TEKE ANDRÁS

# A „BIZTONSÁGI AUDITOK" KOCKÁZATKEZELÉSI KOCKÁZATA

*„Beszéljen, de ne úgy, hogy talán megértsék,*
*hanem úgy, hogy félre ne értsék."*[40]

## 1. Bevezetés

A kockázatok kezelése már magában hordozza azt a kockázatot, ami a kezelésnek nevezett „valami" outputja és a valós kezelési igény, elvárás, lehetőség közti különbségből ered. Már a kiindulás, azaz a kockázatok körülhatárolása is kellőképpen heterogén ahhoz, hogy kockázatok megítélése valós kockázatot jelentsen. Ha a biztonsági kockázatokra csak rendészeti választ keresünk, akkor ezzel akár a lehetséges megoldást is marginalizálhatjuk, ami viszont önmagában is komoly kockázatot jelenthet.

A kockázat általános megközelítésében[41] valamely formalizált eljárás során vagy intuitív alaponképzett olyan jellemző, viszonyítási érték,amely behatárolja valamely rendszer fenyegetettségének mértékét, egyfajta valószínűséget vagy valószínűtlenséget prognosztizál. A kockázatok kezelése is egy folyamat, amely önmagábannem szünteti mega kockázati tényezőket, csupán segít(het) abban, hogy hatásuk viszonyítható, számszerűsíthető és valamilyen módon a hatásmechanizmusra és a következményekre tekintettel alakítható legyen. Ez a tény önmagában már elegendő ahhoz, hogy a kockázatokat statisztikailag közelítse meg az érintett, ami újabb kockázatot generál, mert a kivitelezésben a rendészeti DRM[42] gondolkodás mellett az üzleti élet SES[43] megközelítése is ezt katalizálja.

Meghatározó maga a szemlélet. A kockázatok emlegetése, meghatározása, kezelése egyfajta üzleti filozófiai szlogenné lett és a világhálón a biztonsági auditra (safety audit) kattintva tízezres nagyságrendben találhatunk anyagokat. Mint általában a biztonsággal kapcsolatos probléma-megközelítéseknél, jelen esetben is komoly fogalmi heterogenitás figyelhető meg. A kockázatkezelésnek csak részét képezi a helyzetértékelés és a felmérés, esetleg az audit, de a teljes folyamatot nem fedi le. Az idegen nyelvről jól-rosszul lefordított kifejezések tartalma és környezete is eltérhet a hazai és az eredeti feltételek vonatkozásában. Gondoljunk csak a sokat emlegetett security és safety közti különbségekre, ami magyarul egyformán biztonságként kerül fordításra.

A biztonság értelmezése sem konszenzusos, a technokrata megközelítéstől egészen a filozófiai fejtegetésekig van példa. Ehhez jön, hogy a rendészet és rendvédelem is hasonló helyzetben van.

---

[40] Marcus Fabius Quintilianus. Vö. https://pozitivgondolatok.wordpress.com/tag/felreertes/ (Letöltés ideje: 2014.07.11)
[41] Jelen anyag vonatkozásában ez a bázis.
[42] DRM:Determinált-Redukcionista-Mechanisztikus
[43] SES:Simplification(egyszerűsítés), Effectivity(hatékonyság), Specification(specializálódás)

A kockázat megítélésének vonatkozásában erős a szakterületi elhatárolódás és társadalmi szinten is eltérő lehet ugyanannak a dolognak a politikai, gazdasági, szakmai, egyéni, közösségi, stb. kockázati megítélése, így a konferencia címét akár egy sok ismeretlenes egyenletként is felfoghatjuk, aminek a megoldása csak újabb ismeretlen tényezők bevonásával valósítható meg úgy, hogy minden esetben azok száma legalább eggyel növekszik. Paradox helyzet.

A biztonsági kockázatok sem sorolhatók be az általánosan alkalmazott kockázatkezelési receptúrák szempontjai közé, mert gyakorlatilag minden kockázatnak van valamilyen biztonsági vonzata. Ritka a direkt hatásmechanizmusú biztonsági kockázat, általánosnak tekinthető az ún.következmény-mechanizmus. Mindez feltételezi a biztonsági kockázatok vonatkozásában az integrált, komplex, folyamat-és rendszer (hálózatos) szemléletű megközelítést. Ez egy olyan szituáció, amelyben eleve kódolva vanegy„egyszerűnek látszó" megoldás, s ha valaki nem ismeri fel a valós összefüggéseket és azok feltételezhetően valószínű következményeit,az újabb biztonsági kockázatokat generálhat. Erre a helyzetre „kínálnak megoldást"többek közt a divatossá vált a biztonsági auditok. Jelen tanulmány az ún. auditszemlélet biztonsági kockázatok kezelése terén való alkalmazhatóságát vizsgálja, a megoldáskeresésre helyezve a hangsúlyt.

## 2. Biztonsági rendszerek[44]

A biztonsági auditok kockázatkezeléssel összefüggői funkcionális szerepüket az auditok auditkritérium-determináltsága miatt elsősorban adefiniált biztonsági rendszerekben tudják betölteni. A biztonsági rendszer fogalma átfogó értelemben még nem került definiálásra, és lényegi különbség van a nyílt és zárt biztonsági rendszerek között is. Ez alapvetően befolyásolja magát a kockázatkezelést, a rendészet, a rendészeti megoldások, a biztonság és kockázatmenedzsment szerepét, lehetőségeit is. Zárt rendszerek esetében (IT, atomenergia, védett technológiák, adatvédelem, stb.) a szakmai, funkcionális és eredményorientált definiáltság biztosítja az érdemi védelmi rendszeri működést, megfelelő dokumentáltság mellett az auditok szerves részét képezik a biztonsági rendszerműködésnek. A nyílt rendszerek nem hogy nem definiáltak, de sok esetben a szereplők teljes köre sem kerül azonosításra, ez vonatkozik a rendészettel rendszerint kapcsolatba hozott közbiztonságra is. A biztonságvédelemre[45] (safetyprotection, Sicherheitsschutz) létezik több ismert és elterjedt fogalom, legalábbis az intézményi és nagyrészt a tevékenységi oldalt illetően. Ez részben kiterjeszthető a biztonságvédelmi rendszerre is, ugyanakkor a biztonsági rendszer, a biztonságrendszer, a rendszerbiztonság, a környezetbiztonság, biztonsági környezet és ezekhez kapcsolódóan a biztonságmenedzsment és a kockázatmenedzsment értelmezését is célszerű lenne konszenzusos módon körülhatárolni és főleg egymással szinkronba hozni, azaz a kapcsolódási pontok meghatározásával legalább folyamatszinten a kockázatkezelést összehangolni.

A hagyományos rendszerek mellett felmerül még a menedzsment rendszerillesztési problematikája is, amely bármennyire furcsa (főleg a rendészet vonatkozásában) a kockázatkezelés egyik meghatározó aspektusa lehet.

---

[44] A biztonság esetében a rendszer kifejezést sok esetben olyankor is alkalmazzák, ha az nem teljesíti a rendszerkritériumokat

[45] Szerző a témában több publikációt is megjelentetett, először Teke András: A biztonságvédelem, a biztonságvédelmi rendszer körülhatárolása, Detektor plusz 1999/5. sz. 19-23. o. Jelen anyagban egy összegzett gondolatsor jelenik meg.

A biztonsági rendszerre javasolt – szerző által megfogalmazott – munkadefiníció: „*A biztonsági rendszer az a rendszerismérvekkel rendelkező, funkcionálisan biztonsági igények, elvárások, előírások kielégítésére tudatosan kialakított, vagy a meglévő elemek, valamely elv alapján történő rendszerbe szervezésével létrehozott szervezési, intézményi, társulási, tevékenységi, forrásbiztosítási, környezeti illesztési, leírható és körülhatárolható, szabályozott, ideiglenes vagy tartós formáció, amelyben a teljes folyamatvolument tekintve, rendszerkeretek közt a biztonsághoz kötődően, a vezetési, irányítási, koordinálási és megvalósítói,kivitelezői, végrehajtói, valamint támogatói, biztosítói, katalizátor al-ésrészrendszerek, elemek egységes egészként, komplex, összehangolt, leírható funkcionális együtteseként működnek, s a működés során a rendszer védelme, folyamatos fejlesztési feltételei is biztosítottak.*"

Ez elméletileg így szépen hangzik, de kérdés, hogy miért nincs konszenzus a kérdésben? Erre akár a konferencia címe is példa lehetne. Miből célszerű kiindulni? Paradox helyzet, hogy a technikai, technológiai lehetőségek kihasználása terén a hagyományos gondolkodásmód továbbélése, az egyre növekvő strukturálatlan információhalmaz ebből is eredő alacsony hatékonyságú generális, speciális, funkcionális feldolgozása és determinált alkalmazása újabb problémákat generál, mert a gondolkodásmódból eredő megoldási szándék, elv, gyakorlat nem mindig követi a változások valós természetét, és ezáltalújrakonzerválja a problémákat. A biztonság vonatkozásában a környezet is paradox, mert bár a globalizáció támogatja a szabványosítást, ugyanakkor a globalizációra épülő főleg gazdasági, üzleti, fejlesztéspolitikai stratégiák éppen a különbségekben rejlő profitot célozzák meg, amire a biztonságot és a rendészetet érintő tényezők is visszavezethetők. A rendészet lehetőségei az információs, digitális, globalizált(és fogyasztói) társadalom korában lényegesen kibővülnek, így a biztonság, rendészet területén is új megoldások születhetnek, azonban ha a technológiai, technikai megoldások mellé nem társul releváns gondolkodás, akkor, a vélt megoldások a már meglévő ellentmondásokat erősítik fel, illetve újakat eredményeznek.[46]

A biztonságkezelés és kockázatmenedzsment létének elemi feltétele azok megfelelő definiáltsága, azaz a rendszerkeretek meghatározása. A folyamatok leírása csak az alap a szemlélet érvényesítéséhez, indokolt az irányítás, szakirányítás rendszerét is kompatibilissé tenni: azaz, hogy milyen erőforrások felhasználásával, milyen stratégiákkal, milyen célok, igények, elvárások elérése érdekében kerül tervezésre, szervezésre a tevékenység, és a vezetési, irányítási, szakirányítási folyamatok mennyire „fedik le" a funkcionális folyamatokat.Ennek keretében mindig vizsgálni kell, hogy a folyamatok mennyire „teljesek". Lényegi kérdés, hogy azonosítottak-e a folyamatok lépései (bemenet, kimenet, tevékenység, döntés, várakozási idő, késedelem, stb.), lezártak-e minden visszacsatolást, azaz mindegyik útvonal elvezet-e a következő lépéshez vagy a folyamat végéhez, stb.[47]A fentiek lapján az auditok relevanciája prognosztizáltan garantálható.

### 3. Biztonság, kockázatok, menedzsment

Vezetés-elméleti anyagokban, probléma-megoldási ajánlatokban elterjedt és gyakori a menedzser, a menedzsment kifejezés.Mindenre, így a biztonságra, kockázatokra is „létezik"valamilyen (jelzős szerkezetű) menedzsment. Azt viszont kevesen veszik

[46] Bővebben lásd: Teke András: Biztonság-rendészettudomány: ami a dimenziók, aspektusok, komponensek és kompetenciák mögött van. Pécsi Határőr Tudományos Közlemények, 2012. XIII. 15-28.o.
[47] U.o.

figyelembe, hogy a hagyományos hierarchikus-bürokratikus szervezetek működésfilozófiája és a menedzsment szemlélet erősen eltér egymástól, annak ellenére, hogy főleg az informális kategóriák, így a projektek, a programok, az ad hoc tevékenységek során deklaratíve megjelennek, de hatékonyságukat alapvetően a formális szervezeti működési tolerancia határozza meg. Miért lényeges ez az összefüggés?

A rendszerszemlélet alapján menedzsment-rendszerekről kell(ene) beszélni, amelynek a csúcsán a topmenedzsment áll, és akkor tölti be igazán a rendeltetését, ha integrált menedzsment rendszerről beszélünk. Az integrált menedzsment több menedzsment (al)rendszer működtetését jelenti egymással kölcsönhatásban, egymásba integrálva. Az integrált menedzsment rendszerek létjogosultságát alátámasztja, hogy egy szervezeten belül a szabályozások, a célképzés, a technikai és technológiai megoldások egységesítése, tehát átfedések miatt a menedzsmenteket célszerű integráltan kezelni, ami egy formális szervezeti működésben azért sem valósulhat meg teljes körűen, mert a teljes vertikumot átfogó informalitást a formális struktúra egyszerűen kizárja.

A biztonsági kockázatokra adandó rendészeti válaszok esetében, ha menedzsmentről van szó, a topmenedzsment mellett feltétlenül célszerű megvizsgálni a stratégiai, a biztonság- és kockázatmenedzsment, illetve a változtatásmenedzsment viszonyát is.[48]

A folyamatok szabályozatlansága, a fentiek részleges, vagy elmaradó érvényesülése ún. inverz szinergiahatást válthat ki. Ahonnan rendszeresen erőforrást kell, lehet elvonni, ott a tevékenység hatékonysága törvényszerűen nem standardizálható. Ahol a tevékenység hatékonysága alacsony, ott a káros folyamatok felerősödnek. Ez így ismétlődik, és az egyik általánossá váló negatív jelenség vonzza a másikat, az ismétlődés mindig nagyobb negatív hatással jár. A menedzsmentnél maradva, a hierarchiának megfelelően legalább három szinten van, lehet jelen: felsőszintű menedzsment (stratégiai szint, az egész rendszerelsősorban jövőbeni működését határozza meg), a középszintű menedzsment (a részrendszerek, folyamatok, egységek irányítása), az alsó szintű menedzsment (a működés operatív irányítása). Ez tovább bonyolítja a klasszikus hierarchikus-bürokratikus hozzáállást.

A hierarchikus-bürokratikus szervezetek úgy küzdenek a változások ellen, hogy folyamatosan változtatások sorozatát generálják feladatmódosulás, forráshiány, korszerűsítés címén úgy, hogy lehetőleg minél kisebb veszteség érje a szervezetet és lehetőleg semmi se változzon. Ebből következik, hogy a hierarchikus-bürokratikus szervezetek esetében a kockázatkezelés elsődlegesen a szervezeti működést, létet szolgálja és nem azt a funkcionális igényt elégíti ki, amelyre a szervezet létre lett hozva, vagy létének alapját jelentené.

A hierarchikus-bürokratikus szervezetek működésében a kockázatkezelés tehát diszfunkcionális motiváltsággal, extenzív forrás-felhasználással, valós vagy vélt biztonságszolgáltatási célzattal, alapvetően hatósági jog-és érdekérvényesítési alapon jelenik meg.

## 4. Audit vagy nem audit?

„*Az audit auditbizonyítékok nyerésére és ezek objektív kiértékelésére irányuló módszeres, független és dokumentált folyamat annak meghatározására, hogy az*

[48] Forrás: http://www.rendeszet.hu/rendeszeti-szoszedet (Letöltés ideje: 2014.06.01.)

*auditkritériumok milyen mértékben teljesülnek.*"[49] Jelen esetben a minőségügyi meghatározásból indulunk ki, de célszerű megvizsgálni, hogy az audit fogalma más nyelveken, egyéb területek vonatkozásában hogyan, milyen megközelítéssel és alkalmazással jelenik meg. (Ezt jelen esetben közlési korlátok miatt nem lehet megtenni.) Az auditálás valamely vállalat szakszerűségének vizsgálata; könyvvizsgálat.[50]

Informatikai biztonsági auditálás: „Az informatikai rendszerre vonatkozó feljegyzések és tevékenységek független átvizsgálása, a rendszer ellenőrzések megfelelőségének vizsgálata, a kialakított szabályzatok és a működtetési eljárások megfelelőségének elérése, a biztonság gyenge pontjainak felfedése az ellenőrzésben, a szabályzatokban és az eljárásokban ajánlott biztonsági változtatások céljából."[51]

Az audittehát a minőségügyi megközelítésből eredeztethető meghatározások alapján valamely tevékenység, eljárás, folyamat, rendszer, szolgáltatás, szervezet, szervezeti egység, elem,valamint az általa kifejtett hatásmechanizmus következményeként megvalósuló állapot, helyzet, az ezt reprezentáló tényállapot, eredménystrukturált, rendszeres és kritikus, valamely standard-del való összevetésen alapuló elemzése, amely kiterjed a vonatkozó tevékenységi körre, az erőforrások felhasználására, valamint az eredményre és a tevékenység, szolgáltatás életminőségre gyakorolt hatására.

Mindenképpen hangsúlyozni célszerű, hogy az audit az előírt, alkalmazható vagy releváns standardok, szabványok, definiált keretek teljesítésének értékelését jelenti.

A hagyományos (számonkérő) ellenőrző-felügyelő szemlélettel ellentétben az audit nem irányulhat a folyamatok direkt vagy indirekt átalakítására, a beavatkozásra,mert ez kizárólag a megrendelő (felső) vezetőség feladata lehet csak. A szabályosan megvalósított audit hatékony eszköz lehet a megrendelő, a vezetőség kezében arra, hogy megállapítsák az eltervezettek vagy követelmények beteljesülését, betartását. Tehát az audit nem hibákat keres, nem felelősöket azonosít és főleg nem bűnbakot feltételez, hanem eltéréseket rögzít. Lényege abban fogható meg, hogy hiteles adatokkal alátámasztva, rámutatva a működés kritikus pontjaira,segíti a vezetőséget a beavatkozás megalapozásában.

A minőségügyben szerepel még a vezetőségi átvizsgálás is, de ez nem azonos az audittal. Az audit hatékonyság-központú, azaz a követelmények betartásának hatékonyságát, megfelelőségét vizsgálja, avezetőségi átvizsgálás hatásosságot vizsgál. Az audit alapelveit szabvány(ok) rögzíti(k). Létezik két fontos fogalom, amelyek determinálják az auditot, ezek az auditkritérium és az auditbizonyíték. A fentiekből világosan következik, hogy mikor van szó auditról, auditálásról és ez nem keverhető össze a helyzetfelméréssel. A kockázatkezelés során az auditbizonyítékok fontos szerepet játszanak a kockázatok megítélésében, de ehhez egyértelmű, dokumentált kritériumoknak is kell lenniük.

Az auditnak nevezett tevékenység sok esetben üzleti céltatú, valamely szolgáltatás pozicionálását preferáló ajánlat megalapozását jelenti, még akkor is, ha hangzatos és hitelesnek tűnő „Audit Review", „General RiskAnalysis", stb. fedőnéven jelenik is meg. Ha nincsenek auditkritériumok, akkor nem auditról van szó. Az audit értékeléséből levont következtetések önmagukban nem képezhetik egy releváns stratégia alapját, a kockázatértékelés pedig nem azonos az audittal.

[49] Útmutató minőségirányítási és/vagy környezetközpontú irányítási rendszerek auditjához (ISO 19011:2002) MSZ EN ISO 19011:2003 (3.1.)
[50] http://idegen-szavak.hu/auditálás (Letöltve: 2014.04.21.)
[51] Az informatikai biztonsági rendszerek követelményei és kialakítása. Mellékletek. Miniszterelnöki Hivatal Informatikai Kormánybiztossága. Budapest, 2014.07.11.

## 5. A kockázatok kezelésének kockázata

„Valaminek" a kezelése a hierarchikus-bürokratikus, így a rendészeti szervezetek esetében annak politikai következménymechanizmusa függvényében az aktuális probléma-hierarchia csúcsán helyezkedik el, ezen belül maga a szó, hogy „kezelés" sok problémát vet fel[52]. A kezelés hierarchikus-bürokratikus szervezeteket érintő problémák esetében rendszerint az „illetékesek megtették a szükséges intézkedéseket" formában kerül kommunikálásra. De maga az intézkedés csak a komplex kezelési folyamat része, tehát sérül a folyamat- és rendszerelvű megközelítés és ezzel együtt maga a „kezelés" csak részleges lehet, ha csak maga az intézkedés, amelynek megalapozottsága nem ismert, kap prioritást. A következmények vizsgálatának gyakori elmaradása, ami az intézkedési kényszer szükségszerű velejárója is lehet, és a keletkezett szándékon túli eredmény, vagy a nem szándékolt következmény újabb kockázatforrás lehet.

A „kezelési folyamat" megvalósulhat egyrészt formálisan, azaz az SZMSZ és a munkaköri leírások, esetleg valamely eljárás, utasítások, szabályzatok, kézikönyvek, ha működik minőségirányítási rendszer és létezik valós szakirányítás, akkor a folyamatleírások alapján, vagy informális módon, projektek keretében, valamely menedzsment, vagy annak vélt formáció működtetésével, erre kijelölt „vezető", „menedzser" „biztos" stb. „vezetésével", ad hoc módon, vagy a két megközelítés nem dokumentált kombinációjával. A formális kezelés esetén a feladatmegoldás algoritmikus szabályozottsága nem tesz eleget a valós probléma-megoldási igényeknek, mert az ismeretlen tényezőkre nem igazán ad választ. A kockázatok kezelését kockázatfilozófiára, kockázatpolitikára célszerű alapozni, amely irányulhat a kockázatok elkerülésére, csökkentésére, megosztására, áthárítására.

Mindez sajátos „filozófia" mentén történik. A kulcsszó: botrány, és az attól való félelem. Egy tudományosnak csak feltételekkel nevezhető, de mindenképpen szellemes és idevágó megközelítés[53] alapján a botránytól való félelem mozgatja a dolgokat a politikában is. Peter Sandman a biztonság vonatkozásában a félelem hatásaira épít. Abból indul ki, hogy ami ellen lehet tenni, de nem tesznek, az botrány! Például egy terrorista-támadás ellen szervezeti szinten nem túl sokat lehet tenni, tehát a szervezetet és a politikumot érintő botrány viszonylag kezelhető lesz, a közúti balesetek, életellenes cselekmények, stb. esetében már lehet valami konkrétat is tenni, tehát a tömeges bekövetkezés nagy port fog kavarni. Ebből már felállítható egy, társadalmi szinten a politikusok által is könnyen kezelhető egyenlet, mi szerint a {kockázat= veszély + botrány}. Mindent az határoz meg, hogy a környezet hogyan reagál a változásokra, a következményekre, ez pedig erősen összefügg a kommunikációval.

Hogy a kockázatkezelés folyamata, vagy a kockázatmenedzsment fejezi-e ki jobban a kockázatkezelés tartalmi és funkcionális igényeit, az megérne egy külön tudományos konferenciát! A kockázatokat nem „keresni" célszerű, hanem az általános vagy funkcionálisan specifikus helyzetfelmérés, elemzés, értékelés, stb. keretében módszertannal alátámasztott módon azonosítani, tehát ha rendészeti eszközökkel kezelhető biztonsági kihívásokat, kockázatokat keresünk, minden bizonnyal találunk is, de kérdés, hogy ezek a valós kockázatok halmazának mekkora hányadát fedik le, alkalmasak-e arra, hogy valamely módszertan alapján feldolgozhatóak legyenek.

---

[52] Részletesen lásd Teke András: A változásokkal összefüggő kihívások kezelésének tipizálható problematikája korunk rendészetében, Pécsi Határőr Tudományos Közlemények XIV. Pécs, 2013. 13-22. o.

[53] Forrás: S. D. Levitt és S. J. Dubner: „Freakonomics" LÖKONÓMIA (Egy kóbor közgazdász a dolgok mögé néz) Európa Könyvkiadó. Budapest, 2007. 192-195. o.

Célszerű tisztázni a kockázatmenedzsment és kockázatkezelés viszonyrendszerét.Indokolt fogalmilag és biztonsági, rendészeti, környezeti illesztés oldaláról definiálni az alábbiakat:

- kockázatpolitika. kockázatfilozófia,biztonsági kockázat, rendészeti kockázat, kockázatmenedzsment, kockázatkezelés, nemzeti biztonsági kockázati mátrix, rendészeti kockázati mátrix, nemzeti rendészeti kockázatpolitika, nemzeti rendészeti kockázatfilozófia, kockázati szint, kockázati környezet, környezetkockázat, kockázattudatosság;
- kockázatok körülhatárolása, kockázatok felismerése, kockázatazonosítás, kockázatelemzés, kockázatértékelés, kockázatbecslés, kockázatközlés, kockázat elfogadás, kockázati lehetőségek, kockázat profilozás, kockázattervezés, kockázati megbízhatóság;
- kockázat mérés, kockázat optimalizálás, kockázat priorizálás, kockázattűrés, kockázat küszöb, kockázatfinanszírozás, kockázatellenőrzés, kockázat monitoring, kockázatminősítés, kockázat validálás, kockázat felügyelet, kockázat felülvizsgálat;
- kockázattűrés, kockázat csökkentés, kockázat áthárítás, kockázatba bevonás, kockázatkerülés, kockázat megelőzés, kockázat átadás, kockázati megbízhatóság, kockázatkezelés kockázata, kockázatkezelés hatékonysága és hatásossága.

Természetesen szükséges mindazon szabványok, standardok, kézikönyvek, segédletek, oktatási anyagok, módszerek azonosítása, adaptálása, elkészítése, bevezetése és alkalmazása, a meglévők aktualizálása, amelyek a fentiek realizálását garantálják.

## 6. Következtetések

Kijelenthető, hogy a digitalizáció és a globalizáció világában könnyen hozzá lehet jutni az új, vagy annak vélt ismeretekhez, anélkül hogy azok funkcionális kompatibilitását előzetesen megvizsgálták volna, így azok alkalmazása a szükséges és elvárható illesztési műveletek nélkül generális kockázatot jelent.

A biztonsági kockázatok kezelése során a dependencia (függőség), az independencia (függetlenség), az interdependencia (kölcsönös függőség), az interreláció (kapcsolati kölcsönösség), az interafektáció (kölcsönös látszat keltés), szimplifikáció (leegyszerűsítés), a szinergia és az inverz szinergia, az üzleti alapú specifikáció fogalmait, tartalmát és kapcsolódását egységes rendszerben lenne célszerű megvizsgálni, ez a plenáris előadáson a prezentáció során látszólag bonyolult ábrával bemutatásra is került, de erre jelen tanulmány keretei nem adnak lehetőséget, akárcsak a különféle releváns elemzésimódszerek bemutatására sem.

Az emberi, közösségi, társadalmi szükségleteket, ezen belül kiemelten a biztonsági szükségleteket felismerve egy nemzetközi üzletág alakult ki, amely igyekszik ezeket kielégíteni, így nem feltétlenül a valós biztonságszolgáltatás élvez prioritást az üzleti megfontolással szemben.

Az „igénykielégítés” sok esetben valamely eszköz vagy módszermarketingalapú értékesítését jelenti, hangsúlyozva, hogy az igénylőnek pontosan „erre van szüksége”, illetve ez a legjobb megoldás.

A helyzetfelmérés nem döntés! Megfelelő műveletek, eljárások nélkül a rendelkezésre álló adat, információhalmaz nem alapoz meg egy döntést. A címben jelzett

audit kapcsán érdemes megnézni, hogy milyen „fedőnév” alatt jelennek meg a „megoldások”!

A folyamatokban rejlő kockázat kiszűrésének, kezelésének minden szabályozási szinten meg kell jelennie, a kockázati minimalizálást segítik a működési alapelvek: szabályosság, szabályozottság, gazdaságosság, hatékonyság, eredményesség.

A kockázatkezelés, mint módszer, a vezetés gyakorlati eszköze, a tervezés és döntéshozatal a végrehajtás alapvető része. A vezetés feladata az, hogy a kockázatokra, amelyek lényegi befolyással lehetnek a célkitűzésekre, tudjon válaszolni oly módon, hogy lehetőség szerint elősegítse a szervezet eredeti céljai elérhetőségének, teljesítésének valószínűségét, s ezzel egy időben minimálisra csökkentse az ezt veszélyeztető tényezők bekövetkeztének esélyét, lehetséges hatását.

Végezetül hangsúlyozni célszerű, hogy a biztonsági kockázatok nem instant módon jelennek meg, mert minden veszélynek, fenyegetésnek van direkt és indirekt biztonsági kockázata, ami csak valamely részterület prioritásainak szelektív biztosításával, direkt intézkedési hozzáállással nem ellensúlyozható önmagában. Ezért társadalmi szinten célszerű a „3C”[54] szellemében megközelíteni a problémát.

## 7. Befejezés

„Távozz el magadtól, hogy eljuss magadhoz!”[55] A biztonság nem szűkíthető le kizárólagosan állami „feladattá”, nem lehet és nem szabad dominánsan kriminálpolitikai, formális statisztikai szemlélettel és a változásokhoz nem igazodó megoldásokkal kezelni. A rendészet evidens módon rendészeti válaszokat adhat, ami részét képezi az összes válasznak és előnyös, ha szinergiára törekszik. A kockázatok körülhatárolása és kezelése statisztikai szemlélettel csak akkor lehetséges, ha az hiteles, validálható, naprakész és integrált adatbázisokra és adekvát módszertanra, szakmai kompetenciára támaszkodik és reális, konszenzusos igény-kielégítésre törekszik.

A megoldások tevékenységi, szabályozási és intézményi hátterét társadalmi szinten célszerű ekvivalenciába hozni. A rendészet rendészeti szemüvegen keresztül látja a problémákat, ami természetes és helyén való, mert funkcionálisan működik, de a biztonsági problémák nem szűkíthetők le rendészeti problémákra és főleg nem rendőrségi problémákra, így a felmerülő kockázatok azonosítása más megoldások tolerálását is feltételezi. A rendészeti intézményi működés hierarchikus-bürokratikus keretei jelenleg nem támogatják a globalizációs, digitális, gyorsan változó környezet kihívásainak főleg informális eszközökkel és módszerekkel kezelhető megközelítését, ezek alkalmazása további problémákat, kockázatokat generál. A modellek, vagy azok részeinek átvétele azok eredeti környezeti feltételeinek hiányában az elvárható honi környezeti illesztés elmulasztásával csak tovább növelik a kockázatokat.

A változó feltételek között a szerepkörök, a funkcionális tartalom, a viszonyrendszer is változik, ha ez nem kerül felismerésre, akkor valószínűleg a kockázatok azonosítása is a korábbi beidegződésekből indul ki, ami determinálja a válaszokat. Hogy a valós helyzet megismerése milyen módszerrel történik, azt maga a helyzet befolyásolja, de a módszertannak is kompatibilisnek kell lennie. Ha auditról van szó, akkor szükséges az auditkritériumokat meghatározni, azonban hazai viszonylatban biztonsági, közbiztonsági,

[54] Communication, Coordination, Cooperation.
[55] Lao-Ce kínai filozófusnak tulajdonított mondás.

rendészeti szabványok, standardok társadalmi szintű felhasználhatósági formában nem állnak rendelkezésre, így a zárt és definiált biztonsági rendszerek kivételével a biztonsági auditnak titulált tevékenységek egyelőre nem tekinthetők hitelesnek és döntési alapot képezőnek. Válaszokat természetesen elvár minden érintett és érdekelt, válaszok voltak, vannak, lesznek és ezek a válaszok olyanok, ahogy a döntések előkészítésre kerülnek, és ahogy az intézményi működés azt lehetővé teszi vagy elvárja.