



Fehér Péter

Mindennapi Kockázataink



Fehér Péter: Mindennapi Kockázataink, megjelent: Harvard Business Review (magyar kiadás), 2008. dec.—2009. jan.

Nem tudhatjuk, hogy szervezetünk kockázataiból
mikor lesz ténylegesen veszteség – de felkészülhetünk rá.



Mindennapi Kockázataink

A működési kockázatok kezelése



A KÜLÖNBÖZŐ SZERVEZETEKNEK SZÁMTALAN veszteséget és költséget jelentő kockázattal kell szembenéznük működésük során: a természeti katasztrófák (földrengés, árvíz, hurrikán, stb.) mellett igen jelentős mértékben a hanyagságból vagy rosszhiszeműségből elkövetett, ember által előidézett veszélyekkel is (csalás, informatikai rendszer feltörése, hanyag működtetés, szakértelem hiánya). Habár a működési kockázatok kezelésének kihívásával hangsúlyosan a pénzügyi szektor szervezetei kapcsán találkozunk, szinte minden vállalat esetében szükséges tudatosan foglalkozni a problémakörrel, melyet gyakran jogszabályi előírások is megkövetelnek.

A működési kockázatok kiemelt kezeléséhez jelentősen hozzájárultak az elmúlt majd két évtized vállalati és banki botrányai: gondoljunk itt a Barings Bank 1995-ös nagy veszteséget okozó esetére, melynek hatása az brit királyi családot is elérte (Lásd: *Barings Bank, 1995* című keretes írást), vagy ennek szinte tökéletes másolatára a közelmúltban a Société Générale esetében (Lásd *Société Générale, 2007* című keretes írást).

A pénzügyi szektoron kívül is számos nagyvállalat szolgáltatott látványos ügyeket: Enron, Parmalat, Wordcom, Xerox (Lásd *Könyvelési botrányok c. keretes írást*). Hazánkban a közelmúltban a MÁV Biztosító Egyesülethez felügyeleti biztosokat küldött ki a PSZÁF, és egymilliárd forint értékű sikkasztás és pénzmosás ügyében indult nyomozás a biztosító vezetője és több társa ellen. A gyanú szerint a vezetők különböző megoldásokkal kivonták az összeget a biztosító kezeléséből, és azokat magánszámlán helyezték el. A vizsgálathoz az adott kezdőlökést, hogy pénzügyi nehézségek miatt az egyesület nem tudta a megfelelő mértékű tartalékot felmutatni biztosítási állományra vonatkozóan.

Fehér Péter (pfeher@corvinno.hu) közgazdász, a Corvinno Technology Transfer Center tanácsadó partnere, a Budapesti Corvinus Egyetem Információrendszerek Tanszékének adjunktusa. Főbb tevékenységi területei közé tartozik a folyamatmenedzsment, kockázatmenedzsment és informatikai szolgáltatásmenedzsment.

A működési kockázatok értelmezése

A banki és más szervezetekben tapasztalható viszásságok mellett, az környezeti kockázatok (terrorizmus, katasztrófák) növekedése is hozzájárult a működési kockázati terület felértékelődéséhez. Maga a globalizáció, azaz az üzleti környezet is növeli a fenyegetettséget, mivel egyre elterjedtebbé válnak az anyagilag előnyösebb, de kockázati szempontból veszélyesebb megoldások, mint a kiszervezett tevékenységek, illetve a szoros szervezeti együttműködések, hálózati egymásrautaltsági viszonyok.

Kockázat minden üzleti tevékenységünkhöz kapcsolódik, mely kockázat alatt valamilyen jövőbeli veszélyt, ill. veszteség bekövetkezésének esélyét értjük. Általánosabb értelemben a kockázat nem más, mint a jövő kiszámíthatatlansága, bizonytalansága, ami veszteséget okozó eseményekhez vezethet. Ilyen lehet például a minőség romlása, a teljesítések idejének növekedése, pótlólagos erőforrás igény megjelenése, melyek – akár áttételesen is, de minden esetben – költségtöbbletet okoznak. A kockázatkezelés célja a veszteség elkerülése, illetve mérséklése.

A kockázatok az emberek tevékenységéből, a működési folyamatok elégedetlenségéből, a technológiai megoldások nem megfelelő, vagy hibás működéséből, illetve külső környezeti hatásokból származhatnak. A két leggyakoribb kockázat a külső csalásokhoz, illetve a nem megfelelő belső működéshez kapcsolódik.

A közelmúltban Magyarországon esett meg, hogy egy volt ügyvéd hamis bírósági ítéletekkel nyújtott be inkasszót gazdasági társaságok számláival szemben, és cégenként 8-9 millió forintot próbált megszerezni. Mivel korábban már voltak ilyen esetek, ezért a pénzügyi intézetek nem fizették ki automatikusan a kívánt összeget, hanem ellenőrizték az ítéletek valóságtartalmát, így az elkövető lebukott.

Sajnos napjainkban mind a természeti katasztrófák, mind a terrorista támadások is élő veszélyt jelentenek, és nagyon sok cég fel is készül ilyen helyzetekre. A 2001-es World Trade Center elleni támadás amellett, hogy emberáldozatokat követelt, az informatikai infrastruktúrát, és számos cég adatait is megsemmisítette. Sok esetben ugyanakkor a biztonsági mentéseknek köszönhetően a működés néhány nap (vagy például a Deutsche Bank esetében 2 óra) elteltével már zavartalanul folyt.

Miami-ban inkább a hurrikánok jelentenek veszélyt. A Banco Santander Central Hispano egy a világ tíz legnagyobb bankja közül. Miami központja nem csak turistalátványosság, hanem egyben kimelt helyet foglal el a hurrikánok által veszélyeztetett területek között. 2004-ben például a sorozatos hurrikánok négyszer is leállásra kényszerítették a Miami-

Barings Bank, 1995

1995-ben szinte teljesen váratlan módon a Barings Bank egy fiatal kereskedője, Nick Leeson egymaga csődbe juttatta a nagy múltú bankházat, egyszerre szolgáltatva példát a piaci, pénzügyi és működési kockázatokból adódó lehetséges veszteségekre. A kockázatos pénzügyi műveletek mellett a tevékenységi kontroll hiánya, illetve a tudatos csalás is hozzájárult ahhoz, hogy a bank nevében 827 millió fontos veszteséget halmozzon fel. A bukásban jelentős része volt annak, hogy Leeson gyakorlatilag belső ellenőrzés nélkül hajthatta végre tevékenységét.

Annak érdekében, hogy felhalmozott veszteségeit eltakarja, meghamisította saját számláit, és a veszteségei fedezéséhez szükséges összegeket más számlákról vette el, illetve megakadályozta, hogy tevékenysége belekerüljön a londoni központnak küldött beszámolóba. A Barings Bankház 1994-ben kezdte meg kockázatmenedzsment tevékenységének kiépítését, de kezdetben a szingapúri egysége – ahol a csalássorozat történt – még nem volt bevonva ezekbe a tevékenységekbe. Szingapúrban gyakorlatilag nem volt senki, aki ellenőrizhette volna Leeson tevékenységét, hiszen ő maga volt az a személy is, akinek ellenőriznie kellett volna a számlákat. Emiatt a nyilvánvaló belső működési probléma miatt sokan (köztük Leeson is) a Bankházat is hibáztatták a csőd miatt.

A brit Board of Banking Supervision (bankfelügyelet) megállapítása szerint a csőd elsődleges oka a kockázatkezelési rendszerek teljes használhatatlansága, illetve a megalapozott kockázatkezelési tevékenység hiánya volt. Kiemelendő hiányosságok voltak a működést tekintve:

- a végrehajtási és ellenőrzési funkciókat nem választották szét (így Leeson saját magát ellenőrizte)
- a mátrix alapú beszámolási rendszerben szétaprózva jelentek meg az információk, így szinte lehetetlen volt összeilleszteni a csalásra utaló jeleket
- nem volt világosan meghatározva a felügyeleti tevékenység
- a bankcsoporton belüli pénzáramlásokra nem határoztak meg sem az ellenőrzési mechanizmust, sem az igénybevételi korlátot
- az 1994-ben végrehajtott belső audit eredményeit és ajánlásait nem vették időben figyelembe, és nem alakították át a bank működését

A bankot végül – még 1995-ben – az ING vette meg, szimbolikus 1 fontnyi összegért, és létrehozta az ING Barings bankot. Nick Leeson menekülés közben elkapták, és Szingapúrban 6 és fél évnyi börtönre ítélték. Jó magaviselettel 1999-ben szabadult³.

Société Générale, 2007

Szinte lemásolta a Barings Bank esetét egy francia bankár. A Société Générale – mint minden pénzintézet – ismerte a Barings Bank esetét, és így tisztában volt a működési kockázatok fontosságával. De ugyanennyire tisztában volt ezzel Jerome Kerviel is, aki korábban épp a kockázatkezelési osztályon dolgozott, és így ismerhette az ellenőrzési szabályokat, illetve ismerte azokat a lehetőségeket is, melyekkel ezek a szabályok kijátszhatóak.

Kerviel 2005-től kezdődően kötött fiktív határidős ügyleteket, megtevéstve a belső ellenőrzési rendszert. Később azt állította, hogy nem ő az egyetlen alkalmazott, aki a saját szakállára (de nem feltétlenül a saját hasznára) dolgozik. Kerviel hamis kliensszámlákat felhasználva egy másra épülő határidős ügyleteket kötött, az általa felépített pozícióit elrejtette, és úgy tűnik, hogy igazából maga a bank sem akarta nagyon megtalálni.

A bank automatikus rendszerei többször is kiadták a riasztást, és ekkor Kerviel felettesei számon is kérték a történéseket (főleg, mivel túllépte az engedélyezett összegeket), de ilyenkor mindig sikerült hamis dokumentumokkal igazolnia, hogy ügyletei nem jelentenek kockázatot a bank számára. Ebbe beletartozott az a hamis portfólió is, mely elvileg fedezte a kockázatosabb ügyleteket. Az ügyészség hamisításért, hamisított okiratokkal való visszaélésért és informatikai adatok automatizált rendszerébe történő behatolásért indított eljárást.

Melyek az eset tanulságai?

- Az emberekhez köthető kockázatok nem mindig egyéni haszonszerzés céljából történnek. Kerviel annak ellenére nem a saját zsebére dolgozott, hogy fizetése ebben a szakmai körben nem volt kiemelkedő, csak egyszerűen szerette volna bebizonyítani, hogy kivételes képességű bróker.
- Az eset rávilágít arra, hogy hiába van tisztában egy bank a működési kockázatokkal, nem biztos, hogy mindent megtesz ezek kivédése érdekében. Sőt, az intézmények sok esetben tudatosan vállalnak bizonyos fokú kockázatot, mivel félnek, hogy a túlzott ellenőrzés és kontroll megöli a kezdeményező kedvet.
- Hiába használ egy intézmény informatikai rendszert a kockázatok felderítésére, ha ezeket hagyományos eszközökkel ki lehet játszani. Hogy fordulhat elő, hogy hamis okiratok fedezik az ügyleteket? Bár elvileg minden tranzakció az informatikai rendszereken keresztül folyik (és mindennek nyoma van), úgy tűnik még mindig nem elég hatások a szabályok, az ellenőrzés, sem pedig a támogató informatikai megoldások.

ban található adatközpontot. Mivel veszélyhelyzetre felkészülve háttér szolgáltató-központot építettek ki New-York-ban, a hurrikánveszély ellenére is tudtak foglalkozni ügyfeleikkel.

A hírekben gyakran hallható, hogy egy bank ATM rendszere nem működik, ezt általában valamilyen központi szerver, alkalmazás vagy adatbázis hiba okozza. Nemrégiben a Barclays Bank volt kénytelen szembesülni ilyen problémával, mely fél Nagy Britanniát megbénította. A hírek szerint a problémát egy adatbázis szoftver frissítése okozta, bár a bank az esetet áramszünetre fogta. Az mindenestre tény, hogy nem gondoskodtak megfelelően a kieső informatikai szolgáltatás kiváltásáról.

Az itt bemutatott példák közül több szélsőséges veszteségeket okozott, illetve jelentős működési kihívást hordoz magában. A kockázatok elemzése során vizsgálni kell a kockázatok realizálódásának gyakoriságát, illetve a kapcsolódó veszteség súlyosságát is, hogy megválaszthassuk a megfelelő kockázatkezelési módszert. Általában a ritka, és kis veszteséggel járó kockázatok esetében nem szükséges jelentős kockázatkezelési tevékenységet folytatni, míg a másik véglet (nagy gyakoriságú és súlyos veszteséget okozó események) esetében az adott területen vagy jelentős beavatkozásra van szükség, vagy pedig mérlegelni kell az érintett tevékenység feladását.

A kockázatkezelési feladatok (Lásd *Működési kockázatok gyakorisága és súlyossága* c. ábrát) ugyanak-

kor nagyjából kockázatok a nagy gyakoriságú, de kis veszteséget okozó, illetve ritka, de nagy veszteséget okozó szeletére koncentrálódnak. A nagy gyakoriságú kockázatok esetében viszonylag jól ismertek a kockázatok (mivel gyakoriak), így fel lehet tárni a kapcsolódó mélyebb összefüggéseket, és fel lehet készülni az ellenintézkedések megtételére.

Az áramszolgáltatók számára visszatérő veszteséget jelent az áramlopás. Ez a jelenség mind az iparágban, mind pedig az egyes vállalatok tevékenységében ismert, jól mérhető, és az árazásba beépíthető. Ez olyan kockázat, melynek mértéke jól becsülhető, és mértéke nem veszélyezteteti közvetlenül a vállalatok működését. A vállalatok igyekeznek ezeket a veszteségeket visszaszorítani, és igyekeznek az áramlopásokat is felderíteni.

Nagyobb kihívást jelent a ritka, de nagy veszteséget okozó kockázatok esetében, mivel ekkor nem ismert, mire is kell egy szervezetnek felkészülnie. Ekkor a szakértőknek kell elképzelniük és azonosítaniuk ezen szélsőséges eseteket. Az ilyen katasztrófa-tervezések esetében a szakértőktől olyan szélsőséges esetek feltárását várják, melyek akár létükben veszélyeztetnek egy szervezetet. Az ilyen kockázatok egy részére fel lehet készülni, és a váratlan események következményeit – részben vagy egészben - át lehet hárítani másra (biztosítás, alvállalkozó, kiszervezés). Ugyanakkor a nagyon ritka de nagyon nagy hatású kockázatok realizálódása esetében a szervezeteknek maguknak kell viselniük a kockázatot. Az ilyen kockázatok esetében az iparági tapasztalatok is inkább

Könyvelési botrányok

A pénzügyi szektoron kívül valószínűleg az Enron esete volt az, amely igazán felkeltette a világ figyelmét, illetve elindította a könyvelési botrányok felgöngyölítésének folyamatát. Az Enron bukását az okozta, hogy számtalan iparágba szállt be a haszon reményében, de befektetései nem térültek meg. Ez a probléma még a piaci kockázat kategóriájába tartozna, ha a cég vezetői nem hamisították volna meg a kimutatásokat és a könyvelést, ezáltal megtévesztve mind a piacot, mind a befektetőket, miközben a cég vezetői dollármilliókat vettek ki a vállalatból. A történet végén elkerülhetetlen volt a csőd, melynek értéke 31 milliárd dollárra rúgott.

Az Enron botrányba belebukott a világ egyik legnagyobb könyvvizsgáló cége is, az Arthur Andersen, mivel a nagy tevékenység mellett felmerült az a gyanú is, hogy tudatosan semmisítették meg bizonyítékokat az ügyben. Ezután nagy ügyfelei sorra mondták fel a szerződéseket.

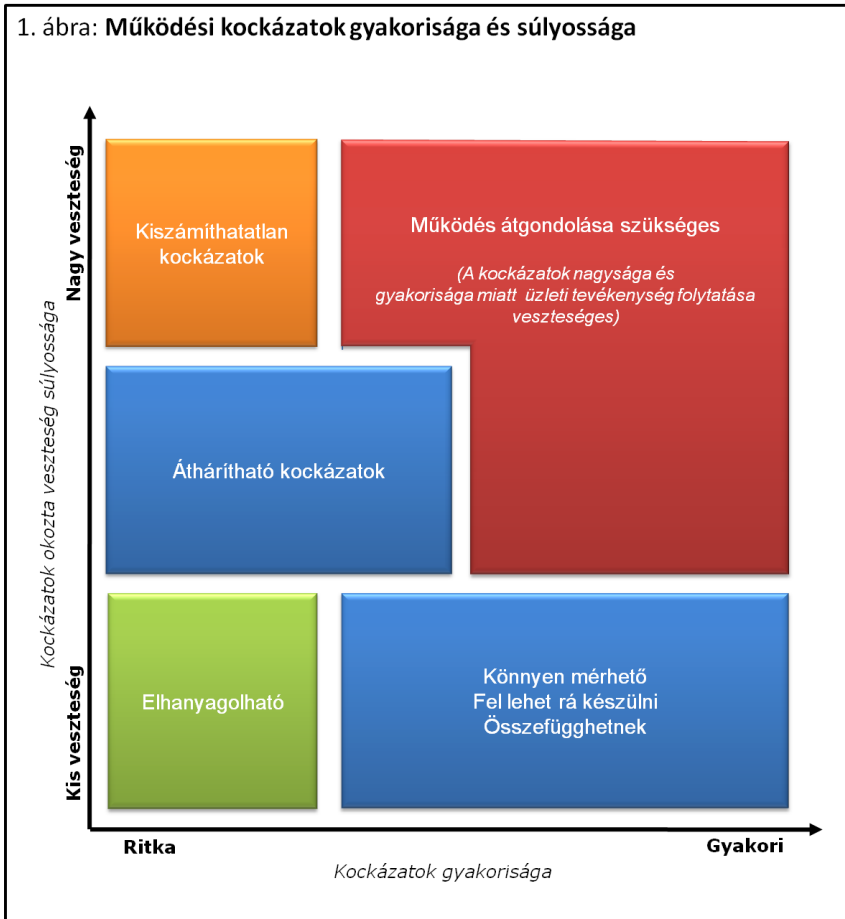
Az Enron-hoz hasonló eset történt Európában is: a könyvelési visszasságokra, és így a befektetők és tulajdonosok félrevezetésére talán a legnagyobb európai példa az olasz Parmalat esete (melyet európai Enron-ként is emlegetnek), ahol 2003 végén fedezték fel a 14 milliárd Euro értékű könyvelési csalást. A problémák oka az 1990-

es évek végi expanzióra, felvásárlásokra vezethető vissza, melyeket a cég hitelekkel finanszírozott.

Mivel a befektetések veszteségesnek bizonyultak, Fausto Tonna, a pénzügyi vezető igyekezett ezeket a lyukakat elrejteni. A problémákat 2003-ban az új pénzügyi vezető fedezte fel, aki feltárta, hogy a cég hitelállománya több mint kétszerese annak, amiről tudtak. A cég fizetéképtelenségét hosszú ideje az éves beszámolójának és banki kivonatainak meghamisításával takargatták. Később kiderült, hogy a Parmalat égisze alatt pénzügyi csalássorozat, pénzmosás, sőt sikkasztás is meghúzódott, miközben igyekeztek a cég vagyonát más vállalkozásokba kimenteni.

Meg lehetne még említeni a Worldcom, a Xerox és még számtalan - nem kis vállalat - hasonló problémáit is. Ezek az esetek rámutatnak arra, hogy a vezetők manipulációi milyen károkat tudnak okozni, főleg akkor, ha az elvileg független könyvvizsgálók is összejártsanak velük, illetve a hitelező bankok szemet hunynak a problémák felett. Mindezen jelenségek hozzájárultak ahhoz, hogy a szabályozó testületek és a törvényhozók olyan új rendelkezéseket hoztak, melyek erősítik a kontrollt a szervezeti tevékenységek felett, illetve rákényszerítik a szervezeteket, hogy mérjék fel és kezeljék saját működésükhöz kapcsolódó kockázataikat.

1. ábra: Működési kockázatok gyakorisága és súlyossága



útmutató jellegűek, mivel az ilyen jellegű kockázatok jelentős része szervezetspecifikus, és egyedien kapcsolódik az egy konkrét szervezet működéséhez.

Szabályozási keretek

A működési kockázatok felméréseinek és kezelésének kialakulása a legkarakteresebben a pénzügyi szervezetekhez, elsősorban bankokhoz kötődik, ugyanakkor – ahogy a veszteségeket illusztráló példákban is kiténik – nem csak ezen szervezetek sajátossága. A bemutatott példákhoz hasonló esetek arra ösztönözték a politikai és szakmai döntéshozókat, hogy különféle szabályozásokkal erősítsék meg a működési kockázatokhoz kapcsolódó szervezeti feladatokat és felelősséget.

A szabályozási elvárásoknak való megfelelés maga is kockázatot hordoz magában, mely része a működési kockázatnak, de legalább is szoros kapcsolatban áll vele (szabályozási és reputációs kockázat). A különféle szabályozási elvárásoknak való megfelelés ugyanakkor külön működési területként jelenik meg, mivel a szabályozások összefüggései, összetettsége önmagában jelentős kihívás elé állítja a szervezeteket (A legfontosabb szabályozási eljárásokat a táblázat szemlélteti). Emiatt igen sok cég számíthat büntetésre, illetve tevékenységének korlátozására is.

Az iraki háborúban beszállítóként részt vevő cégeknél végzett ellenőrzés számtalan hiányosságot tárt fel, mely az amerikai adófizetőknek több mint 8 milliárd dolláros veszteséget okozhatott. Az ellenőrzés eredményeképpen a szabályozási előírások be nem tartása miatt több céggel azonnali hatállyal felbontották a szerződést, mely jelentős bevétel-kiesést okoz számukra.

A különféle külső szabályozásoknak való megfelelés mellett biztosítani kell a vállalat belső elvárások szerinti működését is, ez a belső ellenőrzés felelőssége. Feladat körébe beletartozik a csalások felderítése, és a szervezeti erőforrások (beleértve a fizikai és immateriális javakat is) védelme is.

Különféle ajánlások és szabványok fogalmazhatóak meg speciálisan, a működési kockázatok egyik kiemelt területével, az informatikával szemben is. Mivel sok szervezet, de kiemelten a

pénzügyintézetek és telekommunikációs cégek esetében az üzleti szolgáltatások igen erősen az informatikai megoldásokon alapulnak, ezért az informatikai problémák jelentős kieséseket és veszteségeket okozhatnak. Mindezen okok miatt az informatikai infrastruktúra és szolgáltatások folyamatos működése évek óta kiemelkedő fontosságú, és ezen területre kiforrott módszertanok, élenjáró iparági gyakorlatok, sőt szabványok állnak rendelkezésre (pl. CobIT, ITIL, ISO 17799).

Miközben a működési kockázatok kezelése egyre inkább önálló területként jelenik meg – és így pl. a Bazel II szabályozás is önálló kockázati területként írja elő a kezelését – addig más vélemények szerint nem szabad szétválasztani a működési kockázatokot más kockázatainktól, hiszen a működési kockázat minden más tevékenység, így kockázati terület szerves részét képezi. Amikor pl. informatikai kockázatról beszélünk, ennek jelentős része működési kockázatot (is) takar, vagy a szabályozási megfelelés (compliance) kockázata is magába foglalja a működési kockázatot.

A szabályozási elvárásoknak való megfelelés maga is kockázatot hordoz

Egy hazai bank úgy értékelte, hogy a legnagyobb működési kockázat az informatikai eszközeihez kapcsolódik, ezért elsősorban az informatikai erőforrások kockázatának és hatásának felmérésére koncentrált. Az elemzés során vizsgálták, hogy az egyes informatikai eszközök milyen üzleti folyamatokat támogatnak, és így az IT szolgáltatások kiesése milyen üzleti hatással és veszteséggel jár együtt. Az összefüggések feltárását nehezítette, hogy egy informatikai eszköz több üzleti folyamatnak is részese volt, illetve egy folyamatban több IT szolgáltatást is igénybe kellett venni. Ezen komplex összefüggérendszer hatásának elemzésére, illetve a lehetséges szolgáltatási kiesések kezelésére szolgáló tervek ki-

alakítására újabb informatikai támogató eszköz beszerzésére volt szükség.

Az informatikától való erős függőséget illusztrálja egy hazai telekommunikációs cég példája is: mind a távközlési szolgáltatások, mind pedig az ezekhez kapcsolódó adminisztratív feladatok – így a számlázás is – informatikai támogatással működnek. A cég számlázási szoftverének frissítése során olyan hiba került a rendszerbe, mely néhány nap múlva leállította az alkalmazás működését. Ennek eredményeképpen egy bizonyos ügyfélcsoport ingyen telefonálhatott, azaz a cég érzékelte a felhasznált kapacitást, de azt nem volt képes ügyfélhez kötni, így a hiba

Szabályozás	Leírás
Bázel II / Capital Requirement Directive (CRD)	A Bázel II szabályozás a pénzügyintézetek számára határozza meg a tőkefedezet képzésének feltételeit a bankok hitelezési, piaci és működési kockázatát figyelembe véve, így biztosítja a bankok stabil működését. A szabályozás meghatározza a működéshez kapcsolódó felügyeleti, illetve nyilvánossági feltételeket is.
Markets in Financial Instruments Directive (MiFID)	A direktíva szabályozza a befektetési szolgáltatások működési kérdéseit, mely meghatározza egyben a működési folyamatokat is, beleértve az ügykezelés hatékonyságát, érdekkonfliktus kezelést, valamint a kereskedelem átláthatóságát és nyitottságát.
Sarbanes-Oxley Act (SOX) EU 8. direktíva (Euro-SOX)	Az amerikai törvény célja a könyvelési botrányok által megrendített bizalom helyreállítása volt, és előírja a könyvelési és beszámolási folyamatokra vonatkozó kontroll tevékenységeket, valamint szabályozza a nyilvánosságra hozandó adatok körét. Az EU 8. direktívájának 2005-ös kiegészítése a SOX európai megfelelője, elsősorban a pénzügyi-számviteli kockázatokra koncentrálna.
Gesetz Zur Kontrolle Und Transparenz Im Unternehmensbereich (<i>KonTraG</i>) Transparenz- und Publizitätsgesetz (<i>TransPuG</i>)	A KonTraG egy 1998-ban született német szabályozás, mely előírja a vállalatok kockázatkezelési szabályozásának és gyakorlatának független auditálását a pénzügyi beszámolókra vonatkozóan. Ennek kiegészítése a 2002-es TransPuG, mely előírja a pénzügyi beszámolókhöz kapcsolódó nyilvánosságot.
Pénzmosás és terrorizmus elleni szabályozások USA: Financial Anti-Terrorism Act of 2001 Ausztrália: The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) EU: Third Anti-Money Laundering Directive (2005/60/EC) Magyarország: A pénzmosás megelőzéséről szóló 2003. évi XV. törvény	A különféle szabályozások elsősorban a pénzügyintézetek számára írják elő kontroll folyamatokat az illegális pénzmozgások, illetve illegális szervezetek támogatásának kiszűrésére.

kijavításáig közvetlen veszteséget volt kénytelen elszenvedni.

A működési kockázatok kezelésének feladatrendszerét hiba lenne önálló területként kezelni, hiszen jelentős átfedéseket mutat a szabályozási megfelelés, illetve a belső ellenőrzés területein túl más működési területekkel is. De ugyanígy hibás egyszerűsítés lenne a működési kockázatok kezelését ezen kiegészítő területek elvárásainak való megfelelésként értelmezni, és ezeknek teljes mértékben alárendelni.

Sőt, a tapasztalatok ugyanakkor azt mutatják, hogy a különféle szervezetek minden egyes szabályozási kihívásnak megfelelően egyedi, egymással nem összefüggő kockázatkezelési keretrendszert hoznak létre, miközben az egyes szabályozási elvárások igen sok átfedő elvárást fogalmazznak meg. Így például a Bazel II, SOX vagy Mifid szabályozások elvárásait egységes formában kezelve megtakarítható egyes folyamatok, tevékenységek megsokszorozása¹.

A szabályozásoknak való megfelelés ugyanakkor nem jelenti azt, hogy a szervezetek tudatosan ki is használják a működési kockázatok kezelésében rejlő lehetőségeket, inkább csak a szabályzó testületeknek való minimális megfelelésre törekcsenek. Miközben a szabályozások sokszor megelégednek a kockázatok azonosításával, és az azokra adott minimális válaszokkal, addig a tudatos működési kockázatmenedzsment lehetővé teszi a kockázatokra való felkészülést (nem csak a pénzügyi tartalékképzést), a kockázatok megelőzését, elhárítását, illetve a kockázatok realizálódásakor az azokra adható hatékony válaszleépések előkészítését is. A tudatos kezeléssel nem így nem csak elszenvedői, hanem irányítói is lehetnek a kockázatoknak.

A szervezeteket érintő veszélyeket egységes szemléletmód és keretrendszer szerint kell kezelni, még akkor is, ha az egyes kockázati területeknek megvannak a maga sajátosságai. Ugyanakkor az egységes kezelés éppen a szinergiák kinyeréséhez járulhat hozzá. További előnyök elérése érdekében meg kell teremteni a szoros kapcsolatot a belső ellenőrzés, kockázatkezelés, illetve szabályozási elvárásoknak való megfelelés között.

Működési kockázatok kezelése

Míg a területen élenjáró, sok tapasztalatot felhalmozó pénzügyintézetek esetében a működési kockázatmenedzsment feladatok elsődleges hajtóereje a tőkefe-

dezet képzés, illetve a szabályozásoknak való megfelelés biztosítása, addig más szervezetek esetében a kockázatok elhárítására és mérséklésére irányuló tevékenység kerül a fókuszba. Habár a pénzügyintézetek számára is előírás annak hitelt érdemlő bizonyítása, hogy a kockázatok elhárítására és mérséklésére kellő figyelmet fordítanak, ezen intézmények által választott módszerek mégis inkább a felmérésre és tőkefedezet képzésre koncentráltak - eddig alapvetően a múltra vonatkozó információk felhasználásával -, így ezen a területen még további fejlesztésekre van szükség.

Ráadásul a kockázatok azonosítása és kezelése során elsősorban a jól megfogható (hard) tényezőkre koncentrálnak, míg a puhább (soft) kérdésekkel nem foglalkoznak. Való igaz, hogy a szervezeti kultúrával, vagy a dolgozói motivációval sokkal nehezebb megküzdeni, sőt hosszabb időbe is telik, mint mondjuk egy informatikai szerver funkcionalitását katasztrófa esetében kiváltó hátterét létrehozni. Ugyanakkor a puha tényezők azonosításával és fejlesztésével nem csak hosszabb távú (tartósabb), de nagyobb mértékű eredmény is érhető el.

A kockázatok azonosítása során tehát a tevékenységek minden elemére figyelmet kell fordítani, beleértve a végrehajtó személyeket is, akik sokszor maguk is előidézői a veszteségeknek. Például egy olyan szervezet esetében, ahol a dolgozókra nagy munkateher és nyomás nehezedik, a túlhajszoltság miatt a dolgozók figyelmetlenebbé válnak, és hajlamosabbak hibák elkövetésére. De lehet kockázati ok egy olyan szervezeti kultúra is, ahol az előírások, szabályok tisztelete nem érték.

Tipikus eset, amikor közös irodaházban több cég is bérel irodát, és ez lehetőséget biztosít információk nem kívánt áramlására a vállalatok között. Egy hazai könyvelő cég hosszú időn keresztül tapasztalta, hogy bizalmas belső információk kerülnek ki, mi-

közben képtelen volt azonosítani a szivárgás forrását. Egy véletlen során fény derült arra, hogy az irodaház közös liftjében több vállalat alkalmazottai is utaztak, és a dolgozók az alagsori étkező felé igyekezve is tárgyalták az éppen aktuális feladatokat, illetve problémákat. Egy ilyen kis helységben akaratlanul is könnyű kihallgatni mások beszélgetését, és más cégek alkalmazottait semmilyen titoktartási szerződés nem korlátozza. A vizsgálat eredményeképp végül a dolgozók figyelmét felhívták arra, hogy a szakmai kérdéseket ne beszéljenek meg a liftben, főleg akkor ne, ha ismeretlen személyek is tartózkodnak benne.

A kockázatok azonosítása során a tevékenységek minden elemére figyelmet kell fordítani

A kockázatkezelési rendszer

A működési kockázatok tudatos kezelésének feltétele egy szervezeti kockázatkezelési rendszer létrehozása, melynek legfontosabb részeit tekintjük át a továbbiakban.

Kockázatkezelési stratégia². Ennek keretében meghatározásra kerül, hogy a kockázatkezelés során mely területekkel, milyen kockázatokkal kíván foglalkozni a szervezet (célok), ezek kezeléséhez milyen szabályok, eljárások és folyamatok tartoznak (eszközök). Szintén a stratégia szintjén kell meghatározni a szervezet kockázatokkal szembeni toleranciaszintjét.

Szervezeti megoldások. Annak meghatározása, hogy a kockázatkezelési stratégiában meghatározott célokat hogyan lehet támogatni a szervezetben kialakított kockázatkezelési egységekkel, feladatkörökkel, illetve szerepekkel, illetve, hogy mi a feladat- és hatásköre a szervezeti egységeknek.

Több szervezet külön kockázatkezelési hierarchiát alakított ki. Egy hazai bank esetében három kockázatkezelési szintet határoztak meg: az első szinten az üzleti és működési egységek feladata a működési folyamatok felmérése, és az azokhoz kapcsolódó ellenőrzési tevékenység kialakítása. A második szint a központi szabályozást és ellenőrzést végző szervezeti egységek alkotják, míg a harmadik szinthez a működéstől független belső ellenőrzés tartozik. A legnagyobb feladat a második szinthez kapcsolódik, ahol vizsgálják a szabályozási elvárásoknak való megfelelést (pénzmosás elleni törvény, Bazel-II, Mifid, stb.), a banki biztonsági, csalási kérdéseket, illetve az üzleti működés folytonosságának biztosítását is.

Beszámolók, mutatószámok. A kockázatok folyamatos figyelemmel kísérése érdekében el kell dönteni, hogy mely adatokat, milyen mutatószámokat kell vizsgálni, illetve a változásokról milyen gyakorisággal számoljanak be a kockázatkezelők a vezetésnek. Az egyes folyamatokhoz és tevékenységekhez kulcs kockázati indikátorokat (Key Risk Indicators – KRI) rendelhetünk, melyek változásából következtethetünk a veszélyeztetettség változására. Ilyen mutató lehet például a munkaerő fluktuáció aránya, ügyfélpanaszok száma, szolgáltatások rendelkezésre állása vagy akár a leltárveszteség értéke.

Kockázatkezelési megoldások. A kockázatok felmérésének, monitorozásának, értékelésének, illetve ellenintézkedések meghozatalának folyamatai, beleértve a közös értelmezési keret (nyelv) kialakítását, illetve a kockázatkezelési tevékenység kapcsolódási pontjait is. Ennek keretében szükséges a stratégia akciótervekre bontása, azaz, hogy a stratégiában meghatározottak közül milyen eszközöket lehet felhasználni a kockázatok mérséklésére, illetve kezelésére.

Informatikai támogatás. A kijelölt eljárásokat (melyek megfelelnek a stratégiai céloknak) megfelelő informatikai megoldásokkal szükséges, illetve lehet támogatni. Ennek elemei pl. a kockázatok nyilvántartására szolgáló eszközök, modellező eszközök, statisztikai eszközök, automatizációs eszközök, stb.

A kockázatkezelési rendszereknek jó alapot jelent a folyamat alapú megközelítés, mivel alkalmas arra, hogy tevékenység szinten azonosítsa a kockázati elemeket, illetve meghatározza az azokhoz kapcsolódó kontroll elemeket. Ez a megközelítés lehetővé teszi a kockázati stratégia részletes lebontását.

Kockázatok azonosítása és értékelése

A folyamat alapú megközelítés biztosítja, hogy mind az üzleti tevékenységek kiesésének kockázata, mint pedig a folyamatok mentén jelentkező kockázatok azonosíthatóak legyenek. Ezen megközelítés keretében a folyamatok leképezése jelenti az első lépést. Ekkor az egyes tevékenységekhez, az azokat elvégző személyekhez, szervezeti egységekhez, illetve a támogatást jelentő informatikai rendszerekhez kapcsolódóan határozhatóak meg a lehetséges kockázatok. Ez a megközelítés lehetővé teszi, hogy egy szervezet kijelölt folyamataihoz kapcsolódóan teljes körű kockázatfelmérés történjen.

Következő lépésben kerülhet sor a kockázatok mértékének, azaz a kockázatban szereplő esemény felmerülési gyakoriságának, illetve az általa okozott veszteség súlyosságának meghatározására. A folyamat alapú megközelítés esetében lehetőség van a kockázatok részletes dokumentálására, illetve a kockázatok változásának folyamatos átvezetésére is. Megjegyzendő, hogy habár e módszer a működési kockázatok kezelését támogatja a legjobban, a folyamatmodellhez kapcsolódóan más kockázatok is nyomonkövethetők.

Egy telekommunikációs cég a szerződéskötési folyamatának eredményeképpen magasnak ítélte meg a hibásan kitöltött iratok számát. A vizsgálat során kiderült, hogy a túlterhelt és sokszor formális képzés nélkül dolgozó alkalmazottak nincsenek tisztában az elvárásokkal, ezért – ha nem is szándékosan – sok hibát vétenek. A vizsgálat azt is kiderítette, hogy a szerződésminták, illetve a szerződések megkötését segítő informatikai rendszer sem nyújt megfelelő támpontokat a dolgozók részére. Ebben az esetben a folyamat részletes vizsgálata során azonosításra kerültek az erőforrások, és feltárhatóak voltak a kapcsolódó kockázatok. A szerződéskötési folyamat kapcsán kockázati tényezőként így azonosításra került az alkalmazottak megfelelősége, a szerződésminták megfelelősége, illetve a támogató informatikai rendszer is.

A kockázatok kezelésének egyik eszköze a folyamatok átszervezése és kockázatokhoz kapcsoló optimalizálása

Mivel a működési kockázatok sok helyen keletkezhetnek és különböző jellegűek lehetnek, ezért az elemzés elvégzéséhez nem csak a tevékenységek, hanem az azok végrehajtásához szükséges erőforrások felmérése is célszerű.

Folyamatok meghatározása. Az egyes tevékenységek sorrendiségének, kapcsolódási pontjaik és egymásra hatásának modellezése.

Szükséges technológia. A folyamatok végrehajtása során felhasznált technológiai megoldások, kiemelten informatikai rendszerek számbavétele, azok egymással való kapcsolata.

Szervezet. A szervezeti struktúra, a hierarchia, a szerepek, felelősségi és feladatkörök rögzítése. Kihívást jelent, hogy az emberek (dolgozók) és szerepek között többféle kapcsolat van, illetve kritikus a felelősségi körök egyértelmű kijelölése.

Dokumentumok, adatok. A folyamatok végrehajtása során keletkező és felhasznált dokumentumok, adatok és információk gyűjteménye.

A kockázatok nem csak a tevékenységekhez, folyamatokhoz, hanem magukhoz az erőforrásokhoz is kapcsolhatóak, így egy támogató rendszer működéséhez, egy dolgozóhoz (aki végrehajt egy feladatot), vagy akár egy papír alapú vagy elektronikus dokumentumhoz is. A kockázatok azonosítása során rögzíteni kell a kockázat típusát (működési, reputációs, piaci, stb.), a kockázat minőségi és mennyiségi értékelését, illetve ha rendelkezésre áll, akkor az ezen kockázathoz kapcsolódó korábban már felmerült veszteségek adatait.

Egy hazai bank– hasonlóan több pénzintézethez – a hitelezési folyamatainak átszervezésébe vágott bele. Mivel a pénzügyi válság miatt a hitelek kockázata megnövekedett, ezért azok elbírálási és jóváhagyási folyamata során is csökkenteni volt szükséges a működési kockázatokat. Ennek folyamán áttekintették a szükséges információkat, az érintett végrehajtókat, illetve úgy szervezték át a folyamatot, hogy annak végrehajtása során erősebb kontroll legyen gyakorolható.

Kockázatok kezelése

A kockázatok kezelésének egyik eszköze a folyamatok átszervezése és veszélyekhez kapcsoló optimalizálása. Ezzel a módszerrel a problémák akár el is tűntethetők a folyamatokból, illetve a működés logikájából adódóan mérsékelhetőek. A folyamatok

kockázati szempontú optimalizálása lehetővé teszi azt is, hogy átfogó jellegű kontroll folyamatokat határozzunk meg, melyek több kockázathoz, kockázatsoporthoz is kapcsolódnak.

Ezen tevékenység végrehajtása során építeni kell a folyamatmenedzsment általános alapelveire is, és a kockázatalapú szemlélet mellett a folyamatok átalakításakor figyelembe lehet venni az időbeli átfutásra, költségekre és minőségre vonatkozó lehetőségeket is. Ez ugyanakkor jelentősen megnöveli a folyamatfejlesztés végrehajtásának komplexitását és időbeli lefutását is.

Ezen a ponton kapcsolódik egymáshoz és mutat jelentős átfedést egymással a folyamat alapú kockázatmenedzsment, illetve a kockázatalapú folyamatmenedzsment koncepciója. Ebből adódóan a folyamat alapú kockázatmenedzsment megjelenhet különálló tevékenységként, de lehet egy szélesebb körű folyamatfejlesztési projekt része is, erőteljesen megjelenítve a kockázati tényező fontosságát az optimalizáció során.

A felmérés lehetővé teszi a megfelelő kockázatkezelési megoldások megtalálását. Elsődleges cél a kockázat csökkentése, vagy akár teljes elkerülése, melyre több megoldás is adódik.

Proaktív megközelítés. A kockázatcsökkentés egyik módja a bekövetkezési valószínűség csökkentése, mely tipikusan megelőző, többnyire védelmi megközelítések révén érhető el. Éppen ezért szükséges, hogy tisztában legyünk a várható kockázatokkal, hogy fel tudjunk rá készülni. Ennek leghatékonyabb módja a már bemutatott folyamat alapú kockázatfelmérés.

Reaktív megközelítés. Ebben az esetben nem a kockázat bekövetkezését, hanem egy esemény hatásának mérséklését állítják a középpontba, azaz azt vizsgálják, milyen intézkedések szükségesek, ha megtörténik egy esemény. Természetesen ennek is előfeltétele, hogy a kockázatok köréről valamilyen előzetes ismeretünk legyen.

Teljes elkerülés. Ez olyan megközelítés, mely során a szervezet lemond egy kockázatosnak ítélt tevékenység folytatásáról. Ez nem tekinthető a szó szoros értelmében kockázatcsökkentési módszernek. Azokban az esetekben, ahol a kockázat különösen nagy, vagy nagy gyakoriságú, ez az egyetlen lehetőség, mivel a kockázatkezelési megoldásokkal együtt sem valószínű, hogy megéri folytatni az adott tevékenységet.

Amennyiben más módszerekkel nem lehetséges a veszélyek további csökkentése, úgy még mindig lehetőség van a azok megosztására, mellyel mérsékelhetőek az esetleges veszteségek. Ennek egyik logikus módja a biztosítók bevonása (amelyek saját kockázatuk csökkentése érdekében elvárják a szervezetektől a kockázatmérséklési tevékenységet), illetve a kockázatos tevékenységek kiszervezése, alvállalkozók számára történő átadása (melyek a szolgáltatási díjba ugyan beépítik a kockázatok kezelését, de esetleg nagyobb speciális szakértelemmel rendelkeznek, kiszámítható költségért megbízhatóságot nyújtanak). Az informatikai kockázatok áthárításának jellegzetes megoldása az informatikai infrastruktúra üzemeltetésének kiszervezése, mely esetben a megbízó csak a szolgáltatásokért fizet, míg az infrastruktúrához kapcsolódó kockázatokat már a szolgáltató viseli.

A bemutatott nagyobb kockázatkezelési lehetőségek közül a nagyobb hatású kockázatok esetében több is alkalmazható: egy hazai központi állami hivatal működése szempontjából kritikusnak tekinthető az informatikai támogatás. A működési kockázatok kezelése érdekében azonosították az informatikai szolgáltatásokat, majd megállapították azok hatását a folyamatos működésre. A kockázatok elemzése után az egyes informatikai szolgáltatások, illetve az ezeket nyújtó IT megoldások prioritizálásra kerültek. A nagy kockázatú, de az ügyvitel szempontjából fontos rendszerek esetében többszintű kockázatkezelési megoldást is felhasználtak. A kockázatelemzés során a múltbéli tapasztalatokra alapozva, illetve a szakterületi dolgozók segítségével tárták fel a lehetséges fenyegetettségeket, melykehez meghatározták a lehetséges kezelési megoldásokat. Így például rendszerkiesés esetén a leállít informatikai szolgáltatások funkcionalitását más szerverek látják el. Egy esetleges szélesebb körű katasztrófa esetére pedig az adatokat külső adathordozóra mentik, melyeket külső telephelyen tárolnak. A kockázat megosztása érdekében több rendszer üzemeltetési feladatait meghatározott szolgáltatási szint szerződés (SLA) által szabályozva alvállalkozók látják el, melyek felelősek a rendszerkiesések által okozott károkért.

Természetesen mindig marad olyan kockázat, melyet egy szervezet viselni kénytelen, vagy azért, mert ebben az esetben nincs már mód arra, hogy a kockázatok bekövetkezését, vagy hatásukat egy szervezet hatékonyan csökkentse (pl. költség-haszon összevetés során lemond a csökkentésről), vagy pedig azért, mert a kockázatok mértéke az elviselhetőség határán belül van.

A kockázatkezelés során meg kell határozni megelőző lépéseket, amelyek szükségesek a kockázat felmerülésének elkerülésére, illetve amennyiben a kockázat mégis bekövetkezik, úgy azt, hogy milyen ellenintézkedéseket lehet tenni a kár mérséklésére. Nyilvánvalóan a kockázatkezelés előfeltétele, hogy a kockázatok ismerete.

A folyamat alapú kockázatfelmérés biztosítja a kockázatok felmérésének teljességét, és ezáltal a különböző kockázati kategóriák elkülönítését is. Ezáltal lehetővé válik annak vizsgálata, hogy a kisebb kockázatú események összességében milyen veszteséget jelentenek. A tárolt adatok köre lehetőséget nyújt a kockázatok összesítésére és mutatószám rendszerek kialakítására, ami lehetővé teszi a kockázatok folyamatos felügyeletét.

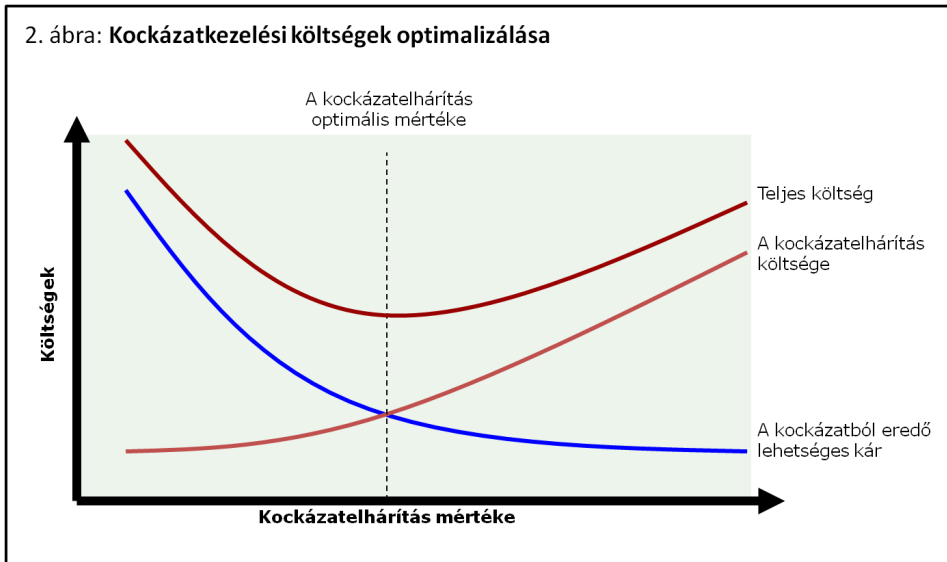
A kockázatok megismerése lehetővé teszi a kapcsolódó (lehetséges és megvalósuló) kontroll tevékenységek meghatározását. A kontroll tevékenység maga lehet egy egyszeri tevékenység, vagy egy teljes kontroll folyamatcsoport, mely akár több kockázathoz is kapcsolódik. Sőt sokszor magához a kontrollfolyamathoz is kapcsolódik kockázat, gondoljunk a Société Générale, vagy a Barings Bank esetére, ahol a kontroll tevékenységeket kijátszották a banki alkalmazottak.

Az informatikai rendszerekben indított tranzakciók folyamán már megszokott, hogy a sikeres, vagy éppen sikertelen végrehajtásról visszajelzést ad a rendszer. Ugyanakkor ennek a kontroll algoritmusnak a hibás működése hamis információkat is hordozhat magában, azaz például a rendszer sikeres végrehajtást jelez, miközben a tranzakció sikertelen volt. A hasonló problémák ellensúlyozására kritikus folyamatok esetében többszörös, független alrendszerek által végrehajtott ellenőrzést szoktak beiktatni.

Az atomerőművekben az több műszer is méri az egyes berendezések működését, melyek állapotát a vezérlőtermekben lehet leolvasni. Ez a kontroll biztosítja, hogy az ügyeletet ellátó döntéshozók folyamatosan teljes képet kapjanak az erőmű működéséről. Előfordulhat, hogy az egy kijelző rossz adatot mutat, mivel vagy az érzékelő, vagy pedig maga a kijelző elromlott. Egy rossz adat ismeretében hozott döntés súlyos következményekkel járhat. Az ilyen kritikus létesítményekben a hasonló hibák kezelését – mint kockázatkezelés – folyamatosan gyakoroltatják a dolgozókkal, így a megfelelő tapasztalattal rendelkező szakemberek a többi adat ismeretében felismerhetik a hibás jelzéseket, és ennek kontrollálását kérhetik a műszer személyes vizsgálata által.

A folyamat alapú kockázatkezelés elképzelhetetlen a megfelelő támogatást jelentő informatikai megoldások nélkül

2. ábra: Kockázatkezelési költségek optimalizálása



Az ellenőrzések esetében törekedni kell arra, hogy ezek megelőző, mintsem reagáló jellegűek legyenek, illetve lehetőség szerint automatikusan működjenek, azaz a legkevesebb teret adjuk az emberi tényezőnek. Ez utóbbi elvárás megköveteli, hogy az egyes folyamatokat aktív ellenőrzést biztosító folyamatmenedzsment rendszer (pl. workflow) támogassa.

A kockázatok azonosítása és nagyságuk meghatározása teszi, hogy eldöntsük, mely kockázatok kezelésére érdemes erőfeszítéseket tenni: amennyiben a kockázatkezelés költsége meghaladja a kockázatból adódó veszteség költségét, úgy nem éri meg a megelőző tevékenységek végrehajtása.

Mivel ellenintézkedések, vagy kontroll folyamatok nem csak egyes egyedi kockázatokhoz, hanem kockázatok csoportjához is tartozhatnak, ezért a kockázatkezelési költségeket is érdemes hasonló logika mentén csoportosítva értékelni. Összességében azt az optimális pontot kell megtalálni, ahol a kockázatkezelési költségek, valamint a kockázatokból eredő veszteségek együttes értéke minimális. E mérlegelés előfeltétele az, hogy már előzőleg megtörténjen a kockázatok, és azok jellemzőinek – a folyamatokhoz kapcsolódó – felmérése, illetve a lehetséges kezelési eljárások ismertek legyenek. (Lásd: *Kockázatkezelési költségek optimalizálása* c. ábra).

Egy folyamatra épülő működési kockázatokat kezelő rendszer kiépítése korántsem egyszerű folyamat. A folyamat alapú kockázatkezelés megvalósítása ugyanakkor elképzelhetetlen a megfelelő támogatást jelentő informatikai megoldások nélkül: a folyamatok nagy száma, azok bonyolultsága, illetve így a kapcsolódó lehetséges kockázatok nagy száma átláthatatlan lenne a megfelelő eszközök segítségével. A támogató eszközök felhasználása ugyanakkor egyszerűsíti, áttekinthetővé és kontrollálhatóvá teszi mind a szervezeti folyamatokat, mind pedig a kapcsolódó kockázatok és kontroll tevékenységeket.

A szabályozási területek fejlődésével egyre több szervezetnek kell figyelembe venni a szabályozási kérdésekből adódó kockázatokat, és a kapcsolódó kockázatmenedzsment feladatokat. Itt kiemelten gondolhatunk az Euro-SOX néven említett EU direktívára, melynek széles körű elterjedése már 2-3 éven belül várható, és a szervezetek széles körére vonatkozik.

Az szabályozásoknak való megfelelés megköveteli a folyamat alapú kockázatmenedzsment és kontroll tevékenységek kidolgozását, mely egyben

lehetőséget teremt a folyamatmenedzsment nyújtotta lehetőségek szélesebb körű kihasználására is, úgy mint a folyamatoptimalizálás, teljesítménymenedzsment, folyamatkontroll, vagy költségmenedzsment. Ezen feladatok megvalósítása ugyanakkor komplex, idő és költségigényes feladat, mely hatékony informatikai támogatást igényel.

Az újabb szabályozási elvárásoknak való megfelelést a szervezetek gyakran projektszerűen vizsgálják, miközben a kockázatmenedzsment tevékenységet folyamatos, napi feladatként végzik, és lehetőség szerint automatizáltan. Sajnos kevésbé automatizálható, de hasonlóan fontos feladat a szabályozási környezet változásainak folyamatos elemzése, és a működési gyakorlatban való megjelenítése.

A folyamat alapú kockázatelemzés segítséget nyújt mind a változó kockázatok folyamatos figyelemmel kísérésére, mind pedig a változó szabályozási elvárásoknak való megfelelés ellenőrzésére. Figyelembe véve a folyamatmenedzsmentre épülő kontrollálhatósági és átláthatósági előnyöket a szervezeteknek célszerű kialakítani a saját folyamatmodelljeiket. ■

¹ A vállalatok vezetőinek egyre növekvő számú szabályozási elvárásnak kell megfeleltetniük a szervezet működését. Az aktuális szabályozásokhoz, illetve ezek egységes kezeléséhez kapcsolódik: Tarantino, A.: *Manager's Guide to Compliance* (John Wiley and Sons, Hoboken, 2006)

² Ilyen kockázatkezelési keretrendszert hozott létre az IT Governance Institute a Bazel-II elvárásrendszer támogatására, melynek elemei között szerepel a kockázati stratégia, szervezet, beszámoló, technológia, veszteségadatok gyűjtése, indikátorrendszer, tőkemodelllezés, és kockázatkezelési megoldások. *IT Control Objectives for Basel II*. (IT Governance Institute, 2007)

³ A csalásból származó hírverés jól használta ki Nick Leeson. Nevéhez az általa okozott csaláshoz kapcsolódóan két könyv, számtalan szakkikk kapcsolódik, és szabadulása után igen jól megél előadókörútjaiból, ahol elmeséli, hogyan is sikerült a csalást végrehajtania, illetve mit is kell tenni a hasonló csalások megelőzése érdekében. Ajánlott olvasmány: Leeson, N: *Rogue Trader: How I Brought Down Barings Bank and Shook the Financial World* (Little Brown and Company, 1999)