COBIT
Az informatika tudatos irányításának eszköze

Róth Dénes,
Információrendszer Ellenőrök Nemzetközi Szövetségének Budapesti Szervezete

Az egészségügyi intézmények kivétel nélkül felismerték az informatika nyújtotta lehetőségeket és használják is azokat. Az informatika használata azonban kockázatokkal is jár, ezért a sikerre törekvő szervezeteknek képesnek kell lenniük ezek kezelésére is. A COBIT nemzetközi nyílt szabvány eszközkészletet ad a felső vezetők és az informatikai szakemberek számára, amelynek segítségével megteremthető az informatikai folyamatok szabályozott, kézben tartott működése.

BEVEZETÉS

Minden gazdálkodó szervezet, így az egészségügyi intézmények számára is a sikerességük és hosszú távú fennmaradásuk szempontjából kritikus jelentőségű az információk és az ahhoz kapcsolódó információtechnológia eredményes alkalmazása. A hazai egészségügyi intézmények mára szinte kivétel nélkül felismerték az informatikában rejlő előnyöket. Azonban a lehetőségeket hatékonyan kiaknázó, sikeres szervezetek csak azok lehetnek, amelyek képesek felismerni és kezelni az informatika alkalmazásával járó kockázatokat is. E képességnek viszont előfeltétele az információrendszer folyamatainak tudatos irányítása, kézben tartása – egy „blackbox" belsejében jelentkező kockázatok nem megfoghatóak.

A cikkben bemutatott COBIT egy olyan – nyílt szabvány státuszú – apparátus, módszertani keretrendszer, amelynek segítségével az informatikai folyamatok feletti ellenőrzés úgy valósítható meg, hogy az adott szervezet sajátosságaihoz igazodóan kialakított, változó mélységű és részletezettségű kontrollrendszer tartja egyensúlyban az informatika által nyújtott előnyöket és kockázatokat.

INFORMATIKAI FOLYAMATOK KRITIKUSSÁGA AZ EGÉSZSÉGÜGYBEN

Az egészségügyi intézmények számára az informatikai rendszerekből és folyamatokból olyan kockázatok erednek, amelyek az alaptevékenységre – közvetlenül vagy közvetve, de – stratégiai szinten is hatással vannak. Nézzünk néhányat ezek közül – természetesen megengedve más szempontú és tartalmú csoportosítás létjogosultságát.

Adatok bizalmassága: az egészségügyi informatikai rendszerekben személyes adatokat, köztük nagy arányban különleges adatokat kezelnek; az ezekhez való illetéktelen hozzáférés büntetőjogi és polgári jogi következményekkel járhat.

Informatikai szolgáltatások rendelkezésre állása: az intézmény nem állhat le amiatt, hogy az informatikai rendszer szolgáltatásai és erőforrásai nem elérhetők.

Adatszolgáltatás pontossága: az intézmények bevételének alapját az informatikai rendszer által a biztosítónak szolgáltatott adatok képezik; ezek pontossága, valamint az ezeket előállító folyamat megbízhatósága mind pénzügyi, mind jogi szempontból kiemelkedő fontosságú.

Hatékonyság: az informatikai erőforrások lehető leggazdaságosabb kihasználása minden gazdálkodó szervezet számára fontos kérdés, de a hazai egészségügy pénzügyi helyzetében különösen az.

Minőség: a beteg – mint „vevő" – elégedettsége az ellátás minőségének olyan aspektusaival is, mint pl. a leleteinek, zárójelentésének – mint információnak – a gyors és (akár intézmények közötti) jól szervezett áramlása; valamint az ISO9000-es minőségirányítási rendszerek követelményei szintén kiemelt fontossággal bírnak.

Ellenőrizhetőség: az információs rendszer azon tulajdonsága, hogy működése a megfelelő felhatalmazással rendelkezők – tulajdonos, finanszírozó, leendő befektető, minőségügyi tanúsító, ellenőrző szerv, hatóság – számára ellenőrizhető, auditálható; vagyis az előírásszerű működés formálisan pozitív.

Mérhetőség: az informatikai rendszerek vonatkozásában a vezetői célok kijelölésének és teljesülésük mérésének lehetősége, eszközrendszere; ez a szempont bizonyos tekintetben egyben előkérdése is az előzőekben felsorolt területek kezelésének.

E rövid, bevezető összefoglaló konklúziójaként megállapítható, hogy a hazai egészségügy intézményei – és vezetői – számára sem megkerülhető, hogy az informatikai erőforrásokat és folyamatokat olymódon tartsák kézben, hogy a menedzsment számára ne „vakrepülés", hanem tudatos legyen az informatikai folyamatok irányítása – ezáltal gondoskodva az ezekben a folyamatokban rejlő kockázatok minimalizálásáról.

A COBIT ÁLTALÁNOS BEMUTATÁSA

A COBIT (Governance, Control and Audit for Information and Related Technologies) az IT Governance Institute által kifejlesztett, nemzetközileg elismert és elfogadott nyílt szabvány. A COBIT az Ellenőrzési útmutatót (Audit Guidelines) kivéve online formában bárki számára ingyenesen hozzáférhető. A COBIT élő, organikusan fejlődő eszköz, első kiadása 1996-ban látott napvilágot, jelenlegi, harmadik kiadása

2000-ben jelent meg. A negyedik kiadás a közeli hónapokban várható.

A COBIT szerkezeti felépítése a következő:

- Vezetői Összefoglaló
  - Megvalósítási Segédlet
  - Keretrendszer (átfogó kontroll irányelvek)
    - Vezetői útmutató
      - Érettségi Modell
      - Kritikus sikertényezők
      - Kritikus célindikátorok
      - Kritikus teljesítményindikátorok
    - Részletes Kontroll Irányelvek
    - Ellenőrzési útmutató

A COBIT KERETRENDSZERE

A COBIT abból az egyszerű és pragmatikus alaptételből indul ki, miszerint a szervezet működéséhez szükséges információk biztosításának érdekében az információs rendszer erőforrásait – a tevékenységeket bizonyos természetszerűleg összetartozó folyamatok szerint csoportosítva – menedzselni kell.

Az információs rendszer életciklusa mentén, annak négy fő szakaszához – Tervezés és szervezet, Megvalósítás, Szolgáltatás és támogatás, Monitorozás – kapcsolódóan 34 folyamatot (átfogó kontroll irányelvet) nevez meg; miden egyes folyamatot további tevékenységekre bontva, összesen 318 részletes kontroll irányelvet fogalmaz meg.

A folyamatok és tevékenységek az általános informatikai követelményeknek (eredményesség, hatékonyság, bizalmasság, sértetlenség, rendelkezésre állás, szabályszerűség, megbízhatóság) az adott területre értelmezendő speciális megvalósítása érdekében működnek, miközben informatikai erőforrásokat (emberek, alkalmazói rendszerek, technológia, létesítmények, adatok) vesznek igénybe. E kapcsolatrendszert az 1. számú ábra szemlélteti.

A 2. számú ábrán mutatjuk be – az „Informatikai szolgáltatások folytonosságának biztosítása” folyamaton keresztül – a COBIT „vízesés” modelljét; mind a 34 informatikához kapcsolódó folyamat e formában és szemlélettel kerül definiálásra és részletezésre.

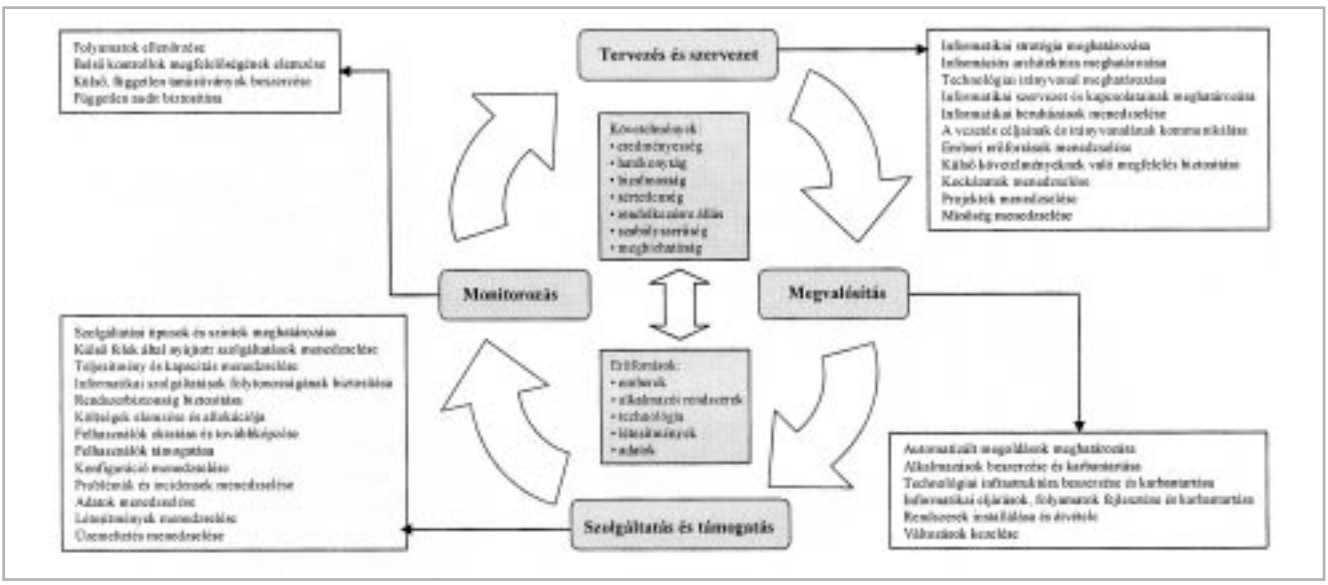
Az életciklus – szakasz – folyamat – tevékenység struktúra alsó rétegeként találjuk az egy-egy folyamathoz (átfogó kontroll irányelvhez) tartozó tevékenységeket (részletes kontroll irányelveket). A cikkben már az előzőekben – és a későbbiek folyamán is – példaként szolgáló Informatikai szolgáltatások folytonosságának biztosítása folyamat tevékenységeinek az egyikét, az IT folytonossági terv tesztelése tevékenységet a COBIT ekképpen definiálja:

„A folytonossági terv eredményességének megőrzése érdekében a vezetésnek rendszeres időközönként, továbbá jelentősebb szervezeti, ügyviteli vagy informatikai változások esetén is értékelnie kell a terv végrehajthatóságát. Ez gondos előkészítést, dokumentálást, a tesztelés eredményeiről történő jelentéskészítést, a tesztelés eredmények értékelését és annak függvényében megfelelő cselekvési terv kidolgozását és végrehajtását foglalja magában.”

Természetesen nem lehet e cikk célja a háromszáznál is több részletes kontroll irányelv egyenkénti ismertetése, azonban ezzel a kiragadott példával is érzékeltetni szeretnénk a struktúra részletezettségét annak legalsó szintjén is.

Mielőtt rátérnénk a COBIT további eszközeinek ismertetésére, mindenképpen szükséges néhány további megjegyzés az eddig érintett kérdésekhez:

- Amint az 1. számú ábrából is kitűnik, a COBIT nem „csak” egy információbiztonsági módszertan, hanem lefedi a szervezet információs rendszerének teljes egészét, mind a folyamatok, mind az erőforrások, mind pedig a követelmények tekintetében.



1. ábra
COBIT keretrendszer

Informatikai szolgáltatások folytonosságának biztosítása	Követelmények							Erőforrások				
folyamattal szemben támasztott **követelmény**	eredményesség	hatékonyság	bizalmasság	sértetlenség	rendelkezésre állás	szabályszerűség	megbízhatóság	Emberek	alkalmazói rendszerek	technológia	Létesítmények	adatok
az informatikai szolgáltatások rendelkezésre állásának biztosítása, az esetleges jelentős kiesések üzleti követelményeinek minimalizálása;	E	M			E			√	√	√	√	√
a követelmény **teljesítésének módja**	*Részletes kontroll irányelvek*											
egy működő és kipróbált informatikai folytonossági terv, illeszkedve a szervezet általános üzletmenet-folytonossági tervébe és összhangban az üzleti igényekkel;	IT folytonossági keretrendszer											
figyelembe véve az alábbiakat:	IT folytonossági stratégia és filozófia											
▪ kritikusság szerinti osztályozás,	IT folytonossági terv tartalma											
▪ alternatív eljárások	IT folytonossági követelmények minimalizálása											
▪ mentési és visszatöltési eljárások	IT folytonossági terv karbantartása											
▪ szisztematikus és rendszeres tesztelés és képzés	IT folytonossági terv tesztelése											
▪ rendszerfelügyeleti és eszkalációs eljárások	IT folytonossági terv oktatása											
▪ belső és külső szervezeti felelősségi körök	IT folytonossági terv kiosztása											
▪ a terv aktiválására, a helyreállításra és a visszaállásra vonatkozó forgatókönyvek	Felhasználói alternatív feldolgozási eljárások											
▪ kockázatkezelési tevékenységek	Kritikus informatikai erőforrások											
▪ „single point of failure" lehetőségek felmérése	Tartalék telephely és erőforrások											
▪ problémakezelés	Tartalékok külső tárolása											
	Tervmódosítási eljárás											

2. ábra
Informatikai szolgáltatások folytonosságának biztosítása
(E-elsődlegesen, M-másodlagosan a jelzett követelmény teljesítése érdekében)

- A keretrendszer által definiált 34 folyamat és 318 tevékenység nem feltétlenül létezik és/vagy releváns minden szervezet esetében; a COBIT nem kőbe vésett szabályokat, hanem készítőinek sok száz emberévnyi gyakorlati tapasztalatán nyugvó megoldási kereteket tartalmaz.
- A követelmények és a folyamatok relációját illetően kiemelendő, hogy a rendelkezésre állás követelménye nem kizárólag az Informatikai szolgáltatások folytonosságának biztosítása folyamatban jelenik meg. Hasonlóképpen a további követelmények mindegyikének teljesülése is több folyamat megfelelő működését igényli, továbbá minden egyes folyamat több követelmény teljesülése érdekében működik.

A COBIT MENEDZSMENT ESZKÖZEI

A keretrendszert alkotó követelmények – erőforrások – folyamatok dimenziók képezik a COBIT statikus részét. De hogyan lehet ezt a statikát felépíteni, mozgásba hozni és önjáróvá tenni? Erre szolgálnak a COBIT menedzsment eszközei, amelyek – a COBIT dinamikáját alkotva – a Vezetői útmutatóban kerülnek bemutatásra.

A menedzsment eszközök központi eleme a folyamatok szabályozottságának érettségi modellje, ehhez kapcsolódnak a kritikus sikertényezők, a kritikus célindikátorok és a kritikus teljesítményindikátorok.

Az Érettségi Modell szerepe, hogy mérhetővé – ezáltal számszerűen is tervezhetővé és ellenőrizhetővé – tegye az egyes folyamatok szabályozottságának, a vezetés általi kézben tartottságának fokát. Az Érettségi Modell hatfokozatú skálát (0 – Nem létező; 1 – Kezdeti/ad hoc; 2 – Ismétlődő, de egyéni kezdeményezéseken alapuló; 3 – Definiált és dokumentált; 4 – Menedzselt és mérhető; 5 – Optimalizált) határoz meg minden egyes folyamatra nézve. Magát az érettséget a következő aspektusok mentén értelmezi: probléma-felismerés és tudatosság – képzés és kommunikáció – folyamatok és mindennapi gyakorlat – technikák és automatizálás – megfelelés és ellenőrzése – gyakorlat és tapasztalat. A 3. számú ábrán látható a COBIT Érettségi Modelljének általános sémája, illetve az Informatikai szolgáltatások folytonosságának biztosítása folyamatra vonatkozó skála. (Itt kell megjegyezni, hogy az egyes folyamatokra vonatkozó értékek a gyakorlatban nem feltétlenül egész számok, hiszen az érettség egyes, fent említett aspektusai eltérő szinten lehetnek.)

Az Érettségi Modell olyan skála, amely egyrészt pragmatikus szemléletű összehasonlítást tesz lehetővé, másrészt amellyel a különbségek egyszerűen mérhetővé tehetők; ezáltal az informatikai folyamatok menedzselésének „profilját" adja.

A kritikus sikertényezők – szintén folyamatonként definiálva – azokat a stratégiai, technikai, szervezeti vagy eljárásbeli körülményeket mutatják, amelyek kézben tartása kritikus fontosságú az adott folyamat irányítása szempontjából. Más megközelítésben: a kritikus sikertényezők a szinte

	Általános skála	Informatikai szolgáltatások folytonosságának biztosítása
0	Érzékelhető folyamat teljes hiánya. A szervezet még fel sem ismerte, hogy megoldást igénylő problémája van az adott területen.	Az informatikai erőforrások, szolgáltatások elvesztéséből vagy kieséséből fakadó kockázatokat, veszélyforrásokat és fenyegetéseket a vezetés nem érzékeli, azok létének nincs tudatában; így a folytonosság biztosítását nem tekinti a vezetés figyelmét igénylő kérdésnek.
1	A szervezet bizonyíthatóan felismerte, hogy megoldásra váró problémákkal néz szembe az adott területen, de nem léteznek formális eljárások. A megoldások individuális alapokon, esetlegesen születnek meg, a vezetés megközelítése szervezetlen.	A vezetés részlegesen felismeri az informatikai szolgáltatások folytonosságával kapcsolatos kockázatok létét, de a folytonosság biztosításával kapcsolatos felelősségek részlegesek és informálisak. A felhasználók megkerülő módszerek használatára kényszerülnek, a hangsúly az egyes informatikai eszközök, nem pedig az üzleti folyamatok védelmén van. A szervezet felkészületlen egy esetleges súlyos kiesés kezelésére. A betervezett üzemszünetek inkább az informatikai szervezet szempontjai és nem az üzleti folyamatok szempontjai szerint kerülnek végrehajtásra.
2	Informálisan (dokumentálatlanul) létező eljárások, amelyeket az adott feladattal megbízottak döntően egyformán végeznek. Nincs formális képzés, a felelősség egyéni, a megbízhatóság nagyban függ az egyén tudásán, ezért a hibák elkövetésének valószínűsége számottevő.	A szolgáltatások folyamatosságával kapcsolatos általános felelősség formálisan is deklarált, de a megoldás tekintetében a megközelítés nem egységes és nem teljes körű. A rendszerek rendelkezésre állását illetően nincs teljes körű jelentési eljárás. Nincsenek dokumentált helyreállítási forgatókönyvek, de létezik az elkötelezettség a szolgáltatások folyamatossága iránt és ismertek az annak biztosítását célzó elvek is. A kritikus rendszerek és szolgáltatások leltára többé-kevésbé megbízható. A vonatkozó eljárások standardizálása megkezdődött, de e folyamat sikere és eredményessége egyéneken múlik.
3	Az eljárások formálisan dokumentáltak és kommunikáltak. Formális ellenőrzés azonban nem létezik, a szabályok betartása az egyéntől függ, az azoktól való eltérés detektálása nem valószínű. Maguk az eljárások részletesen nem kidolgozottak, a mindennapi gyakorlat dokumentálására szorítkoznak.	Az informatikai szolgáltatások folytonosságának tervezésével és tesztelésével kapcsolatos összes felelősség részletesen és egyértelműen deklarált. A tervek, helyreállítási forgatókönyvek az egyes szolgáltatások kritikussága és kiesésüknek az üzletmenetre gyakorolt hatása szerint priorizálva készültek és teljes körűen dokumentáltak. A tervek teszteléséről rendszeres jelentések készülnek. A standardok alkalmazása és a folytonossági intézkedések oktatása egyéni elkötelezettség kérdése. A vezetés egységesen kommunikálja az informatikai szolgáltatások folytonosságának szükségességét. Elszórtan megjelenik egyes kritikus rendszerelemek többszörözése (redundancia), illetve a magas rendelkezésre állást biztosító komponensek használata. A kritikus rendszerek és szolgáltatások leltára folyamatosan és megbízhatóan naprakész.
4	Formális ellenőrző és visszacsatoló funkciók biztosítják az előírások szerinti működést. A szabályzatokat folyamatosan finomítják és a szabályozási rendszert (korlátozott mértékben) automatizált eszközök is támogatják.	Az informatikai szolgáltatások folytonosságával kapcsolatos felelősségek ellenőrzöttek, a tervek karbantartásával kapcsolatos felelősségek is deklaráltak. A tervek karbantartásának tevékenységei figyelembe veszik az üzleti és a technológiai környezet változását, a korábbi tesztek eredményeit. Az informatikai szolgáltatások folytonosságával kapcsolatos adatokat strukturáltan gyűjtik, elemzik, jelentik és e tevékenységek szükség esetén korrigáló intézkedéseket generálnak. A szolgáltatások folytonosságával kapcsolatos folyamatok oktatása megtörténik. Az egyes rendszerelemek többszörözésével (redundancia) kapcsolatos gyakorlatok (beleértve a magas rendelkezésre állást garantáló komponensek alkalmazását is) bevezetésre kerültek, és azok kölcsönhatásban vannak a folytonossági tervekkel. Az egyes informatikai szolgáltatások kiesésével járó incidensek részletes elemzésére sor kerül.
5	A folyamat az ismert „legjobb gyakorlat" (best practice) szerint működik, amit a folyamatos finomítás, és más szervezetek érettségi szintjével való folyamatos összevetés biztosít. A szabályozás informatikai eszközöket is integrál a minőség és az eredményesség, illetve a változási és adaptálási képesség növelése érdekében.	Az informatikai szolgáltatások folytonosságát biztosító folyamatok egységesek, integráltak, proaktív szemléletűek, önellenőrzők, önkorrigálók, figyelembe veszik benchmarking információkat és az aktuálisan elfogadott legjobb gyakorlat (best practice) szerint működnek. A szolgáltatások folytonosságának biztosításával kapcsolatos, harmadik feleket (szállítók, alvállalkozók, szolgáltatók) érintő minden igény a szerződésekben teljes körűen szabályozott, a rendelkezésre állással kapcsolatos feltételek kötelező elemei a szerződéseknek. Az egyes tervek rendszeresen és teljes körűen tesztelésre kerülnek, a tesztek eredményei a karbantartási folyamatokon keresztül a visszacsatolás részét képezik. Az általános üzletmenet-folytonossági tervek, az informatikai szolgáltatások folytonosságát célzó tervek és a kritikus rendszerelemek többszörözésének gyakorlata teljes körűen integrált rendszert alkotnak, amely rendszer az integráltság és az innováció segítségével költségek szempontjából is optimalizált. A vezetés deklarált célja a single-point-of-failure (csak egyszeresen védett) lehetőségek teljes felszámolása; ezt a folyamatot intézkedésekkel is támogatja.

3. ábra
Az Érettségi Modell általános és speciális szintjei

bizonyosan szükséges (de önmagukban még nem elégséges) legfontosabb, ugyanakkor egyszerűen és világosan megfogalmazható teendőket, megoldandó feladatokat jelölik.

A kritikus célindikátorok és a kritikus teljesítményindikátorok magukat az informatikai folyamatokat mérik. Döntő különbség azonban, hogy míg a célindikátorok a folyamat végeredményének teljesülését (vagy nem teljesülését) mutatják, addig a teljesítményindikátorok azt jelzik: a folyamat a számára definiált cél felé halad-e. Ebből következően az előbbiek általában az egyes általános informatikai követelményeknek (lásd: keretrendszer) az adott folyamat esetében értelmezhető megvalósulását – mint a folyamat céljának teljesülését –

reprezentálják; utóbbiak olyan – gyakran számokban vagy százalékos arányban kifejezett – értékek, amelyek arra vonatkoznak, hogy a folyamat el fogja-e érni a célját.

Az Informatikai szolgáltatások folytonosságának biztosítása folyamat kritikus sikertényezőit, célindikátorait és teljesítményindikátorait a 4. táblázatban foglaltuk össze. Természetesen a COBIT itt bemutatott menedzsment eszközeire is érvényes az a korábbi kitétel, miszerint a COBIT nem kőbe vésett szabályok kinyilatkoztatása; az eszközök alkalmazása itt is az adott szervezet igényeihez és sajátosságaihoz igazodva változhat. Ez megnyilvánulhat egyes elemek elhagyásában, átfogalmazásában, új elemek definiálásában.

Azzal, hogy – legalábbis a 34 informatikai folyamat egyikére – az Érettségi Modell szintjeit és a kritikus sikertényezőket bemutatjuk, egyben lehetőséget is adunk egy rögtönzött önértékelés elvégzésére, amelynek alapján az itt példaként említett terület szabályozottsága, kézben tartottsága, megfelelő működése megbecsülhető.

TAPASZTALATOK ÉS LEHETŐSÉGEK AZ EGÉSZSÉGÜGYBEN

A COBIT szektorfüggetlenül alkalmazható, a publikált nemzetközi esettanulmányok között a legkülönfélébb szervezeteket (közigazgatás, pénzügyi szektor, egészségügy, ipar és kereskedelem, szolgáltatások) találjuk. Ami az egészségügyet illeti: hazai alkalmazásról jelenleg nincs tudomásunk, az online formában (www.isaca.org/COBIT) hozzáférhető esettanulmányok között az egészségügyi szektorra vonatkozóan két említésre érdemes is található. Bár földrajzilag egyik sem nevezhető közelinek – egy dél-afrikai magántársaság és egy ausztrál tartományi egészségügyi hálózat; mindkettő kórházakat és más egészségügyi intézményeket működtet –, de azok szempontjaik (folyamatok kézben tartása, informatikai kockázatok csökkentése), amelyekre való tekintettel a COBIT használata mellett döntöttek, nagyon is közel állnak ahhoz, amik a hazai egészségügyi intézményeknél is felmerülnek.

A magyar egészségügyi szektor számára adott a lehetőség, hogy ezt a nemzetközileg széles körben elfogadott módszert igénybe vegye az informatika tudatos vezetésének eszközeként, a szabályozott működés kialakítására, ellenőrzésére és a kockázatok csökkentésére. A COBIT magyar nyelvű változata ingyenesen letölthető a Szervezet honlapjáról (www.isaca.hu), illetve nyomtatott formában is hamarosan megvásárolható lesz. A megoldandó probléma egyrészt már most is adott, másfelől a megoldások kidolgozását sürgető igények a jövőben csak növekedni fognak. A magánbefektetők megjelenése, az EU-csatlakozás, az intézmények közötti egyre szorosabb informatikai kapcsolatok kiépítése, az informatikai tevékenységek kiszervezése mind

Kritikus sikertényezők	Kritikus célindikátorok	Kritikus teljesítményindikátorok
Szünetmentes áramellátást biztosító rendszerek telepítése és rendszeres tesztelése. A rendelkezésre állást veszélyeztető kockázatok proaktív felmérése és kezelése. Az infrastruktúra kritikus komponenseinek azonosítása és folyamatos monitorozása. Az informatikai szolgáltatások folytonosságának biztosítása egységes cselekvéssorozat: előrelátó kapacitástervezés, magas rendelkezésre állást biztosító komponensek alkalmazása, a szükséges redundancia megteremtése, vészhelyzeti (helyreállítási) forgatókönyvek dokumentálása és tesztelése, single-point-of-failure (csak egyszeresen védett) lehetőségek megszüntetése. A korábbi kiesésekből adódó tanulságok levonása, a helyreállítási tervek tesztelése során szerzett tapasztalatok felhasználása a tervek finomítására. A rendelkezésre állási követelmények rendszeres elemzése. Az eszkalációs eljárások a rendelkezésre állási követelmények szerinti osztályozáson alapulnak és készségszinten ismertek. Az informatikai szolgáltatások kieséséből származó költségek – ahol lehet – ismertek; ezek az adatok a vezetést megfelelő védelmi intézkedések kidolgozására sarkalják.	Informatikai szolgáltatások segítségével működő azon fontos üzleti folyamatok száma, amelyek folytonossága megfelelő módon biztosított. Nem fordul elő anyagi vagy erkölcsi kárt okozó kiesés az informatikai szolgáltatásokban. Rendszeresen és formálisan bizonyítható a folytonossági tervek működése. A kiesések (downtime) összideje csökkenő tendenciát mutat. Az informatikai infrastruktúra azon kritikus komponenseinek a száma, amelyek rendelkezésre állását automatikus felügyeleti rendszer monitorozza.	Az informatikai szolgáltatások folytonosságával kapcsolatos, még megoldatlan problémák száma. Kieséssel járó incidensek száma és kiterjedése, időtartamuk és okozott hatásuk alapján. Változások (szervezeti, szabályozási, technikai) bekövetkezése és a folytonossági tervek azok alapján történő frissítése között eltelt idő. Egy incidens észlelése és a folytonossági (katasztrófaelhárítási) terv végrehajtása között eltelt idő. A folytonossági (katasztrófaelhárítási) terv végrehajtása és a szolgáltatások normalizálása (normál üzem visszaállítása) között eltelt idő. Az informatikai szolgáltatások folytonosságával kapcsolatos oktatás gyakorisága. Az informatikai szolgáltatások folytonosságával kapcsolatos tesztelés gyakorisága. A folytonossági (katasztrófaelhárítási) tervekben felfedezettek hibák, hiányosságok és azok kijavítása között eltelt idő.

4. ábra
Sikertényezők, célindikátorok és teljesítményindikátorok az Informatikai szolgáltatások folytonosságának biztosítása folyamatban (példák)

olyan – e lap hasábjain is rendszeresen felbukkanó – kérdések, amelyek az informatika menedzselésével kapcsolatban is feladatokat szabnak, mégpedig nem is elsősorban az informatikai vezető és a rendszergazdák, hanem az intézmények felső vezetése számára.

ISACA

Az Információrendszer Ellenőrök Nemzetközi Szövetségének Budapesti Szervezete az informatikai irányítás, szabályozás, biztonság és ellenőrzés területének szakembereit tömörítő, Magyarországon 1991 óta folyamatosan működő és fejlődő non-profit szakmai egyesület.

ÖSSZEFOGLALÁS

A COBIT által nyújtott, testre szabható eszközök segítségével a hazai egészségügyi intézmények is képesek lehetnek az informatika folyamatok irányítására, kézben tartására. A COBIT megközelítése a szervezet alaptevékenységéhez szükséges információk szolgáltatásában látja az informatika alkalmazásának szerepét, ebből eredően az informatikai folyamatokkal, tevékenységekkel szemben támasztott követelményeket is az alaptevékenység céljaiból vezeti le. A COBIT – mindenekelőtt gondolkodásmódjában és terminológiájában – elsősorban nem (számítás) technikai jellegű, mindazonáltal a módszer alkalmazásának végtermékeként informatikai-számítástechnikai követelmények strukturált rendszere (is) előáll, illetve a már kiépült irányítási rendszer képes arra, hogy a működés technikai jellegű monitoring adatait visszacsatolja és „konvertálja” az alaptevékenység céljaihoz igazodóan (az informatikával szemben) megfogalmazott „üzleti” jellegű követelmények teljesülésének értékelése céljából. Mindezzel pedig átláthatóvá, ellenőrizhetővé teszi az informatikai folyamatokat.

A cikk keretében bemutatott példák kivétel nélkül az információbiztonság egy részterületére, az informatikai szolgáltatások folytonosságra koncentráltak, mivel jellemzően az információbiztonság problémáinak megoldása közben jelenik meg az igény az informatika szabályozása iránt. Ugyanakkor hangsúlyozni kell: nem csak biztonsági, hanem (többek között) eredményességi, hatékonysági, megbízhatósági kockázatok is fenyegetik az informatikai rendszereket; ezek pedig hasonló „terápiát”, vagyis az informatikai folyamatok szabályozott működésének megteremtését igényelik, mégpedig az összes követelményt egységes szemlélettel átfogó módszerrel. A COBIT legfőbb erőssége ennek az átfogó, egységes szemléletnek a következetes képviselete, ami az alaptevékenységből levezetett igények és az informatikai lehetőségek teljes körű összehangolásának lehetőségét adja.

A szerkesztőség ezt a cikket gondolatébresztőként ajánlja a szakemberek számára annak érdekében, hogy ez a nemzetközi szabvány a hazai egészségügyben széles körben alkalmazható-e. Várjuk olvasóink ezzel kapcsolatos szíves véleményét.
Szerk.

IRODALOMJEGYZÉK

[1] IT Governance Institute: COBIT – Governanace, Control and Audit for Information and Related Technologies (Framework, Control Objectives, Management Guidelines), 2000. (Az ábrák és az idézetek a magyar fordítás alapján, az Információrendszer Ellenőrök Nemzetközi Szövetségének Budapesti Szervezete engedélyével. A „COBIT” az IT Governance Institute oltalom alatt álló védjegye.)
[2] www.isaca.org/COBIT, www.itgi.org (esettanulmányok)

A SZERZŐ BEMUTATÁSA

Róth Dénes 1993-ban szerzett diplomát a Kandó Kálmán Műszaki Főiskola informatika szakán, jelenleg az ELTE jogi szakokleveles mérnöki posztgraduális képzésének hallgatója. CISA (Certified Information Systems Auditor – okleveles információrendszer ellenőr) és CMC (Certified Management Consultant – okleveles vezetési tanácsadó) nemzetközi minősítésekkel, valamint elektronikus aláírással kapcsolatos szolgáltatási szakértői (HÍF) és igazságügyi szakértői kinevezéssel rendelkezik. Jelenleg az informatikai rendszerekkel kapcsolatos szabályozási, kockázatkezelési és biztonsági tanácsadással, továbbá az informatikai szerveztek, folyamatok, rendszerek auditálásával foglalkozó Proteus Consulting Kft. ügyvezetőjeként dolgozik.