FÁBIÁN ZOLTÁN, minőségirányítási vezető, Szegedi Tudományegyetem
HORVÁTH ZSOLT, ügyvezető igazgató, INFOBIZ Kft.

Egészségügyi intézmények integrált kockázatfelmérése és kezelése IT támogatással

Az egészségügyben több mint 20 éve követelmény belső minőségbiztosítási rendszer alkalmazása. Az intézmények többsége ezt praktikusan az ISO 9001 szabvány (és/vagy a MEES) alkalmazásával oldja meg. A szabvány 2015-ös kiadása már egyértelműen kockázatalapúnak tekinthető, emellett egyre inkább terjedőben van az integrált rendszerek alkalmazása is, amely során további szabványosított kockázatalapú irányítási rendszerek jelennek meg a szervezetek működésében. Az integrált rendszer valamennyi eleme előírja a kockázatok felmérését és kezelését, amelyet a szervezetek hierarchikus felépítése és a működtetéshez szükséges különböző szakmai kompetenciák miatt általában külön kezelnek. A kockázatok pontos azonosítása, jól megtervezett és összehangolt kezelése egyrészt pénzügyi szempontból is megtakarítást jelenthet a szervezeteknek, másrészt hatékonyabbá teheti magát a kockázatok kezelését.

A kockázatok egységes, holisztikus megközelítése segít meghatározni a vállalható maradék kockázatok szintjét, ami a szűkös erőforrások miatt óriási támogatást jelent a felső vezetésnek a döntések meghozatalában. Jelen publikációnkban a kockázatok azonosításának, elemzésének és értékelésének egységes, IT eszközzel támogatott gyakorlatára mutatunk be egy egészségügyi intézmény viszonyaira felépített példát.

1. Bevezetés

Az egészségügyi ellátó intézményekre – különösen a nagyobb állami tulajdonú intézményekre (pl. megyei kórházakra vagy klinikákra) – számos külső jogszabály vagy egyéb külső elvárás ír elő egyszerre kockázatfelmérésre és kockázatkezelésre vonatkozó követelményeket. A nagyobb ilyen követelményrendszerek a következők:

- Az egészségügyi intézményektől elvárt, hogy minőségirányítási rendszerük legyen és az alapján dolgozzanak. A legtöbb egészségügyi intézmény ezért is alapként használja az ISO 9001 szerinti általános minőségirányítási rendszert, amelynek jelenleg érvényes verziója – az ISO 9001:2015 [1] – átfogó kockázatalapú gondolkodást ír elő. Ez a szabvány számos elem megvalósításakor és fejlesztésekor a kockázatalapú döntés-előkészítést várja el. Itt a kockázatokkal való foglalkozás átfogó és a teljes vállalati / szervezeti működés kockázatairól és a működésre ható külső kockázatok menedzseléséről szól.
- Az egészségügyön belül általánosan elterjedt, és szinte kimondatlanul is minőségügyi elvárás a Magyar Egészségügyi Ellátási Standardok (MEES) használata, amely szintén erősen kockázatok felmérésére és kezelésére épül. Itt kockázatként a betegkockázatokon van a fő hangsúly, azon belül is a kezelések sikerességének és a betegek gyógyulásának, illetve az ellátás során történő esetleges további fertőzések vagy betegségek kockázatainak vonatkozásában.
- A minőségirányítási rendszer szabványának az európai szintű egészségügyi kiterjesztését az EN 15224:2017 [2] szabvány tartalmazza, amely – megfelelve az annak alapját képező ISO 9001:2015-nek – szintén erős kockázatalapúságot és kockázatok felmérésére és kezelésére vonatkozó követelményeket állít.
- A szervezetek a működésük során számos adatot, köztük számos személyes adatot is kezelnek. Az egészségügyi ellátó intézmények legfőbb ügyfelei a „betegek", akiknek mind az egyéni azonosító adatai, mind a betegségükkel összefüggő összes adata is kezelve vannak, amelyek mind ún. különleges személyes adatok, azaz a jogszabály szerint szigorúbb védelmet élveznek. Az EU általános adatvédelmi rendelete (a GDPR) [3] és annak magyar hazai jogszabálya, a 2011. évi CXII. törvény (az ún. info tv.) [4] előírásait a személyes adatok kezeléséről itt is szigorúan be kell

tartani, amely szintén tartalmazza az adatok kezelése és biztonsága kockázatainak felmérését és kezelését.

- Az egészségügy Magyarországon az egyik kiemelt kritikus infrastruktúra ágazat. Ennek keretében az egészségügyi ellátás néhány kiemelt része a központi betegellátást és adatkezelést megvalósító egészségügyi informatikai rendszer kritikus infrastruktúra (azaz más szóval létfontosságú rendszer vagy létesítmény) besorolású. Ezek működtetésére és fenntartására külön jogszabály, a létfontosságú rendszerek és létesítmények védelméről szóló 2012. évi CLXVI. törvény [5] rendelkezik, amely a védelmet szigorúan kockázatalapra helyezi. Külön kiemelendő a kijelölt létfontosságú létesítményeket üzemeltető informatikai rendszerek szerepe, amely ilyen módon kritikus informatikai infrastruktúrának minősül, és ezek informatikai és kiberbiztonságát az állami és önkormányzati szervek információbiztonságáról szóló 2013. évi L. törvény (az ibtv.) [6] alapján kell meghatározni és végrehajtani. Természetesen ez itt külön meghatározott: az informatikai biztonsági kockázatok felmérése és kezelése alapján elvárás a megfelelő biztonsági intézkedések bevezetése.
- A költségvetési szervek belső kontrollrendszeréről szóló 370/2011-es Kormányrendelet [7] a költségvetési szervek teljes működését lefedő, integrált kockázatkezelési rendszer bevezetését és használatát írja elő a szervezeti célokkal összefüggő kockázatok kezelésére.
- Azokban az intézményekben, amelyekben a működésük során egyéb irányítási rendszereket (pl. környezetközpontú irányítási rendszer, munkavédelmi és egészségbiztonsági irányítási rendszer, információbiztonsági irányítási rendszer, energiaközpontú irányítási rendszer) vezettek be, tartanak fenn és tanúsítanak, mindegyik ilyen irányítási rendszer keretén belül a hozzá tartozó kockázatokat folyamatosan kell felmérni és kezelni, majd követni és szükség esetén javítani.

Ezeknek a követelményeknek jó része valamely szempontból egymástól eltérő, ugyanakkor ezek közt számos átfedés is található. Különbségek láthatók mind a kockázatok előfordulása, mind a kockázatok hatásának jellege és területe (pl. kárjelleg) tekintetében is.

De alapvetően mindegyik külön elvárás, amelynek – ha egyáltalán van – ellenőrzése is külön-külön történik, más és más számonkérés keretében. Így jellemzően a szervezetek (amelyek egyáltalán foglalkoznak ezeknek a követelményeknek való megfeleléssel) mindegyik követelmény teljesítésére külön-külön eljárásokat és dokumentációs rendszereket tartanak fenn. A működésre vonatkozó átfedések miatt így megsokszorozódik a redundáns munkavégzés, nem is beszélve a különböző követelményrendszerhez tartozó, de tartalmában ugyanarra vonatkozó kockázatok eltérő elemzéséről és értékeléséről. Ez ilyen formában irreálisan nagy terhet ró az egészségügyi intézményekre.

Jelen publikációban bemutatunk egy módszertant, amivel alapvetően a működési, a működéssel összefüggő és abból eredő kockázatok egységesen, egy logikai rendszerben kezelhetők. Ez a módszer a szervezet (egészségügyi ellátó intézmény) működési modelljéből vezeti le a lehetséges kockázati forrásokat, határozza meg egységesen a lehetséges különböző jellegű kárhatásokat, és egy egységes értékelési és skálázási rendszeren belül egységesen becsüli meg a különböző fajta kockázatok kockázati értékeit. A publikációban bemutatjuk így a működési-, a folyamat-, a munkavédelmi-, a humán erőforrások és az egyéb erőforrások általi, a pénzügyi-, a betegbiztonsági-, a személyes adatvédelmi-, az információbiztonsági- és egyéb hasonló kockázatok egységes azonosítását és kezelését.

Ebben a modellben nem térünk ki többek közt a stratégiai és a pénzügyi likviditási kockázatok, illetve a projektkockázatok stb. elemzésére.

A publikációban bemutatunk egy magyar informatikai eszközt, az ADAPTO[1]-t, amelynek segítségével ezeket a felméréseket egy relációs adatbázis-alapú rendszerben felvehetjük és rugalmasan kezelhetjük. Nem célunk konkrét intézmény bemutatása, hiszen a benne lévő adatok bizalmassága miatt az eredmények amúgy sem lennének publikációra alkalmasak.

Ehelyett szakértőkkel konzultálva felépítettünk egy Minta-Kórházat, és annak kapcsán vizsgáltuk az eredményeket. A publikációban

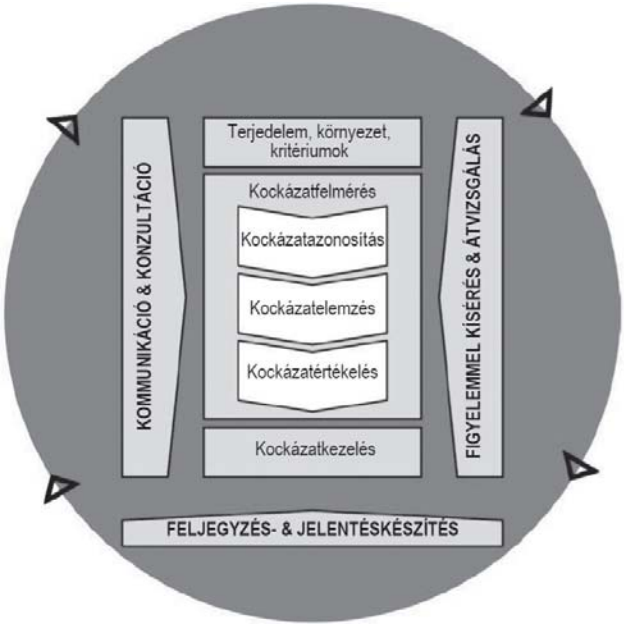
[1] Az ADAPTO szoftver az ADAPTO Solutions Kft. terméke, amelynek fő célja a vállalatirányítás támogatása folyamatalapú integrált kockázatmenedzsment modellezésen keresztül, azonban számos más támogató funkciót is tartalmaz. Információk találhatók erről a https://adapto.hu oldalon.

bemutatott adatok is ennek a Minta-Kórháznak az alapján készültek. Célunk nem az abszolút pontosság volt, hanem egy elképzelhető életszerű példán a módszer működését gyakorlati oldalról bemutatni! A kidolgozott modell alapját Falusi Tímea az Óbudai Egyetemen 2016-ban készített szakdolgozata [8] szolgáltatta.

2. Az alapok megértése

A különböző kockázatok meghatározására, azaz amíg eljutunk a kockázat felismerésétől és azonosításától a kockázati érték meghatározásán át addig a döntési pontig, hogy azt kell-e kezelnünk és hogyan, kockázati területenként és típusonként számos különböző módszer és gyakorlat alakult ki. Ezek a különböző módszerek mégis mind beilleszthetők egy egységes keretrendszerbe, ahol a fő logikai lépések mind azonosak és felismerhetők. Ezt a logikai keretrendszert, mint a kockázatok menedzselésének életciklusát mutatja be egységesen az ISO 31000:2018 szabvány [9].

Ez a szabvány a kockázatmenedzsment folyamatának életciklusát a következő lépésekre bontja (1. ábra), amely lépések egyaránt felismerhetőek minden fajta kockázat felmérésével és kezelésével foglalkozó folyamatban. Természetesen a különböző kockázati területeken kialakult különböző módszereknél ezeknek a lépéseknek a megvalósítása más és más, azonban az egyes lépéseknek mindegyik esetben meg kell történniük és beazonosíthatónak kell lenniük.



1. ábra: A kockázatmenedzsment-folyamat életciklusának lépései az ISO 31000:2018 szabvány szerint

Az alapvető lépések a kockázatfelmérés során [10] a következők:

- a kockázatok azonosítása, azaz annak verbális meghatározása, hogy milyen kockázati események következhetnek be, amelyek hatással vannak a meghatározott céljainkra és a kockázati események meghatározásakor jellemezzük annak bekövetkezési mechanizmusát, valamint a lehetséges hatásokat is;
- a kockázatok elemzése, azaz annak számszerűsítése vagy legalábbis becslése, hogy az egyes kockázati események mekkora kockázati potenciált jelentenek a szervezetek számára; a cél az, hogy az egyes kockázati események a szervezetek szempontjából mért jelentőségük alapján egymással összehasonlíthatóak legyenek;
- a kockázatok értékelése, azaz a már kockázati potenciálokkal meghatározott kockázati események elfogadását, azaz az intézkedési szükségesség meghatározását jelenti.

A kockázatok kezelése során – még ha az elnevezés vagy terminológia néha különbözik is egymástól, – de jellemzően mindig ugyanazok a lehetőségek kerülnek elő: a kockázatok felvállalása, a kockázatok áthárítása, a kockázatok elkerülése, illetve leggyakrabban intézkedések bevezetése a kockázatok csökkentésére. (Megjegyzendő, itt most azokat az eseteket tárgyaljuk, ahol tipikusan a kockázatok mind valamilyen veszélyt, azaz negatív kockázatot jelentenek.)
Amennyiben ugyanaz a szervezet egyszerre különböző kockázati területhez tartozó kockázatokat kezel egyidejűleg, és azokat a kockázatokat egymástól függetlenül más és más személy felelősségi körére bízva, azok egymástól teljesen függetlenül mérik fel és kezelik, jellemzően a következő problémák áll(hat)nak fenn:

- a különböző, alkalmazott kockázatfelmérési (azonosítási, elemzési és értékelési) metodikák miatt az eredmények nem lesznek szervezeti szinten összehasonlíthatóak, összemérhetőek;
- miután ugyanazon kockázati forrásoknak (kiindulási kockázatot generáló eseményeknek) egyszerre többféle hatása is lehet, amelyek különböző kárjelleget jelentve különböző kockázati területhez – azaz más és más felelős szakterületéhez – tartozhatnak egyszerre, azok

felmérése és jellemzése egyrészt párhuzamosan megjelenik több helyen, viszont az eltérő metodikák miatt ugyanannak az elemzése teljesen eltérhet egymástól.

Ezek a veszélyek egyrészt többszörös redundanciát (többletmunkát) jelentenek, másrészt viszont a nem egységes kezelés miatt számos belső ellentmondást és hibalehetőséget is.

Az általunk alkalmazott módszer esetében egy egységes azonosítási, elemzési és értékelési módszert alkalmazunk és ebben vesszük figyelembe a különböző kockázati források esetén létrejövő, különböző kárjellegek általi hatások egységes szempontrendszer szerinti összemérhetőségét. Ez biztosítja, hogy a különböző jellegű kockázatoknak az egész szervezetre kifejtett kockázati mértéke egymással összevethető legyen. Az alkalmazott módszertan nagyon erősen épül a felhasznált informatikai támogató eszköznek, az ADAPTO-nak a működési filozófiájára.

A kiindulást a szervezet működési folyamatmodellje adja, amit a szervezet működése alapjának tekintünk. Itt fel kell venni a szervezet szervezeti felépítését, folyamatait (folyamatkapcsolatokkal), a folyamatok különböző jellegű erőforrásait, ki- és bemeneteit és természetesen ezek kapcsolatait (lásd 2. ábra).

A szervezet működése a folyamatok működéséből áll össze, és a szervezet működésének jóságát a folyamatok működésének jósága adja. Ha egy folyamatalapú szervezet működésében kockázatok lépnek fel, akkor azok – feltéve hogy a folyamatok kapcsolatai és szabályozásai megfelelően lettek kialakítva, – a folyamatok működése során jelennek meg. Problémák (kockázati források) jelenhetnek meg közvetlenül a folyamatok lépéseinek végrehajtásában, de kockázati forrást jelenthet bármely folyamat-erőforrás hiánya, nem megfelelő működése, vagy nem megfelelő bemeneti követelmény teljesülése is. Viszont amennyiben ezek egy egységes rendszerben vizsgáltak, akkor ezek a kockázati források egységesen határozhatók meg, és rendelhető hozzájuk azok jellemző bekövetkezési valószínűsége. A lehetséges kárhatások is lehetnek különbözők, ahol a különböző kárjellegek összehasonlítását egy ún. kárérték-kárjelleg mátrixban táblázatos formában (lásd 3. ábra) lehet szervezet-specifikusan felvenni [11].

2. ábra: Az ISO 9001 szerinti folyamatmodell

A működési és azzal kapcsolatos kockázatok azonosítására és elemzésére az ún. CRAMM módszert használtuk. A CRAMM módszer vagy más néven CRAMM támadási modell az

Kárjellegek | Hatásszintek | Kárérték osztályok

[Összesen: 5 találat] 1 - 5

	Jelentéktelen	Csekély	Közepes	Nagy	Kiemelkedően nagy	Katasztrofális
Közvetlen anyagi kár	10.000,- Ft alatti kár	100.000,- Ft-ig terjedő kár	1.000.000,- Ft-ig terjedő kár	10.000.000,- Ft-ig terjedő kár	100.000.000,- Ft-ig terjedő kár	100.000.000,- Ft-ot meghaladó kár
Közvetett anyagi	a kár 1 embernappal állítható helyre	a kár 1 emberhónappal állítható helyre	a kár 1 emberévvel állítható helyre	a kár 1-10 emberévvel állítható helyre	a kár 10-100 emberévvel állítható helyre	a kár több mint 100 emberévvel állítható helyre
Társadalmi-politikai, humán	nincs bizalom vesztés, a probléma a szervezeti egységen belül marad	kínos helyzet a szervezeten belül	bizalomvesztés a tárca középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel	bizalomvesztés a tárca felső vezetésében, a középvezetésen belül személyi konzekvenciák	súlyos bizalomvesztés, a tárca felső vezetésén belül személyi konzekvenciák	súlyos bizalomvesztés, a kormányon belül személyi konzekvenciák
Jogsértés	nem védett adat bizalmassága vagy hitelessége sérül	hivatali, belső (intézményi) szabályozóval védett adat bizalmassága vagy hitelessége sérül	személyes adatok bizalmassága vagy hitelessége sérül, egyéb jogszabállyal védett (pl. üzleti, orvosi) titok bizalmassága vagy hitelessége sérül	szolgálati titok bizalmassága vagy hitelessége sérül, szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül, banktitok, közepes értékű üzleti titok bizalmassága vagy hitelessége sérül	katonai szolgálati titok bizalmassága vagy hitelessége sérül, államtitok bizalmassága vagy hitelessége sérül, nagy tömegű szenzitív személyes adat bizalmassága vagy hitelessége sérül, nagy értékű üzleti titok bizalmassága vagy hitelessége sérül	különösen fontos (nagy jelentőségű) államtitok bizalmassága vagy hitelessége sérül
Személyi sérülés, haláleset	testi épség jelentéktelen sérülése egy-két személynél	könnyű személyi sérülés egy-két személynél	több könnyű vagy egy-két súlyos személyi sérülés	több súlyos személyi sérülés vagy tömeges könnyű sérülés	egy-két személy halála vagy tömeges sérülések	tömeges halálesetek

3. ábra: Példa egy kárérték-kárjelleg mátrixra

információbiztonsági / informatikai biztonsági gyakorlatban általános ismert és bevezetett kockázatfelmérési módszer. A CRAMM támadási modell a Central Computer and Telecommunation Agency (Egyesült Királyság) által kidolgozott kockázatelemzési és kezelési módszertan. A mozaikszó a „CCTA Risk Analysis and Management Method" kezdőbetűiből adódik.

A CRAMM módszer vagy más néven a CRAMM támadási modell lényege, hogy a kockázatokat fenyegetések okozzák, amelyek kihasználják a sebezhetőségeket, aminek következtében biztonsági események következnek be, amelyek kárt okoznak vagyontárgyakban, és ennek hatása lesz a tulajdonosra nézve. Ez a megközelítés azt jelenti, hogy a biztonsági esemény bekövetkeztéhez három dolog szükséges:

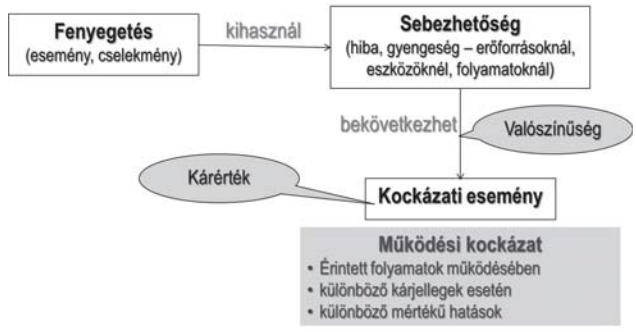
- **cél**, amiben/amivel kárt lehet okozni,
- **sebezhetőség**, amin keresztül a fenyegetés kifejti a hatását (vagy amin keresztül a támadás megindítható), ez lehet magában a védelemben is, és
- maga a **fenyegetés**.

Az informatikai/információbiztonsági kockázatok esetén ez szinte magától értetődő, hiszen ott:

- a cél a védendő információ biztonságának (bizalmasságának, integritásának, rendelkezésre állásának) sérülésén keresztüli károkozás a vállalatnak,
- a fenyegetés az a lehetséges bekövetkezhető esemény, cselekvés (vagy annak hiánya), amelyek bekövetkezésén keresztül az adott információ biztonsága sérülhet,
- a sebezhetőség pedig azon folyamatok, információ-feldolgozó eszközök és rendszerek, adathordozók illetve egyéb erőforrások gyenge védelme, nem megfelelő működése, amely az adott fenyegetés bekövetkezését lehetővé teszi, és ezáltal az adott információ biztonsága sérülhet.

Ez a logika azonban teljes mértékben áttehető és alkalmazható közvetlenül a folyamatok direkt kockázataira, és így más jellegű kockázatok felmérésére is.

Tehát folyamatkockázatokra, működési kockázatokra értelmezve is használhatjuk közvetlenül ezt a logikai gondolatmenetet (lásd 4. ábra.):



4. ábra: A CRAMM modell kockázati hatásmechanizmus megközelítése

Ha működési kockázatok vizsgálata esetén folyamatonként számba vesszük a lehetséges kockázati forrásokat és azok lehetséges kockázati eseményeit, hatásait, amelyek előfordulhatnak a folyamat lépéseihez, adataihoz, eszközeihez vagy egyéb erőforrásaihoz kötötten, akkor felfedezhetjük azonnal ezeket az elemeket. Hiszen a kockázati forrás nem más, mint valamely lehetséges esemény, cselekmény (vagy annak elmulasztása) – azaz mint lehetséges fenyegetés – bekövetkezése, ami azért tud bekövetkezni, mert valamely folyamatlépés, eszköz, erőforrás, stb. nem megfelelően működik vagy nem kellő a védelme az adott fenyegetéssel szemben, tehát sebezhető. Ezt az adott fenyegetés ki tudja használni, és emiatt a bekövetkező kockázati eseménynek hatása lesz valamely célunkra, kárt okoz nekünk.

Az okozott kár jellegénél fogva lehet

- közvetlen anyagi kár (pl. a mindenkori amortizált értékkel, az elmaradt haszonnal vagy a kifizetendő büntetéssel arányos);
- közvetett anyagi kár (pl. a helyreállítási költségekkel, perköltségekkel arányos);
- adatszivárgás (pl. betegek vagy más kórházi személyek adatainak kiszivárgása, kompromittálódása, esetleg az intézmény gazdasági-működési adatainak illetve személyzete személyes adatainak kiszivárgása és ezzel visszaélés);
- egészségi állapot romlása (pl. egészségi állapot különböző szintű vagy maradandó romlása, haláleset);
- kórházi fertőzés (pl. ellátás során fertőzés(ek) fellépése);
- üzemszünet (pl. informatikai vagy egyéb infrastrukturális – vagy más, pl. személyi – okok miatt a betegellátás működtetése,

folyamatai rövidebb-hosszabb ideig szünetelnek vagy leállnak, azok feltételei nem biztosítottak);
- programhiba (pl. a szoftverek hibája, hiányossága miatt hibás jelentések, dokumentumok készülnek, és bizonyos szükséges programfunkciók nem elérhetőek, ez a gazdasági folyamatokat biztosan, de akár a betegellátási folyamatokat is akadályozhatja közvetve.)
- környezeti hatás (pl. környezetre gyakorolt jelentős szennyezői hatás)

Látható, hogy egyidejűleg felmérhetők és kezelhetők ezzel a módszerrel mind a betegellátáshoz kapcsolódó jellemző egészségügyi betegkockázatok, de az intézmény működtetésével kapcsolatos kockázatai, környezetvédelmi kockázatai, informatikai és informatikai biztonsági kockázatai, személyes adatvédelmi kockázatai, kapcsolódó jogi kockázatai és ezek következtében a szervezet működésére ható közvetlen és közvetett pénzügyi kockázatai is. A kárjelleg típusokat és azok skálázását az adott alkalmazásban mindig a vizsgált szervezet (jelen esetben kórház) működéséhez illesztve, arra jellemző módon lehet és kell felvenni.

A bemutatott modell vizsgálatban nem volt célunk az ADAPTO minden funkcióját és lehetőségét bemutatni, hanem inkább egy szemléletes áttekintést szerettünk volna nyújtani kórházi környezetben az integrált kockázatok kezelésének számítógéppel támogatott lehetőségeiről.

3. A BIA modul felvétele

A) A modell-kórház felépítése

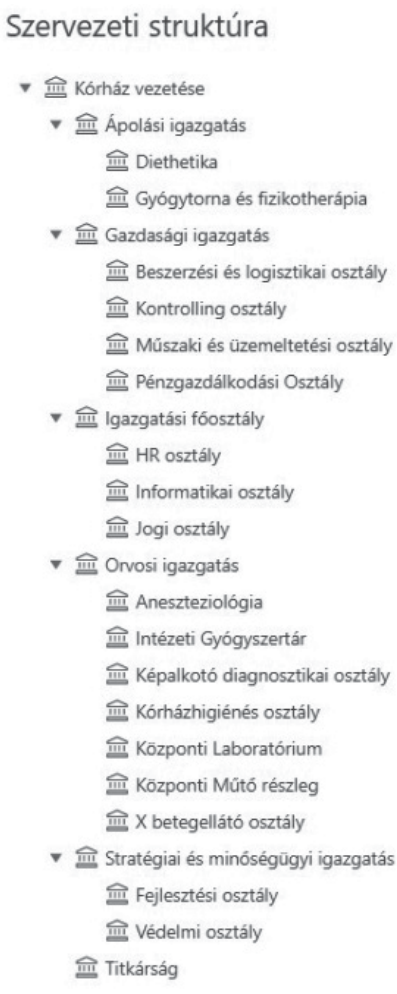
A kockázatok felvételének alapja, hogy a kockázatok hol jelennek meg és hol hatnak, azaz a szervezet folyamatalapú működési modellje. Ezt a funkciót, azaz a szervezet működési modelljének a leképezését tartalmazza az ADAPTO termék BIA[2] modulja.

A példánkban választott minta-kórház nagyságában és működési jellegében megfelel egy magyarországi állami megyei nagykórháznak, amelynek a teljes alkalmazotti állománya több mint 500 fő, és a fekvőbeteg részen is sokszor 600 – 1000 ágyat foglalnak el a betegek. Ahhoz, hogy a modellt minél általánosabban használhassuk, több szempontot is figyelembe véve kellett meghatároznunk az optimális megoldást. Mivel a szervezési szempontok szerinti csoportosításban a hagyományos osztályszerű működés elterjedtebb és talán egyszerűbben kezelhető, mint a mátrixszerű működés, így az utóbbi sajátosságait nem vettük figyelembe. Ugyanakkor a szervezet méretének növekedése is negatívan hat az átláthatóságra, másrészről a kisebb kórházak, illetve egyes szakmák hiánya jelentősen ronthatja a minta-kórház általános modellként történő használhatóságát. További szempont a kórház felépítése: itt az egy telephely mellett döntöttünk, ugyanakkor a tömbkórház és a pavilonrendszerű infrastruktúra közül ez utóbbit választottuk, mivel így karakteresebben jeleníthetők meg a logisztikai és szállítási kockázatok.

A minta-kórház egyszerre lát el járóbeteg-ellátási feladatokat (ambulanciák) és fekvőbetegellátási feladatokat is. A kórháznak saját laborjai (pl. laboratóriumi medicina, mikrobiológia, citológia) vannak. Ezeket egy központi laboratóriumban vontuk össze, mint ahogy a képalkotó diagnosztikai egységeket is (pl. Rtg, CT, MR stb.), amelyek kiszolgálják a különböző kórházi betegellátó osztályokat. A betegellátó osztályokat a példában egyszerűen csak „X betegellátó osztálynak" vettük fel (az „X" jelen esetben bármely szakmacsoportot jelölheti, éles alkalmazásnál természetesen mindet külön kell felvenni). Megjelenhetnek kapcsolódó kezelések és ápolások is (pl. a gyógytorna, fizikoterápiás kezelések) és egyéb speciális beteg-tanácsadások (pl. dietetikai). A kórházhoz tartozik egy saját önálló gyógyszertári részleg is. A minta-kórház működését saját kiszolgáló egységek támogatják. Ennek megfelelően szervezeti ábrájának egyszerűsített felépítése az 5. ábrán látható.

Összefoglalva: a rendszer kialakításánál minta-kórházként egy pavilon rendszerű, egytelephelyes, teljes szakmai spektrumú és teljes diagnosztikával (laboratóriumok és képalkotó) rendelkező, kb. 1000 ágyas intézményt specifikáltunk. Ennek megfelelően épül fel a szervezet folyamatstruktúrája is, ahol a folyamatok besorolhatóak „igazgatási, irányítási folyamatok"-ba, „támogató folyamatok"-ba illetve „üzleti, működési folyamatok"-ba. A folyamatoknak sok esetben van meghatározott egymásutánisága, kapcsolata.

[2] BIA – Business Impact Analysis / üzleti hatáselemzés – modul



5. ábra: A minta-kórház egyszerűsített sematikus szervezeti felépítése

Értelemszerűen az üzleti, működési folyamatok a főtevékenységek, azaz a betegellátás és ápolás tevékenységeit jelentik. A főfolyamatok közül néhányat főfolyamat-csoportba (vagy más néven teljes üzleti folyamatba) rendeztünk. Ilyen teljes üzleti folyamat tevékenységei például:

Teljes üzleti főfolyamat – fekvőbeteg-ellátás – tevékenységei:

- fekvőbeteg előjegyzése,
- fekvőbeteg felvétele,
- fekvőbeteg vizsgálata,
- fekvőbeteg kezelési terv készítése,
- fekvőbeteg gyógykezelése,
- fekvőbeteg ápolása és ellátása,
- fekvőbeteg elbocsátása.

Hasonlóan teljes üzleti főfolyamatnak tekintettük még például a járóbeteg-ellátást, a gyógyszer-ellátást és a műtétek elvégzését is.

A támogató folyamatok alapvetően, mint az üzleti folyamatok függőségei jelennek meg, azaz az üzleti folyamatokat megelőző, annak alapvető feltételét biztosító folyamatok. Például egy műtét lefolytatását nem lehet elkezdeni, amíg a műtő az előző műtét után nem lett kitakarítva. A speciális berendezéseket igénylő vizsgálatokat (pl. röntgen, CT vagy MR vizsgálatokat) nem lehet lefolytatni a berendezések rendszeres kötelező karbantartása nélkül.

A felvett folyamatokhoz a szervezeti szerepköröket a RACI[3] mátrix módszere alapján kapcsoljuk hozzá. A folyamat megvalósításában különböző fizikai eszközöket, berendezéseket, informatikai (hardver és szoftver) eszközöket veszünk igénybe, amelyeket különböző logikai funkciók elvégzésére használunk. A kezeléshez vagy vizsgálathoz igénybe vett eszközök, berendezések maguk eszközként, az általuk ellátott funkciók pedig logikai funkcióként értelmezhetők. Informatikai eszközök esetében logikai funkciók lehetnek azok az alkalmazások (pl. kórházi informatikai rendszer, laboratóriumi mérőrendszer, különböző vezérlő rendszerek), amelyeket a kezelés során igénybe veszünk, és amely megvalósításához számtalan különböző hardver és szoftver elem összehangolt jó működése szükséges. A sebezhetőségeket és fenyegetéseket így a logikai funkciókhoz is tudjuk kötni, de ha mélyebb elemzésre van szükség, akkor továbbmenve az adott logikai funkciót megvalósító eszközök vagy azok részeinek a szintjére is lebonthatóak.

Gyakorlati tapasztalat, hogy az operatív folyamatok szintjén az ott dolgozók az egyes eszközök funkcióit veszik igénybe, a problémákat (kockázatokat) azon a szinten értik és kezelik. Amikor már a probléma ok-elemzésére van szükség, akkor a műszaki szakértői gárda a fenyegetéseket és sebezhetőségeket, kockázatokat visszavezeti az egyes fizikai eszközök működésének szintjére. Jelen modellben legtöbb esetben a funkciók szintjén vizsgáltuk a kockázatokat, de a modell és az eszköz lehetővé teszi a részle-

[3] RACI mátrix vagy módszer több informatikai alapú folyamatmodellezési rendszerben terjedt el. A RACI egy betűszó, ami az egyes folyamatfelelősségeket fogja össze. Az egyes betűk a következőket jelentik:
R (responsible) – felelős a saját maga által elvégzett munkáért, azaz ő dolgozik;
A (acccountable) – elszámoltatható a folyamat eredményéért, azaz ő a felelős vezető;
C (consulted) – egy szakértő, akinek tudását igény szerint igénybe veszik;
I (informed) – a folyamat eredményeiről informált, tájékoztatott személy.

tes, fizikai eszköz szintjén történő modellezést, elemzést is.

Ilyen módon a folyamatokban használt, azokat megvalósító eszközök, berendezések mind, mint erőforrások felvételre kerültek és a folyamatban felhasznált logikai szerepük szerint a folyamatokhoz hozzá lettek kapcsolva. Természetesen ez több-több kapcsolatot jelent, hiszen egy erőforrást több folyamat is használhat, és ugyanakkor egy folyamatot jellemzően egyszerre több erőforrás valósít meg.

A folyamatok mind kezelnek adatokat, ezért a felhasznált illetve kezelt adatok, adatkör szerinti csoportosításban felvételre kerültek, összesen mintegy 64 adatkör. Adatkörön értjük az azonos jellegű és azonos funkciót ellátó, azonos védelmet igénylő együtt kezelt elemi adattípusokat együtt. Ilyen adatkörök lehetnek például:

- Betegek kórházi azonosító adatai – azok az adatok, amelyekkel a kórházi nyilvántartó rendszer a betegeket azonosítja. Ilyenek pl. a név, lakóhely, születési adatok, valamint a beteg kórházi azonosító adatai (amelyeket ott a kórházi egészségügyi rendszeren belül generáltak és ezekkel azonosítják).
- Kiadott gyógyszerek listája – a központi gyógyszertár által az osztálynak a megrendelésre átadott gyógyszereinek tételes listája.
- Laborleletek – a normál labor vizsgálati eredményei (pl. vér, vizeletvizsgálat) és/vagy a mikrobiológiai labor vizsgálati eredményei.
- Leltári jelentések – havi, éves leltári jelentések a raktár forgalmáról.
- Egyéb adatkörök.

Az adatok, adatkörök mind kapcsolódnak a folyamatokhoz, itt is sokszor a több-több kapcsolat a jellemző. Az egyes adatok előfordulása jellemzően informatikai rendszerben, és/vagy papíron (vagy egyéb hagyományos típusú adathordozón) található. Az informatikai eszközökön tárolt és kezelt adatok folyamathoz kapcsolása a folyamat által használt informatikai eszközön, illetve az adott logikai funkción (pl. alkalmazás programon) keresztül valósul meg. A papíralapú dokumentumon (vagy egyéb hagyományos adathordozón) tárolt adatok szintén kapcsolódnak a folyamatokhoz, felvételük az adatokat tartalmazó adathordozók kapcsolatán keresztül valósul meg.

Az adatok tartalmuknál fogva lehetnek különböző jellegű adatok, ezért biztonsági igényeik is különbözők. Az adatok vonatkozhatnak a kórház pénzügyi vagy szervezeti működésére, az informatikai eszközök működésére, a betegellátás folyamatainak részleteire, de ugyanakkor vonatkozhatnak a dolgozók vagy betegek személyes adataira is. Ez utóbbi esetben a követelményeket szigorú jogi előírások is szabályozzák.

B) Személyes adatkezelések felmérése

A BIA modul – az előzőekben láthatóan – tartalmazza minden folyamat adatkapcsolatát, azaz a folyamat által kezelt/feldolgozott/tárolt adatokat. Ezek az adatok a folyamat funkcióit megvalósító, illetve követő vagy irányító informatikai rendszereken (pl. alkalmazásokon) vagy a közvetlen papírokon vagy egyéb hagyományos médiákon keresztül kapcsolódnak a folyamatokhoz. Betegadatok kapcsolata például a kórházi informatikai rendszereken, a képalkotó diagnosztikai berendezések PACS rendszerén, mint informatikai rendszereken vagy a papíralapú kórlapokon, leleteken, megírt recepteken, mint papíralapú médiákon jelenik meg a betegellátási folyamatokban.

Ilyen módon a felvett BIA modell tartalmazza az adatkörök között azokat az adatokat, mint információkat is, amelyek természetes személyekhez kapcsolhatók, tehát amelyek „személyes adatok”. Az adatkörök felvételekor megadható paraméter, hogy az adott adatkör tartalmánál fogva személyes adatot jelent-e. Ebben az esetben külön munkalapként tölthető ki az adott adatkör (mint személyes adat) adatkezeléséhez kapcsolódó technikai és jogi működést és megfelelést igazoló információ. Ezt tartalmazza az ún. „Személyes adatok kezelésének nyilvántartó lapja”. Erre bemutatunk egy példát egy különleges személyes adatkör esetén. A bemutatott adatkör a ’Képalkotó diagnosztikai leletek’, amelyek tartalmuknál fogva a betegek vizsgálati eredményeinek leírását tartalmazzák, amiből a beteg is és a betegsége is azonosítható. Itt a nyilvántartó lap központi részletét a 6. ábra mutatja be.

A rendszerrel ilyen módon meg lehet felelni a GDPR adatkezelési nyilvántartási, valamint a következő fejezetben bemutatott módon az adatvédelmi kockázatok elemzési követelményeinek is.

Személyes adatok kezelések nyilvántartása

Megnevezés	Képalkotó diagnosztikai leletek
Adatgazda szerepkör	diagnosztikai orvos
Adatkezelés rövid leírása	
Képalkotó diagnosztikai felvételek kiértékelése alapján a leletek elkészítése, azok rögzítése a PACS rendszerben, majd azok átadása a kórházi egészségügyi informatiaki rendszerbe a beteg diagnosztizálása céljából.	
Az automatizált döntéshozatal (profilalkotás) működésének leírása	
Adatkezelés jogalapja	
törvényi előírás	
Adatkezelés célja	
a beteg diagnosztizálása, kezelési mód meghatározása	
Érintettek kategóriái	Betegek
Személyes adatot tartalmaz?	Igen
Személyes adatok kategóriái	Kórházi azonosító adatok
Különleges személyes adatot tartalmaz?	Igen
Különleges személyes adatok kategóriái	Egészségügyi adatok
Címzettek listája, akiknek az adatot továbbítják	
Harmadik országba vagy nemzetközi szervezet részére történő továbbításra vonatkozó információk	
Megtartási idő	30 év
Megtartási szabályzatok	
kórházi egészségügyi rendszerben mentés	

Adatkezelők és adatfeldolgozók

Név	**Teleradiómatria Kft.** (Adat feldolgozó)

6. ábra: Példa egy Személyes adatok kezelésének nyilvántartása adatlapra

4. A különböző kockázatok felvétele és kezelési módjai

A) Működési és információbiztonsági kockázatok CRAMM módszer alapú felmérése

Modell-kórházunkban a különböző kockázatok felvétele egységesen a BIA modulban felvett működési modellre és kapcsolatrendszerre épít, és egységesen ugyanolyan értelmezésű skálát vesz figyelembe.

A különböző kockázatok kapcsolódhatnak a folyamatok erőforrásaihoz (humán erőforrások, mint kapcsolódó szerepkörök; infrastruktúra elemek, mint épületek, helyiségek, berendezések és eszközök; informatikai infrastruktúra elemek, mint hardver vagy szoftver elemek stb.) vagy közvetlen a folyamatokhoz is. Ezek az elemek lehetnek fenyegetéseknek kitéve, amelyek folytán a kockázati esemény bekövetkezési lehetőségét az adott elem adott fenyegetéssel szembeni sebezhetősége (gyenge védelme, szabályozatlan működése) adja. A kockázati esemény pedig a fenyegetés és a kapcsolódó sebezhetőség párosításából következik, amelynek bekövetkezési valószínűsége és kárértéke a két jellemző paramétere, és amelyből a kockázati érték számítható. Attól függően, hogy a kockázat hatása közvetlen a működésre, vagy valamely információ biztonságának (bizalmasságának, sértetlenségének vagy rendelkezésre állásának) sérülésén keresztül hat, nevezzük a kockázatokat működési vagy információbiztonsági kockázatoknak.

A kockázatok azonosítását (verbális jellemzését és meghatározását) követően a kockázati kárértékek és bekövetkezési valószínűségi értékek meghatározása során megkülönböztettük a (közvetlen) működési kockázatokat és az információbiztonsági kockázatokat. Ennek a megkülönböztetésnek az alapját az adja, hogy a lehetséges káresemény bekövetkezése közvetlenül valamelyik fenti kárjelleg bekövetkezésében jelenik-e meg, vagy pedig valamely kezelt, feldolgozott, vagy tárolt információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának a sérülését okozza, és ezen keresztül következik-e be a károkozás. Amennyiben információbiztonsági kockázatként azonosítottuk az adott kockázatot, akkor a lehetséges kárhatásnál megkülönböztettük és külön-külön elemeztük, hogy az az információ bizalmasságának sérülésén, integritásának a sérülésén vagy a rendelkezésre állásának a sérülésén keresztüli kárt jelent, majd természetesen a legnagyobbhoz tartozó értékekkel számoltunk tovább. Ennek a megkülönböztetésnek a majdani kockázatcsökkentő intézkedések kiválasztásában lesz gyakorlati jelentősége.

Nézzünk (a teljesség igénye nélkül) néhány példát ezekre, hogy könnyen érthető legyen:

- Humán erőforrások (illetve folyamatokhoz rendelt szerepkörök) kockázata lehet:
  - A gyakori munkaerőhiány következtében a „***túlterheltség***”, „***kialvatlanság***” (mint sebezhetőségek) miatt, „***figyelmetlenség és hibázás***” (mint fenyegetés) következtében az „***orvosi műhiba***” vagy „***ápolói tévedés***” kockázatának bekövetkezése lehetséges.
  - A „***biztonságtudatosság hiánya***” (mint sebezhetőség) miatt, „***pletyka, kifecsegés***” (mint fenyegetés) következtében a „***betegadatok kiszivárgása***” kockázat bekövetkezése lehetséges.

- Épület vagy berendezés kockázata lehet:
  - A fekvőbeteg-ellátásnál a rossz állapotban lévő kórházi folyosón a *„nem megfelelő tisztaság”* vagy *„nem megfelelő (esti) megvilágítás”* (mint sebezhetőség) miatt, a *„betegek elcsúszása, megbotlása”* (mint fenyegetés) következtében a *„betegek újabb sérülése”* kockázat bekövetkezése lehetséges.
- Médiák vagy adathordozók kockázata lehet:
  - Az ápolási dokumentáción a *„rosszul olvasható kézírás a dokumentumon”* (mint sebezhetőség) miatt, *„információ félreértés”* (mint fenyegetés) következtében a *„betegek felcserélése”*, *„hibás, felcserélt gyógyszerelés”* kockázatának bekövetkezése lehetséges.
- Hardver elemek kockázata lehet:
  - A *„nem megfelelő informatikai karbantartás”* (mint sebezhetőség) miatt, az *„információs rendszer meghibásodása”* (mint fenyegetés) következtében a *„IT hálózat leállása meghatározott időre”* kockázat bekövetkezése lehetséges.
- Szoftver elemek kockázata lehet:
  - A *„nem megfelelő jogosultságkezelés”* vagy *„gyenge jelszóhasználat”* (mint sebezhetőségek) miatt, az *„illegális adathozzáférés”* (mint fenyegetés) következtében a *„betegadatok kiszivárgása”* vagy *„betegadatok jogosulatlan módosítása, meghamisítása”* kockázatának bekövetkezése lehetséges.
- Maga a folyamat kockázata lehet:
  - A *„nem kellően szabályozott folyamat”* vagy *„szabályozatlan folyamat”* (mint sebezhetőségek) miatt, a *„figyelmetlenség, lustaság és/vagy kapkodás”* vagy *„adott orvosnak ismeretlen szituáció fellépése”* (mint fenyegetések) következtében bármely folyamat esetén, a *„folyamat vagy kezelés nem megfelelő vagy hibás működése”* kockázat bekövetkezése lehetséges, ami meghatározott folyamat esetén meghatározott hiba is egyúttal.

A felmerülő kockázat hatása alapján besorolható a következő kockázati típusokba:

- **betegbiztonsági kockázatok** (ha pl. a betegek gyógyulását veszélyeztetik vagy kórházi fertőzését okozhatják),
- **működési kockázatok** (ha pl. egyes folyamatok, tevékenységek hibás működését vagy leállását okozhatják, akárcsak időlegesen is),
- **pénzügyi kockázatok** (ha pl. az intézmény finanszírozási vagy kontrolling rendszerében jelentkeznek),
- **jogi kockázatok** (ha jogsértéseket illetve jogi peres ügyeket idézhetnek elő),
- **információbiztonsági kockázatok** (ha adatszivárgást, vagy illetéktelen / jogosulatlan adathozzáférés által különböző károkat okozhatnak),
- egyéb kockázati típusok.

Ezeket az általános kategóriákat módszerünkben a lehetséges károk területeinek, mint kárjelleg típusokat különböztettük meg. Így a kockázatok elemzése során lehetséges kárértékeket ennek kapcsán állítottuk fel, és a kárértékek skálázását ezekre a kárjelleg (osztályokra) típusokra határoztuk meg:

Kárjelleg (osztály)	Leírás
Közvetlen anyagi kár	pl. a mindenkori amortizált értékkel vagy az elmaradt haszonnal arányos
Közvetett anyagi kár	pl. a helyreállítási költségekkel arányos
Egészségi állapot romlása	pl. egészségügyi állapot különböző szintű vagy maradandó romlása, esetleg haláleset
Kórházi fertőzés	pl. ellátás során fertőzés(ek) fellépése
Adatszivárgás	pl. betegek (vagy más kórházi személyek) adatainak kiszivárgása, kompromittálódása, esetleg az intézmény gazdasági-működési adatainak illetve a személyzet személyes adatainak kiszivárgása, ezzel visszaélés
Üzemszünet	pl. informatikai vagy egyéb infrastrukturális (vagy más, pl. személyi) okok miatt a betegellátás működése, folyamatai rövidebb-hosszabb ideig szünetelnek vagy leállnak, azok feltételei nem biztosítottak
Programhiba	pl. a szoftverek hibája, hiányossága miatt hibás jelentés-dokumentumok készülnek, és bizonyos szükséges programfunkciók nem érhetők el

Ezek közül minden egyes kárjelleg típusra verbálisan határoztuk meg a kárérték-skála értelmezését, az adott intézményre jellemző esetekhez. Például nézzük ezt a „Közvetlen anyagi kár" és az „Egészségi állapot romlása" kárjellegek esetén:

Kár-érték	Közvetlen anyagi kár	Egészségi állapot romlása
1	≤ 100.000 Ft	Kórházi baleset, szerencsétlenség, hibás kezelés vagy egyéb ok miatt a beteg lassabban gyógyul az indokoltnál.
2	> 100.000 Ft	Kórházi baleset, szerencsétlenség, hibás kezelés vagy egyéb ok miatt a beteg jóval lassabban gyógyul az indokoltnál, vagy valamilyen nem maradandó sérülést szenved.
3	> 1.000.000 Ft	Kórházi baleset, szerencsétlenség, hibás kezelés vagy egyéb ok miatt a beteg valamilyen nagyobb maradandó sérülést szenved.
4	> 10.000.000 Ft	Kórházi baleset, szerencsétlenség, hibás kezelés vagy egyéb ok miatt a beteg valamilyen nagyobb maradandó sérülést szenved vagy meghal, vagy több betegnek lesz számottevő maradandó sérülése.
5	> 50.000.000 Ft	Kórházi baleset, szerencsétlenség, hibás kezelés vagy egyéb ok miatt több beteg komoly maradandó sérülése vagy halála.

A bekövetkezési valószínűségek lehetséges értékeit szintén (1…5)-ös skálán definiáltuk, a következő módon:

Megnevezés	Leírás
1 – elenyésző	szinte lehetetlen, 10 évnél is ritkábban következhet be
2 – ritka	várhatóan 8-10 évente egyszer bekövetkezhet
3 – közepes gyakoriságú	várhatóan néhány (3 – 5) évente egyszer bekövetkezhet
4 – gyakori	várhatóan évente csak egyszer bekövetkezhet
5 – rendszeres	várhatóan havonta bekövetkezhet

Természetesen figyelembe kell venni, hogy a felvett skálázások mind példaértékűek, hiszen egy valós kórház kockázatainak felvétele esetén ezeket az értékeket mind egyesével, a kórház viszonyaira az ott dolgozó szakemberekkel egyeztetve egyénileg kell meghatározni.

Az egyes kockázatok kockázati értékének meghatározása mindig a
kockázati érték = bekövetkezési valószínűség * kárérték
képlettel lett meghatározva.

Az egyes kockázatok egymáshoz mérése első sorban a kockázati érték alapján lehetséges, és itt a szemléletesebb kockázatértékelés miatt a kockázatokat kockázati szintekbe osztottuk, és aszerint ábrázoltuk őket. Az 1…25-ös kockázati érték skálán:

- 20 – 25 értéktartományban a kockázatokat kiemelkedően nagy kockázatoknak,
- 15 – 19 értéktartományban a kockázatokat nagy kockázatoknak,
- 8 – 14 értéktartományban a kockázatokat közepes kockázatoknak,
- 3 – 7 értéktartományban a kockázatokat csekély kockázatoknak,
- 1 – 2 értéktartományban a kockázatokat jelentéktelen kockázatoknak

minősítettük.

A felvett kockázatoknál – példaként néhány kiemelkedően nagy és nagy kockázat esetén – felvettünk néhány javasolt kockázatcsökkentő intézkedést, ahol becsültük annak bevezetési költségét, valamint bevezetése esetén hatását a kockázati érték csökkenésére (a bekövetkezési valószínűség és/vagy kárérték csökkenésén keresztül.) Ezek alapján van lehetőség dönteni az intézkedési javaslat bevezetésének elfogadásáról.

B) Személyes adatok adatkezeléséhez (GDPR-hoz) kapcsolódó kockázatfelmérések

A személyes adatkezelési tevékenységek során az adatkezelések kockázatainak felmérését előírja a GDPR is, illetve a kapcsolódó magyar jogszabály, az infotörvény is.

A 'személyes adat' – a fogalom definíciója szerint is – mind olyan 'információ', amely tartalmánál fogva természetes személyekkel hozható közvetlenül vagy közvetve összefüggésbe, rajta keresztül természetes személyek beazonosíthatók. Tehát miután a személyes adatok mind 'információk', így részét képezik a modell-kórházunk működésében szereplő összes információnak, amelyeket adattípusonként mind jelle-

meztünk, a folyamatokhoz hozzákapcsoltunk, és kockázataikat – mint információbiztonsági kockázatokat – részletesen felmértük.

A beazonosítást segíti, hogy a BIA modul részeként minden adattípusnak egyik jellemző paramétere, hogy az tartalmánál fogva 'személyes adatnak' minősül-e. Innentől fogva a személyes adatoknak minősülő adattípusok információbiztonsági kockázatai egyben értelmezhetők a GDPR szerinti személyes adatbiztonsági kockázatainak. A kockázatfelmérés módszeréből adódóan az adatszivárgás, programhiba, üzemszünet kárjellegek direkt a személyes adatok adatbiztonsága sérüléseinek következményeiként léphetnek fel, de indirekt megjelenhet, mint kárjelleg az anyagi kár is, pl. mint a kiszabott büntetés mértéke.

Ezek a kockázatok tehát megjelennek mind és részét képezik a megelőző lépésben bemutatott információbiztonsági kockáztok felmérésének és kezelésének.

C) Eszközök és berendezések működésével összefüggő FMEA alapú kockázatfelmérések

A BIA modul lehetővé teszi az épület vagy berendezés, fizikai eszköz (gép), hardver vagy szoftver elem, adathordozók (médiák) meghibásodásainak (vagy hibás működéseinek) a felvételét, és külön modellezését, és ehhez kapcsolódóan azoknak mint lehetséges kockázatoknak az FMEA szerinti elemzését. Tehát egy meghatározott (és általunk paraméterezett) 1…10-es skálán felvettük néhány ilyen meghibásodás bekövetkezési valószínűségét, bekövetkezése esetén a rejtettség mértékét, illetve a lehetséges kár mértékét.

Ilyen módon is különböző kockázatok azonosíthatók, elemezhetők és hasonlíthatók össze, figyelembe véve az elemzés során a kockázatok rejtettségét is. A kockázat mértéke az FMEA klasszikus számítási módja alapján:

kockázatprioritási szám =
bekövetkezési valószínűség * kárérték *
rejtettség mértéke.

A kockázatokhoz itt is rendelhetők kockázatjavító intézkedések, amelyeknél becsülhető az intézkedés bevezetése után annak hatása maradványkockázat becslésének formájában, az intézkedés bevezetésének hatása következtében a becsült, csökkent mértékű valószínűségi érték, rejtettség vagy kárérték megváltozásának következtében. Természetesen a kockázat mértékének (itt a kockázatprioritási szám értékének) csökkenésével itt is arányba állíthatjuk mindig a kockázatjavító intézkedés bevezetésének költségét, és annak alapján van lehetőség dönteni az intézkedési javaslat bevezetésének elfogadásáról.

5. Az eredmények megjelenítése és értelmezése

Az előzőekben meghatározott módon modelleztük egy minta-kórház működését, majd a működéshez felvettünk – az erőforrásokban, illetve közvetlen a folyamatoknál megjelenő – sebezhetőségeket és az azokat kihasználó fenyegetéseket, amelyek együtt kockázatokat határoztak meg. Ilyen módon az azonosított kockázatokat elemeztük, azaz bekövetkezési valószínűségi értéket és lehetséges kárértéket becsültünk hozzájuk, amelyekből a rendszer már számította az egyes kockázatok kockázati értékeit.

A példa projektben a CRAMM módszerrel mintegy 100 kockázatot vettünk fel, köztük információbiztonsági kockázatokat is, és többségében (80 – 90 %-ban) folyamatkockázatokat. A folyamatkockázatok – kockázati típus szerinti besorolásban – egyaránt tartalmaznak betegkockázatokat, intézmény-működési kockázatokat, karbantartási és egyéb eszközökre vonatkozó kockázatokat és pénzügyi kockázatokat. Ezek megjeleníthetők együttesen is, illetve bármilyen szempont szerint csoportosítva, illetve sorba rendezve.

Lehetőségünk van a kockázatok egységes, táblázatos megjelenítésére mind maguk a kockázatok esetén, mind megjelenítve a hozzájuk kapcsolódó kockázatkezelési intézkedéseket az intézkedések becsült költségével illetve a bevezetésük esetén becsült maradvány kockázati szinttel. Az FMEA szerinti hibakockázatokat és az azokhoz kapcsolódó kockázatkezelési terveket ugyanolyan módon, de külön táblázatos megjelenítésben láthatjuk.

Egy külön, ún. **'vezetői műszerfal**on' (dashboard-on) összefoglalva láthatjuk pl. a CRAMM módszerrel meghatározott összes kockázat közül a legjelentősebbeket kiemelve (lásd a 7. ábrát). (*Megjegyzés: Az ábrán a kockázati potenciál megadása kötőjellel elválasztva kétféleképp történik: először maga a kockázati érték, majd annak százalékos megfelelője az 1…25-ös skálán.*)

Kockázat megnevezése	Kockázat típus	Kockázat potenciál	Kockázati szint
Késedelmes karbantartás	Folyamat	20 - 80 %	Kiemelkedően nagy
Steril eszközök kezelése nem megfelelő	Folyamat	20 - 80 %	Kiemelkedően nagy
Műtéti anyagok, eszközök hiánya	Folyamat	16 - 64 %	Nagy
Műtét utáni sebfertőzés	Folyamat	16 - 64 %	Nagy
Műtét előtt hibás - hiányos antibiotikum profilaxis	Folyamat	16 - 64 %	Nagy
Betegadatok kiszivárgása	Információ-biztonsági	16 - 64 %	Nagy
Hibás diagnózis miatti félrekezelés	Folyamat	16 - 64 %	Nagy
Hibás altatás-ébresztés	Folyamat	16 - 64 %	Nagy
Gyógyszer osztásnál hibázás	Folyamat	16 - 64 %	Nagy
Beteg műtét alatti elmozdulása	Folyamat	16 - 64 %	Nagy
Beléptetőrendszer meghibásodása	Folyamat	16 - 64 %	Nagy
Könyvelési hiba 2	Információ-biztonsági	16 - 64 %	Nagy
Gyógyszercsere	Információ-biztonsági	16 - 64 %	Nagy
Műtéti hiba, orvosi műhiba	Folyamat	16 - 64 %	Nagy
Beléptetőrendszer meghibásodása 2	Információ-biztonsági	16 - 64 %	Nagy

7. ábra: A legjelentősebb jelenlegi kockázatok kockázati potenciál szerint rendezve

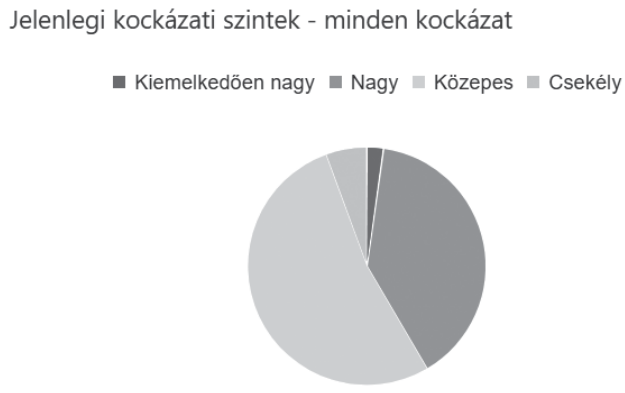
A kockázatok kockázati szint szerinti eloszlása is kördiagramon vizualizálható, egyrészt az összes kockázat tekintetében (lásd a 9. ábrát), másrészt az egyes kockázati kategóriák szerint is. Itt például a 10. ábrán az információbiztonsági kockázatok kockázati szint szerinti eloszlását mutatjuk be egymás mellett háromféle összehasonlításban.

A kockázatok felmérése és az elemzés során lehetőség volt arra is, hogy az adott kockázati esemény jelen állapotbeli működését jellemző értékek mellett felvegyük azt az elképzelt állapotot is, amit az adott fenyegetés okozhatna, ha a jelen működésben semmilyen meglévő védelem az adott fenyegetéssel szemben nem lenne. Ez jelenti az ún. bruttó kockázat fogalmát, a jelenlegi működést és biztonságot jellemző állapot pedig a nettó kockázat fogalmát. Ehhez képest persze sokszor még ez a nettó kockázat (jelenlegi állapot kockázata) is túl nagy, és valamilyen kockázatkezelési intézkedést kell bevezetni, aminek a bevezetése után érhetjük el az ún. maradvány-kockázatot. A bruttó és a nettó kockázat fogalma bevezetésének és figyelésének az a legfőbb jelentősége, hogy a bruttó és nettó kockázat közötti különbség mutatja meg és indokolja is egyben a jelenlegi biztonsági intézkedéseket. A jelen állapotban meghatározott kockázatkezelési intézkedések többletberuhá-

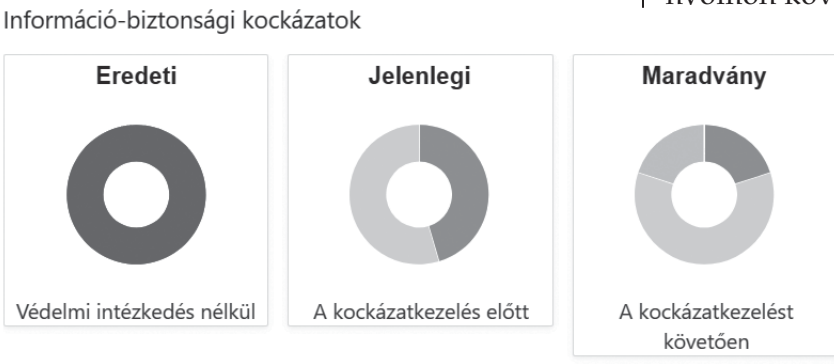
A rendszer (lásd 8. ábra) a kockázatokhoz javasolt legjelentősebb kockázatkezelési intézkedéseket is összefoglalva kiemeli és bemutatja. Megjegyezzük, hogy a minta-kórházi projektben a kockázatkezelési intézkedések költségeit nem becsültük meg, így az automatikus rendezés itt ezt az elvet nem tudta követni.

Kockázatkezelési terv megnevezése	Kockázat típus	Maradvány kockázati szint	Becsült költség
Beléptetési rendszer szoftverének rendszeres ellenőrzése, tesztelése	Információ-biztonsági	Közepes	-
Verziófrissítés utáni ellenőrzési rend kialakítása	Folyamat	Csekély	-
Gyógyszerészi konzíliumok gyakoriságának növelése	Információ-biztonsági	Csekély	-
Adategyeztetés és ellenőrzés könyvelés előtt	Információ-biztonsági	Közepes	-
Új verziók előzetes tesztelése	Információ-biztonsági	Közepes	-
Folyamatos ellenőrzés és karbantartás	Folyamat	Közepes	-
Ápolási dolgozók oktatása	Folyamat	Közepes	-
Helyettesítési, pótlási rendszer kialakítása	Folyamat	Csekély	-
Munka és helyettesítési rend betartatása, ellenőrzése	Folyamat	Közepes	-
Szigorú ellenőrzés és munkautasítási rend	Folyamat	Csekély	-
Gyógyszerészi konzíliumok gyakoriságának növelése	Folyamat	Csekély	-
Gyógyszerfelügyelő rendszer bevezetése	Folyamat	Csekély	-
Kötelező konzultáció bevezetése	Folyamat	Közepes	-
Raktározási monitoring rendszer bevezetése	Folyamat	Csekély	-
Tervszerű megelőző karbantartás biztosítása	Folyamat	Közepes	-

8. ábra: A legjelentősebb jelenlegi kockázatkezelési intézkedések bemutatása



9. ábra: A Dashboardon a kockázatok eloszlása kockázati szintek szerint, jelen állapotban



10. ábra: A Dashboardon az információbiztonsági kockázatok eloszlása kockázati szintek szerint, eredeti – jelen – maradvány kockázati állapotban

zást jelentenek, és ezek bevezetésével érjük el azt a kockázati szintet, amit most maradvány kockázatként jelöltünk. Viszont a következő kockázatfelmérési ciklus során már ez az állapot lesz az akkor „jelen állapot", és (ha minden jól működik, akkor) a jelenleg meghatározott maradvány-kockázatok alkotják akkor a nettó kockázatokat (akkori jelen kockázatokat). És azt a szintet a most is már működő, illetve a most bevezetett új kockázatkezelési intézkedések együttesen teszik lehetővé, aminek szemléletes indokát a bruttó (ami nem változik) és az akkori nettó kockázatok közti különbség mutatja majd meg.

A vezetői műszerfalon bemutatott legjelentősebb kockázatok mutatják meg, hogy mik azok a kockázatok, amelyek csökkentésével foglalkozni kell. A javasolt intézkedések hatásait is egyben áttekinthetjük. A kockázatok eloszlása megjeleníthető kockázati területenként és kockázati szintenként, tehát gyorsan képet ad arról, hogy melyek a legveszélyesebb, legkritikusabb területek.

A kockázatkezelési intézkedések meghatározásakor lehetőség van arra is, amit a jelen modell-kórházas példa esetén nem használtunk ki, hogy az egyes kockázatkezelési intézkedéseket hozzákapcsoljuk különböző követelményrendszerek egyes pontjaihoz. Ilyen követelményrendszerek lehetnek például az ISO/IEC 27001 szabvány „A" mellékletének információbiztonsági követelményei vagy az információbiztonsági törvény végrehajtási rendeletéhez kapcsolódó informatikai biztonsági követelmények vagy akár a MEES standardjainak követelménypontjai. Ezzel a hozzárendeléssel egyben az adott követelményrendszerhez kapcsolódó megfelelések is igazolhatók, nyomon követhetők.

6. Összefoglalás

A szervezet működési kockázatainak modellezéséhez alapvető fontosságú volt az első lépés, magának a szervezetnek a definiálása. Az gyorsan egyértelművé vált, hogy valós szervezet adataival történő teljes körű vizsgálathoz nem rendelkezünk elegendő kapacitással. Bár csábítónak tűnhet egy kis kórház komplex vizsgálata, azonban célunk az volt, hogy minél több típusú kockázat felmérését és kezelését tudjuk egységes modellben bemutatni.

A modellben először az ellátási folyamatokat definiáltuk, a továbbiakban ezekhez kerestük meg a kapcsolódó szerepköröket. Ahhoz, hogy a folyamatkockázatok mellett kezelni tudjuk a további kockázatokat is, rögzítenünk kellett a folyamatokhoz kapcsolódó elemi erőforrásokat, valamint a szükséges infrastrukturális elemeket. Az alapadatok felvitelét követően elvégezhető a hatáselemzés. Fontos kiemelni, hogy a rendszerben elvégezhető a személyi adatok hatáselemzése is a GDPR megfelelőség érdekében, sőt teljes körűen biztosítani lehet a szükséges GDPR nyilvántartásokat is. A logikai rétegek megfelelősége különböző követelményekhez köthető így az integrált rendszer valamennyi eleme egységesen kezelhető.

Az alkalmazott CRAMM módszertan segít abban, hogy nagyszámú kockázatot lehessen azonosítani, majd ezeket többféle szempontból

elemezni. A kockázatokra hozott intézkedések lehetséges hatásai is vizsgálhatók eredeti – jelenlegi – maradvány-szempontok szerint (azaz bruttó – nettó – maradvány kockázatként), és akár szcenáriókat is összeállíthatunk, ami nagymértékben megkönnyítheti a vezetői döntéseket. Ezek együttesen könnyen kezelhető, jól áttekinthető integrált eszközt adnak a felső vezetés kezébe a különböző kockázatkezeléssel kapcsolatos döntéseik támogatására.

Referenciák

1. ISO 9001:2015 Quality management systems. Requirements (magyar szabványként: MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények)
2. EN 15224:2017 Quality management systems – EN ISO 9001:2015 for healthcare (magyar szabványként: MSZ EN 15224:2017 Minőségirányítási rendszerek. Az EN ISO 9001:2015 az egészségügyi ellátásban)
3. AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről
4. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
5. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
6. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
7. A 370/2011. (XII. 31.) Korm. rendelet a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről
8. Falusi Tímea: „Egészségügyi intézmények egy kiválasztott folyamatának kockázatelemzése támogató szoftver segítségével", Óbudai Egyetem, Rejtő Sándor Könnyűipari és Környezetmérnöki Kar, szakdolgozat (2016)
9. ISO 31000:2018 Risk management. Guidelines (magyar szabványként: MSZ ISO 31000:2019 Kockázatmenedzsment. Irányelvek)
10. Horváth Zsolt – Solymosi Ildikó – Fekete István: Gyakorlati tanácsok a kockázatfelmérés és kezelés szervezeti szintű bevezetésére a vonatkozó szabványok alapján, Magyar Minőség XXV. évfolyam, 2016/05. szám, 6-28.old.
11. Dr. Horváth Zsolt: Kockázatmenedzsment a vállalati sikeresség érdekében, Magyar Minőség XXVI. évfolyam, 2017/01. szám, 16-24.old.

FÁBIÁN ZOLTÁN, vegyész üzemmérnök, TQM szakközgazdász, EOQ MNB Minőségügyi Szakértő, TQM és Kockázatmenedzser. 1987 óta dolgozik minőségügyi területen. Több iparágban szerzett 16 éves ipari tapasztalattal került a Szegedi Tudományegyetemre, ahol 12 éven át volt az SZTE Szent-Györgyi Albert Klinikai Központ minőségügyi vezetője. Ez idő alatt a szervezet kétszer nyerte el az IIASA-Shiba Díjat. Szakterülete a TQM és az integrált irányítási rendszerek fejlesztése és működtetése. 2005 óta a Magyar TQM Szövetség elnöke. Jelenleg a Szegedi Tudományegyetem MIR vezetője.

DR. HORVÁTH ZSOLT, CSc., szilikátipari mérnök, matematikai modellezési szakmérnök, a műszaki tudomány kandidátusa. EOQ MNB Minőségirányítási és Információbiztonsági Rendszermenedzser és Auditor. 10 évi ipari majd 3 évi IT vezetői gyakorlat után 10 éven keresztül a Siemens magyarországi szoftverházának, a Sysdata Kft-nek (amiből közben a Siemens PSE Kft. lett) minőségügyi vezetőjeként dolgozott. Négy évet az Óbudai Egyetemen információbiztonságot oktatott, jelenleg a Budapesti Metropolitan Egyetemen az Információbiztonsági menedzser c. szakirányú továbbképzési szakon információbiztonságot oktat. 2000-től folyamatosan több tanúsító szervezetnél minőségügyi és információbiztonsági vezető auditor. 2006-tól az INFOBIZ Kft. vezetőjeként és vezető tanácsadójaként minőségügyi és információbiztonsági tanácsadó.