/1746/qualitative-risk-analysis-management-tool-cramm/103133
[23] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks.
[24] ISO/IEC 31010:2019 Risk management - Risk assessment techniques
[25] ISO/IEC 33004:2015 Information technology - Process assessment - Requirements for process reference, process assessment and maturity models
[26] ISO/IEC 38500:2024 Information technology - Governance of IT for the organization
[27] MSZ ISO 28001:2024 Az ellátási lánc biztonságirányítási rendszerei. Az ellátási lánc biztonságának, felméréseinek és terveinek megvalósítására vonatkozó legjobb gyakorlatok. Követelmények és útmutató (Security management systems for the supply chain.

Best practices for implementing supply chain security, assessments and plans. Requirements and guidance)
[28] MSZ ISO 31000:2018 Kockázatmenedzsment. Irányelvek.
[29] MSZ ISO/IEC 20000-1:2019 Informatika. Szolgáltatásmenedzsment. 1. rész: A szolgáltatásirányítási rendszer követelményei.
[30] MSZ ISO/IEC 20000-2:2024 Informatika. Szolgáltatásmenedzsment. 2. rész: Útmutató a szolgáltatásirányítási rendszerek alkalmazásához (Information technology. Service management. Part 2: Guidance on the application of service management systems)
[31] MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények (ISO 9001:2015)
[32] MSZ EN ISO 14001:2015 Környezetközpontú irányítási rendszerek. Követelmények alkalmazási útmutatóval (ISO 14001:2015)
[33] MSZ EN ISO 22301:2020 Társadalmi biztonság és rugalmasság. Üzletmenetfolytonossági irányítási rendszerek. Követelmények (ISO 22301:2019, angol nyelvű)
[34] MIL-STD-882E, System Safety. Department of Defense. Standard Practice. USA, 2012.
[35] AIAG & VDA, *Hibamód és Hatás Elemzés - FMEA Kézikönyv*, 2019
[36] Belső Ellenőrök Magyarországi Közhasznú Szervezete, Ajánlás a COSO kockázatkezelési keretrendszer alkalmazására, 2023., p.20.
[37] CObIT 5, Vállalati IT irányítás és menedzsment üzleti keretrendszere. ISACA 2012., p. 104.
[38] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management* (Compliance Risk Management: Applying the COSO ERM Framework), 2020., p. 48.
[39] Institution of Mechanical Engineers, *ALARP for Engineers*: A Technical Safety Guide. Report, 2024., Version: 1.1.
[40] Project Management Institute, *Projektmnedzsment Útmtató* (Project Management Body of Knowledge - PMBOK Guide. Akadémiai Kiadó, 2006.
[41] AIRMIC - Association of Insurance and Risk Managers, ALARM - The National Forum for Risk Management, IRM - Institute of Risk Management, *A Risk Management Standard*, 2002.
[42] Supply Chain Council. *Supply Chain Operations Reference (SCOR) Model. Overwiev*. Version 10.0, 2010. [on-line], Elérhető: https://pessolutions.com/wp-content/uploads/2018/02/SCOR10-Overview.pdf
[43] Trusted Business Partners Kft. (szerk. Iványos János): *Kockázatkezelési kézikönyv v.2.1.* (Irányítási forgatókönyvek alkalmazása az integrált vállalati kockázatkezelés megvalósítására), 2014., p.93.