BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 1. SZÁM

Az IT biztonsági programok sikerességére ható szervezeti képességek I.

The impact of organizational capabilities on the success of IT security programs I.

Kiss Miklós
Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
ORCID: 0000-0002-8826-0573
kismkls@gmail.com

Összefoglalás: **nagy változást hozott a 2013. évi L. törvény a magyar közigazgatási szféra számára. Ezen szervezeteknek ezentúl mind a jelenleg üzemeltetett, mind a jövőben kialakításra kerülő rendszerek tekintetében meg kell felelni az új, eddig az állami környezetben nem alkalmazott információbiztonsági keretrendszernek. Jelen cikk bemutatja mindazon – a szervezet részéről fontos – szempontokat és kompetenciákat, amelyek hatással vannak a törvény által megfogalmazott feladatok végrehajtására, különös tekintettel az Európai Uniós források segítségével megvalósuló beruházásokra, valamint összeveti az állami és privát szférát jellemző kompetenciákat.**

Kulcsszavak**:** COBIT, ITIL, projekt, kiberbiztonság, kompetencia

Abstract: **the L law of 2013 has changed the Hungarian public administration sector significantly. Beginning 2013 these organizations – in regards of currently used and newly established systems – have to comply with this new information security framework that has previously not been applied in the government sector. This writing will showcase all considerations and competencies important for an organization, which affect the execution of regulatory tasks, especially regarding investments funded by the European Union. It will also compare competencies of the government and private sector.**

Keywords**:** COBIT, ITIL, project, cybersecurity, competency

1 BEVEZETÉS

Magyarországon 2013-ban jelentős változás következett be mind az állami és önkormányzati szervek, mind a privát cégek informatikai rendszereinek napi üzemeltetésében, illetve a jövőben kialakításra kerülő IT rendszerek külső és belső fejlesztési projektjeiben.

Amíg az államigazgatási szervekre a 2013. évi L. törvény, azaz az Információbiztonsági törvény (Ibtv) [1] és végrehajtási határozatai ró ki jelentős feladatokat, addig a vállalatokra az Európai Unió Adatvédelmi rendelete, azaz a GDPR (General Data Protection Regulation) [2], illetve a NIS irányelv (A hálózati és információs rendszerek biztonsága) [3] fog kifejteni jelentős hatást. A felkészülési folyamatot minél hamarabb meg kell kezdeniük az érintett szervezeteknek, hogy készen álljanak a 2018. május 25-én életbe lépő változásokra. Ne felejtsük el azonban, hogy a GDPR hatása ugyan a civil szektorban fog jelentős változásokat hozni a személyes adatok kezelésében, mindazonáltal számolni kell a közigazgatási szervezetek érintettségével is. [4]

Mindezen keretrendszerek alapjaiban alakították át a kormányzati és privát szféra IT biztonsággal való kapcsolatát. A megváltozott IT fejlesztési és beruházási igények velejárója, hogy a beszállítóknak, integrátoroknak és fejlesztőknek is változtatni kell a jelenlegi stratégiájukon, valamint eme szándékoknak a vállalati kontrollokban is előbb-utóbb meg kell jelennie.

A kontrollok kiépítése és a szervezetek érettségi szintjének meghatározása most is zajló folyamat. A jelenlegi turbulens környezetben azonban az IT projektek lebonyolítása is egyre komplexebb feladatot ró mind a kormányzati szektor, a koordináló szervezetek és hatóságok, mind a beszállítók számára.

Ahhoz, hogy ezek a határozott, jól definiált kritériumok teljesülhessenek, szükség van arra is, hogy az érintettek meg tudják fogalmazni az igényeiket, tisztában legyenek a saját képességeikkel, valamint a folyamatos fejlesztés keretében magasabb szervezeti szintre tudjanak jutni. [5]

A cikk rámutat arra, hogy az egyes szervezeti jellemzők és kompetenciák jelen vannak-e, illetve milyen mértékben jellemzik a különböző szervezeteket, valamint a hozzájuk tartozó ellátási lánc egyéb elemeit (beszállítók, integrátorok, fejlesztők stb.).

Ennek feltérképezése történik meg az öt, legfontosabb kompetenciacsoport aktuális helyzetét vizsgáló kérdőíves kutatás keretében:

- a szervezet stratégiájának mélysége,
- a szervezet érettségi jellemzői,
- a szervezet kontrollkörnyezete,
- a szervezet fejlődési dimenziói,
- a projektek eredményeinek jellemzői.

A cikksorozat első része bemutatja a rendszerre ható, illetve jelentős hatással bíró tényezőket, míg a második rész arra a kérdésre keresi a választ, hogy a négy magyarázó változó (stratégia, érettség, kontroll, valamint a fejlődés) hatással van-e a projekt sikerességi kompetenciákra, valamint igyekszik feltárni a kompetenciacsoportok legdominánsabb jellemzőit is.

2 A KERETRENDSZER BEMUTATÁSA

2.1 Az Információbiztonsági törvény

Szerencsére a jogalkotók felismerték annak jelentőségét, hogy a hazai elektronikus adatvédelem kiemelt fontossággal bír Magyarország és egyben az Európai Unió érdekei tekintetében, ezért 2013-ban elfogadásra került az ide vonatkozó törvény: a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. [6]

Ennek a jogszabálynak az életre hívását a 2001. november 23-án, Budapesten, az Európa Tanács által jóváhagyott egyezmény (Convention on cybercrime) elfogadása alapozta meg. [7]

A törvény, illetve a végrehajtási határozatai részletesen szabályozzák a hatáskörébe utalt szervezetek számára (állami és önkormányzati szervek), hogy [8]

- mindenekelőtt fel kell mérniük informatikai „érettségi" szintjüket, saját rendszereik tekintetében,
- majd kezelniük kell azon helyzeteket, amikor az adatok, illetve rendszerek nem egyeznek meg az elvárt szinttel (azaz cselekvési tervet kell kidolgozniuk, azonban ebben az esetben a jogszabály türelmi időt biztosít számukra),
- végül a jövőben kialakítandó rendszereiket (itt már nem áll rendelkezésre türelmi idő) azonnal meg kell feleltetni az adott biztonsági szint követelményeinek.

A fenti felsorolásból látható, hogy mennyire fontos a szervezetek jelenlegi és a jövőbeli érettségi szintje, a kontrollok implementálása, valamint a szervezeti, esetleg IT stratégiák megléte ahhoz, hogy a megfelelő fejlődési ütem biztosítva legyen, valamint a sikeresen kivitelezett projektek száma az elvárásoknak (az Európai Uniós pénzlehívásokon túl itt meg kellene jelennie a minőségi és biztonsági kritériumoknak is) megfelelően alakuljon.

Fontos továbbá, hogy a törvényi környezet hatással van (pozitívan, de akár negatívan is) mindazon vállalatokra, akik a közigazgatásban kvázi beszállítóként vagy integrátorként vesznek részt. [9]

Mi a helyzet a jövőben megvalósításra kerülő projektekkel? Honnan tudható, hogy a kellő számú kontrollt tartalmazza-e az eredménytermék? A kontrollok megfelelően működnek-e? Milyen lehetőség van ezek ellenőrzésére, illetve a tervezési fázisban miként lehet az érdekeket érvényesíteni?

Erre a választ a törvény a már korábban idézett feladatszabása adja meg (projektek ellenőrzése). A napi működési szintre vonatkoztatva azonban praktikusan ki kell választani azokat a kiemelt, nagy súlyt képviselő projekteket, amelyek ellenőrzése kézben tartható, utókövetése elvégezhető.

Ennek érdekében a NKI a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program (KÖFOP) projektjeinek tekintetében végzi az ellenőrzési és tanácsadási feladatokat.

Az informatikai relevanciával bíró projekteknél az „üzleti" célok elérését különböző módokon lehet elvégezni, ehhez gyakran modelleket kell választani (pl. felhő alapú szolgáltatások). Ezek azonban érthető módon korlátozva vannak a kormányzati szereplők számára. Ennek betartásának az ellenőrzése is az NKI feladatai közé sorolandó, és nagyban befolyásolja a közigazgatási szervek beszerzési és projekt stratégiáját. [10]

A KÖFOP program célja: „Az operatív program intelligens, fenntartható és inkluzív növekedésre vonatkozó uniós stratégiához és a gazdasági, társadalmi és területi kohézió megvalósításához való hozzájárulására vonatkozó stratégia". [11]

2.2 Érettségi modellek és szolgáltatásmenedzsment

A szervezet aktuális fejlettségi állapotának jellemzésére szükséges volt egy olyan koordinátarendszer, valamint iránymutatás megalkotása, amelyben egyaránt értelmezhető maga a szervezet, a szervezet által nyújtott szolgáltatások, valamint ezen szolgáltatások elvégzéséhez szükséges folyamatok összesítése, illetve a szükséges kompetenciák minőségi jellemzése. [12]

Számos nemzetközi- és hivatalos szervezet adott ki részletes leírást, iránymutatást, hogy miként is kell felépíteni úgy a vállalati portfoliót, hogy az fenntartható, hosszútávon működtethető, ugyanakkor jövedelmező legyen.

A korlátos vállalati erőforrások megfelelő allokációjában segít az észak-amerikai szervezet: az ISACA által kidolgozott COBIT (Control Objectives for Information and Related Technology) ajánlás, amely természetesen nem kötelező jellegű egyetlen szervezetre nézve sem, azonban implementálásával – a jellemzően IT, de egyéb – üzleti folyamatok optimalizálhatók, a szervezet piaci megítélése erősen fejleszthető.

A másik metodológia az un. "IT best practice" azaz legjobb megoldásokon alapuló, az Egyesült Királyság kormányzatának gondolatát tükröző, az informatikai beszerzésnek minőségbiztosítása érdekében életre hívott, már-már szabványként kezelt informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, az ITIL. [13]

Mind a két módszertan ajánlásokat tesz arra nézve, hogy miként lehet meghatározni, mérni, javítani és akár szabványosítani a szervezet által végzett tevékenységeket. Nagyon fontos kiemelni, hogy a folyamatok definiálása után nem ér véget a feladat, kívánatos az elért eredmények fenntartása, illetve folyamatos fejlesztése.

Az üzleti folyamatok tervezése (BPM, Business Process Management) [14] és az üzleti folyamatok üzemszerű állapotától való eltérések kezelése, azaz az üzletmenet folytonosság tervezéséhez is elengedhetetlen eme metodológiák implementálása. (BCP, Business continuity planning). [15]

Ne higgyük azonban, hogy ez a két (és számtalan más) nemzetközileg elismert eljárás szöges ellentétben áll egymással. A későbbiekben bemutatásra kerül, hogy ezek a szabályrendszerek nagyon jól egybeilleszthetők, a közöttük lévő szinergiák így könnyen kihasználhatók.

Az ITIL, valamint COBIT szemléletek olyan erős hatást fejtettek ki az iparágra, hogy az eljárások mélyen beépültek mind az észak-amerikai kontinensen (NIST 800-53) [16], mind Európában (ISO 27001:2013) megalkotott szabványokba. [17]

Azok a szervezetek, amelyek felismerik, hogy a piacon való megmaradásukhoz, illetve az állami szervezeteknél a hatékony feladat végrehajtáshoz elengedhetetlen valamely ismert eljárás implementálása, igen komoly versenyelőnyhöz juthatnak (közigazgatási intézményeknél ez más formában, akár állampolgári elégedettségben, akár nagyobb társadalmi felelősségvállalásban nyilvánulhat meg).

Mivel a kutatás alapváltozóit képezik a most nagy vonalakban ismertetett szabályrendszerek (egyes definiálható, mérhető és kiértékelhető paraméterei), ezért a részletesebb bemutatásuk elkerülhetetlen.

A felmérés alapját képező változók, azaz a stratégia és a kontrollok megléte, a fejlődés, az érettségi szintek, valamint a projekteredményesség beazonosításához meg kell ismerkednünk azokkal a szemléletmódokkal, amelyek alapján a kutatás módszertanban megfogalmazott céloknak megfelelően a kérdőív összeállítása megtörtént.

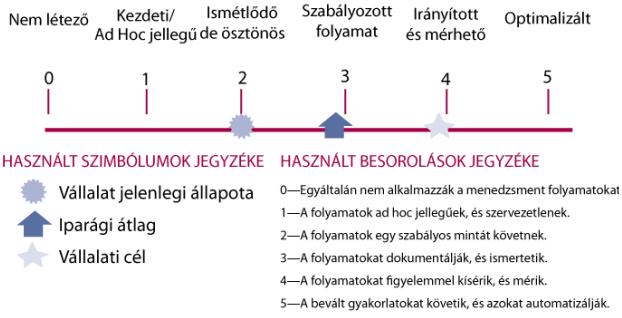
2.3 A COBIT szervezetérettségi szempontrendszere

Az ISACA által megalkotott COBIT egy olyan ún. keretrendszer, amely segítségével az IT menedzsment és az IT irányítás szervezeti szintű megvalósítása elvégezhető. [18]

A keretrendszer hat fokozatú (a nulladik szint egyértelműen a nem létező folyamatokra utal) skálát (érettségi modellt, 1. ábra) határozott meg, hogy az egyre magasabb szervezeti szintek beazonosíthatók legyenek: [19]

- a 0. szinten a folyamatok nem figyelhetők meg,
- az 1. szinten már vannak jelek arra nézve, hogy a vállalkozás felismerte azokat a területeket, amelyre energiát kell szentelnie, de a folyamatok nem szabványosítottak, azok inkább ad hoc jellegűek,
- a 2. szinten a folyamatok hasonló eljárásokat követnek, de nincsen oktatás, nincs tájékoztatás,
- a 3. szinten az eljárások szabályozottak és jól dokumentáltak,
- a 4. szinten a mérés is elvégezhető,
- az 5. szinten a folyamatok optimalizáltak, azok folyamatos fejlesztése megvalósult.

1. ábra: A COBIT szerinti érettségi szintek [20]



2.4 Az Information Technology Infrastructure Library (ITIL) perspektívája

Míg a COBIT egy specifikusabb eljárás eszköztárat biztosít a szervezetek hatékony működtetésére, addig az ITIL módszertan a legjobb eljárásokat ajánlja – és dolgozza egy egységes rendszerbe. Ezek a legjobb gyakorlatok lefedik a szervezetek szolgáltatás portfóliójának teljes életciklus menedzsmentjét, kezdve a tervezési fázistól, egészen a megszűnő szolgáltatások kivezetéséig. [21]

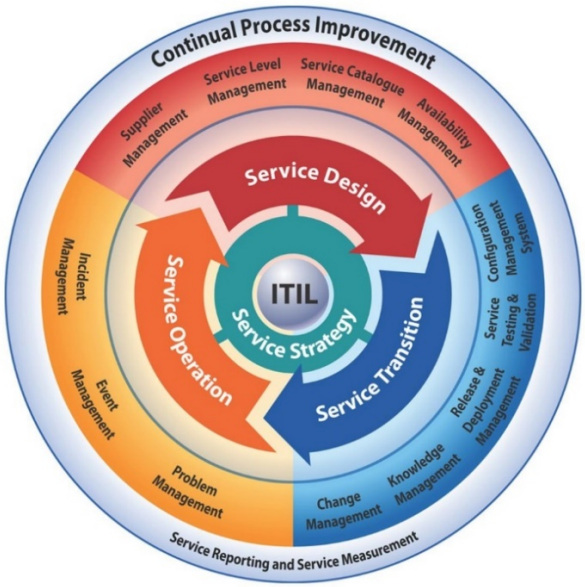
Az ITIL ereje a már korábban említett teljes szolgáltatás életciklus lefedésében megmutatkozik, amennyiben ez a szemlélet implementálva van egyéb szervezeti funkciókba is, úgy jelentős hatást fejt ki a projektek tervezésére, végrehajtására és nem utolsó sorban az utókövetésre is. [22]

Az üzleti folyamatok pontos feltérképezése, menedzselése, valamint a folyamatos fejlesztés ugyancsak megjelenik ebben a metodikában is.

A teljes folyamatmenedzsmentet tehát az ITIL öt egymáshoz kapcsolódó, egymásra épülő tevékenységek végrehajtásával tudja biztosítani: [23]

- Szolgáltatásstratégia: piaci lehetőségek azonosítása, képességnövelés, értéknövelő tevékenység,
- Szolgáltatástervezés: projekt-terv a stratégiában felvázolt szolgáltatás kivitelezésére,
- Szolgáltatáslétesítés és változtatás: a megtervezett szolgáltatás létesítéséhez szükséges konkrét megvalósítás,
- Szolgáltatásüzemeltetés: a folyamatos üzemeltetés biztosítása,
- Állandó szolgáltatásfejlesztés: a minőségmenedzsment tevékenység keretében a szolgáltatások folyamatos fejlesztése következik be.

2. ábra: Az ITIL koncepciója [24]



2.5 Az Információbiztonsági törvénybe implementált modellek és az informatikai rendszerek érettségi szintjei

A hazai törvény és jogszabály gyakorlati útmutatója, azaz a 41/2015. Belügyminisztériumi rendelet szoros összefüggést mutat a NIST 800-53, valamint a COBIT módszertanban megjelenő kontroll és érettség szemléletével.

A Hatóság (NEIH) számára minden közigazgatási szerv köteles megküldeni az informatikai rendszereinek osztályba sorolását (1. táblázat). Az osztályba sorolt rendszerek szintje függ a kezelt adatok minősítésétől, az informatikai rendszerek értékétől, illetve az adatok elvesztése vagy kompromittálása esetén bekövetkezett társadalmi és anyagi kár mértékétől.

1. táblázat: Besorolási útmutató részlete [25]

1.	Sorszám	Intézkedés típusa	Biztonsági osztály				
2.			1	2	3	4	5
3.	2003.01.01	Szervezeti szintű alapfeladatok					
4.	3.1.1.1.	Informatikai biztonsági szabályzat	X	X	X	X	X
5.	3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelős személy	X	X	X	X	X
6.	3.1.1.3.	Az intézkedési terv és mérföldkövei	0	X	X	X	X

A bonyolult besorolási procedúra, valamint az egységes nyelvezet érdekében a Hatóság segédletet biztosít a szervezetek számára, amely nagyban megkönnyíti mind a közigazgatási intézmények, mind magának a Hatóságnak a munkáját.

Amennyiben az elvárható besorolási és a valós osztály között negatív eltérés mutatkozik, akkor az adott szervezetnek intézkedési tervet kell készítenie a megkívánt érettségi szint eléréséhez.

A jogszabályok értelmében a kontrollokat három rétegben kell alkalmazni annak érdekében, hogy a kockázatkezelés a teljes környezetre meg tudjon valósulni:

- fizikai: pl.: beléptető rendszerek,
- adminisztratív: pl.: belső szabályzás, kockázatelemzés,
- logikai. pl.: azonosítás, hitelesítés, hozzáférés ellenőrzése.

A logikai intézkedések alcsoportjai között felfedezhetjük az ún. COBIT kocka üzleti igények dimenziójában elhelyezkedő ún. CIA modellt (COBIT). Ennek a modellnek a hazai jogszabályi környezetbe történő implementálása teljes mértékben megtörtént.

A CIA modell kritériumrendszere pontosan jellemezni tudja a szervezet informatikai rendszereinek érettségét, azaz megmutatja a rendszer biztonsági képességeit:

- Confidentiality, bizalmasság:
- Integrity, sértetlenség,
- Availability, rendelkezésre állás aspektusából.

Az egyes biztonsági osztályok elérésének ugyanis igen komoly feltételei vannak, kezdve a fizikai eszközök minőségétől, a kollégák tudásának és kompetenciájának bővítésén át magának a szervezet érettségének (stratégiai tervezés, projektszemlélet stb.) magasabb szintre történő eljuttatásáig.

3 A PROJEKTMENEDZSMENT ALAPKÉRDÉSEI

Különösen fontos tisztázni tehát azt, hogy mitől függ egy projekt sikeres végrehajtása, mi az, ami az adott projektet eredményessé, a megvalósított eredményterméket pedig elfogadhatóvá teszi.

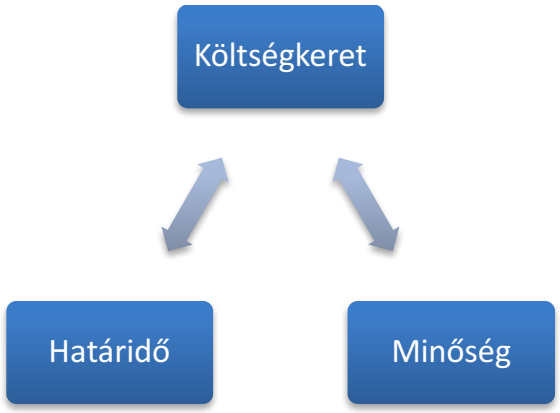
3.1 Az elsődleges projektcélok

Ahhoz, hogy sikeresen be tudjuk kategorizálni egy adott projekt végkimenetelét, és meg tudjuk határozni az adott szervezet projektsikerességét érdemes először azt tisztázni, hogy mitől is függenek a projektek megvalósítási határfeltételei. [26]

A szervezetek számára a projektek egyszeri, komplex feladatokat jelentenek, amelyek kezdeti és befejezési időtartama, valamint költségvetése behatárolt. [27]

Ebből a definícióból látható, hogy a hármas peremfeltétel, azaz a „mágikus projektháromszög”, vagy „szenthárom-ság” a következők szerint alakul: [28]

3. ábra: A projektmenedzsment háromszöge [29], saját szerkesztés



A peremfeltételek paramétereinek mérését fontos folyamatosan elvégezni, illetve rendszeres időközönként az érintettekhez eljuttatni a mérések eredményét annak érdekében, hogy a megfelelő GAP analízissel elősegíthető legyen a projektek sikeres végrehajtása. [30]

3.1.1 Költségkeret

A finanszírozási kérdések mindig is kritikus pontját jelentették a projektek végrehajtásának. Ennek a célnak a megfelelésénél azt kell vizsgálni, hogy a végrehajtáshoz szükséges erőforrásokkal rendelkezik-e az adott szervezet?

Mivel a közigazgatási, és különösen az Európai Uniós projekteknél elsődleges fontossággal bírnak a tervezhető költségek, ezért ilyen esetben a javasolt elszámolási rendszer az árbázisú, költségcél típusú, esetlegesen (amennyiben jól tervezhető) a költségbázisú elszámolási rendszerek. [31], [32]

Megjegyzendő, hogy az Európai Uniós projekteknél (pl. KÖFOP) nem minden esetben elsődleges a költségcél tényleges betartása. Jellemző a túltervezés, a nagyvonalú keretmegállapítás, amely magával vonja a pazarlás lehetőségét is.

Ennél a szempontnál ezért érdemesebb azt vizsgálni, hogy a projekt megvalósíthatósági fázisában tervezett költségek struktúrája miként korrelál a befejezett projekt költségvetésével.

3.1.2 Időkeret

Az időkeret arra ad választ, hogy a projektnek mikorra kell befejeződni, illetve amennyiben a korábban meghatározott időkeret nem tartható, úgy lehetőség van-e azon változtatni?

Az időkeretben bekövetkező csúszások óhatatlanul magukkal vonják a költségek növekedését, illetve a projekt céljának nem teljesítését.

Amennyiben egy projekt számára az időkeret tartása létkérdés, úgy javasolt a határidőcél alapú elszámolási mód tartása, hiszen ebben az esetben a jellemzően külső vállalkozók inkább pozitívan élik meg az időnyomás jelentette sokkot.

Amennyiben az időkeretet az Európai Uniós kritériumok szemszögéből vizsgáljuk, úgy megfigyelhetjük, hogy az aktuális tervezési ciklus időkerete adott (a program 2020-ban ér véget). Ezen időszak végére teljes egészében le kell tudni hívni azokat az összegeket, amelyeket a szervezetek céljaik eléréséhez allokáltak.

3.1.3 Minőség

A projekt céljának eléréséhez szükséges paraméterek, illetve állapotok. Ezek a paraméterek általánosságban a projekt specifikációjában vannak rögzítve, azonban rendkívül nehéz feladat meghatározni minden egyes paramétert, ha a cél elérése nem pontosan definiálható, vagy az rendkívüli komplexitással bír. [33]

Amennyiben az a cél, hogy eme paraméterek feltétlenül megvalósulhassanak a projekt végrehajtása során érdemes a paramétercélú elszámolási módot választani, ugyanis ebben az esetben az ösztönző erőt pont az így definiált kritériumok képviselik.

Az Európai Uniós projektek tekintetében azonban el kell mondani, hogy ezen peremfeltételt nem minden esetben sikerül betartani. Sőt leggyakrabban ez az a feltétel, aminek kárára történik a projektek kivitelezése, hiszen itt a legnehezebb bizonyítani az eredeti céloktól való eltérésből adódó esetleges hiányt.

3.2 Projektek sikerességi tényezői

A korábban tárgyalt kritériumok teljesülése nem vezet egyenesen a projekt teljes sikeréhez. Kizárólag a hármas kritérium alkalmazása nem minden esetben elegendő, Atkinson négyes peremfeltétel-rendszert határozott meg, amely már figyelembe veszi az egyéb sikert befolyásoló tényezőket: [34]

- hármas peremfeltétel,
- a rendszer jellemzői,
- a szervezet támogatása,
- valamennyi érintett támogatása.

Az említett jellemzők alapján építkeznek az ún. sikeresség vizsgálati referenciamodellek is. Ezek a modellek segítenek abban, hogy a szervezet nyomon tudja követni a képességeit, adottságait, illetve az eredményeit is. Ilyen modellek pl. a Projekt kiválóság modell (Project Excellence), az EFQM (European Foundation of Quality Management), illetve az erre a modellre épülő közigazgatási sajátosságokat is adaptáló Általános Értékelési Keretrendszer (CAF, Commom Assassment Framework) is.

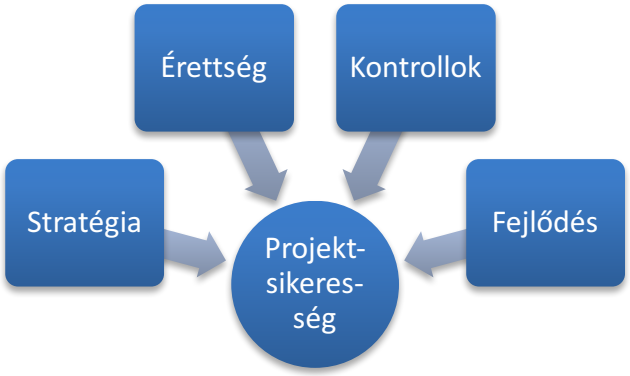
A projektsikeresség vizsgálata igen komplex feladat, több kutatás (empirikus) is készült az okok és okozatok feltárására. Ezen tanulmányok összegzését Dr. Szabó Lajos a Projekt menedzsment című könyvében részletesen elvégezte. Ebből a közigazgatási aspektusok tekintetében a következő befolyásoló tényezők kerülnek kiemelésre: [35]

- A topmenedzsment támogatása, nagyon fontos szempont, ahogy az a Standish Group 2014-es kutatásából is kitűnik, ugyanis a felsővezetői támogatás jelentősen befolyásolja a projekt sikerességét. Szomorú azt tapasztalni, hogy még a kiemelt beruházások tekintetében sem tudják a vezetők a megfelelő időmennyiséget allokálni, [36]
- A célok definiálása, illetve a cél iránti elkötelezettség, is gyakran problémát jelent a közigazgatásban, ugyanis az ilyen hosszú távú projekteknél (pl.: KÖFOP 2020) a célok (amennyiben nem kerültek pontosan meghatározásra) jelentős mértékben változhatnak, átalakulhatnak, ezzel veszélybe sodorva az éppen folyamatban lévő projektek végrehajtását.

4 AZ IT BIZTONSÁGI PROJEKTSIKERESSÉGET ÉS A SZERVEZETI FEJLŐDÉST ÉRINTŐ KUTATÁS ÉS EREDMÉNYEI

4.1 Kutatási modell

4. ábra: kutatási modell, saját szerkesztés



4.2 Hipotézisek, feltételezések

H1: A vállalatok magasabb érettségi szinten állnak, mint a közigazgatási szervezetek.

H2: A fejlődési potenciál magasabb a vállalatoknál.

H3: A stratégia minősége hat a projektek sikerességére.

H4: A szervezetek érettsége befolyásolja a projektek végrehajtását.

H5: A kontrollok implementálása hatással van a projektekre.

H6: A fejlesztések előmozdítják a projektek sikerességét.

4.3 A változók konceptualizálása

- Stratégia: a szervezet hosszú távú célkitűzései meghatározzák a célok eléréséhez elengedhetetlen erőforrásokat és a fejlesztési akciókat.
- Érettség: a szervezetben végzett folyamatok mérésével meghatározható a szervezet aktuális érettségi szintje. Az érettségi modell számszerűen tervezhetővé és ellenőrizhetővé teszi az egyes folyamatok szabályozottságának és a vezetés általi kézben tartottságának fokát.
- Kontroll: az olyan irányelvek, szabályzatok, eljárások, gyakorlatok és szervezeti struktúrák összessége, melyeket arra hoztak létre, hogy ésszerű bizonyosságot adjanak arra, hogy a célkitűzések elérhetők, a nemkívánatos események megelőzhetők, illetve felismerhetők, és helyesbíthetők legyenek. [37]

- Fejlődés: olyan fejlesztési tevékenység, amelynek a célja egy szervezet fejlődésének elősegítése, túlélési esélyeinek növelése (Szervezetfejlesztés).
- Projektsikeresség: a projekt szereplőinek a projekt eredménytermékét a minőségi, idő és költség szempontok alapján osztályozó véleménye.

4.4 A változók operacionalizálása

Stratégia: a stratégia megléte, részletessége, operatív jelenléte és betartása az érintett szervezeteknél.

A változót a következő kritériumok jellemzik a legjobban:

- a stratégia megléte különböző szinteken (szervezeti, IT és IT biztonsági),
- a célkitűzések érintettekkel történő megismertetése,
- a kitűzött célok végrehajthatósága,
- a stratégia kidolgozásában való részvétel lehetősége,
- a stratégia felülvizsgálatának gyakorisága.

A stratégia, mint legalapvetőbb szervezeti kompetencia megjelenik mind az ITIL, mind a COBIT keretrendszerek vonatkozásában is, így a vizsgálni szándékozott kérdések is ezen értékrendek szerint lettek megfogalmazva.

Tekintettel arra, hogy az ezt a változót leíró ismérvek egymásra épülnek ugyan, de arányosításuk nem elvégezhető, ezért a változó mérése ordinális skála segítségével történt meg.

Érettség: a szervezet működését leíró folyamatok megléte, azok illeszkedése a valós tevékenységekhez.

A változó leírása a következő kérdések vizsgálatával lett kialakítva:

- döntéshozatal,
- folyamatok,
- dokumentáltság,
- mérés,
- fejlesztés.

Látható, hogy a fent meghatározott irányok a COBIT metodika érettségi modelljére épülnek, amely nagyban összefügg a projektmenedzsmentet érintő, érettségi modellel.

A változó mérése úgy lett kialakítva, hogy annak mérése magas mérési, azaz Likert-skálán történjen meg.

Kontrollok: a szervezet IT biztonsági folyamatait szabályozó kontrollok megléte, azok viszonya a ténylegesen elvégzett, illetve betartott kontrollokhoz képest.

A változó vizsgálata a következő tényezők alapján történt:

- biztonságtervezés,
- adatvédelem,
- kockázatelemzés,
- incidenskezelés,
- biztonsági képzés.

Az Ibtv. végrehajtási rendeletében 41/2015. Korm. Rendelet szerepeltetett logikai kontrollok kerültek be a kérdőívbe, amelyek mérése szintén magas mérési, azaz Likert-skálán történt meg.

Fejlődés: a kezdeti, a jelenlegi, illetve tervezett fejlődési szintek összehasonlítása.

Vizsgált kérdések:

- általános képzés,
- folyamatfejlesztés,
- projektszervezet kialakítása.

Az ITIL keretrendszer alapján meghatározott változó mérése ugyancsak magas mérési, azaz Likert-skála segítségével lett elvégezve.

Projektsikeresség: a vizsgálat alapját az EFQM modell eredmények oldala képezte.

A vizsgált szempontok:

- belső érintettek,
- külső érintettek,
- társadalmi elvárások,
- eredménytermék,
- terv-tény összehasonlítás.

A referenciamodell alapján jellemzett változó mérése szintén magas mérési, azaz Likert-skála segítségével lett kialakítva.

4.5 Adatgyűjtési módszer

A kvantitatív vizsgálatok kérdőív segítségével kerültek lebonyolításra. A vizsgálatba bevont megkérdezettek száma (előzetesen) legalább 50 fős mintanagyságra lett tervezve (figyelembe véve a téma jellege miatti kitöltési hajlandóságot), ezért a kérdőívvel történő felmérés jó alapot teremtett az egyes szervezeti típusok összehasonlítására is.

Az elemzési kör: közigazgatási szervezetek és azok beszállítói.

A kvantitatív kutatás során kitöltésre előkészített kérdőív 2 fő részre tagolódott. Az első részbe a személyes, valamint a vállalatra jellemző kérdések kerültek (10 db kérdés).

A második, jellegében nagyobb terjedelmű részben került vizsgálatra az öt változóhoz (stratégia, érettség, kontroll, projektsikeresség, fejlődés) tartozó kérdéssor összesen 23 db kérdés formájában.

A kérdőíveket a célcsoportokhoz (közigazgatási és hozzájuk kapcsolódó partnerek) több csatornán (kör e-mail, közösségi hálózat, személyes megkeresés) történt. A válaszadás önkéntes és anonim volt, a válaszadók beazonosítására később semmilyen módon nincs lehetőség.

5 Összefoglaló

A cikk ezen része azokat a tényezőket mutatta be, amelyek hatását figyelembe kell venni az IT projektek végrehajtásánál, hiszen a feltárt képességek nagyban befolyásolják a szervezetek kiberbiztonsági potenciálját is. A cikk következő része magával a kutatással, illetve az eredmények kiértékelésével foglalkozik, valamint tanácsot ad a szervezetek kibervédelmi képességeinek fejlesztésére vonatkozólag.

IRODALOMJEGYZÉK

[1] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[2] 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 (általános adatvédelmi rendelet)

[3] Az Európai parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[4] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[5] Liz Gallacher, Helen Morris: ITIL Foundation Exam Study Guide; John Wiley & sons, London, 2012.,

[6] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[7] ETS 185 – Convention on Cybercrime

[8] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[9] Kápolnai András: E-business stratégia vállalati felsővezetőknek; Aula, Budapest, 2002., pp. 48-56

[10] Bőgel György: Terepszemle; Typotex, Budapest, 2012., pp. 42-60

[11] Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program

[12] ISACA: COBIT 4.1; ISACA, Rolling Meadows, 2007.,

[13] What is ITIL® Best Practice?: https://www.axelos.com/best-practice-solutions/itil/what-is-itil, Letöltés: 2017. április 07.

[14] Jan vom Brocke – Michael Rosemann: Handbook on Business Process Management 2; Springer, New York, 2015., pp. 5-44

[15] Adam Gordon: CISSP Training Series; CRC Press, New York, 2015., pp. 1-60

[16] National Institute of Standards and Technology: Security and Privacy Controls for Federal Information Systems and Organizations; NIST, USA, 2013.,

[17] International Organization for Standardization: ISO 27000:2013; International Organization for Standardization, Genf, 2013.,

[18] ISACA: COBIT 4.1; ISACA, Rolling Meadows, 2007.,

[19] ISACA: COBIT 4.1; ISACA, Rolling Meadows, 2007., pp. 17-47

[20] Dr. Borda József: IT menedzsment; TÁMOP-4.1.2, Budapest, 2013.,

[21] Adam Gordon: Official (ISC)2 Guide to the CISSP CBK; CRC Press, New York, 2015., p. 94

[22] Molnár Bálint – Kő Andrea: Információrendszerek auditálása; Corvinno, Budapest, 2009., pp. 291-318

[23] Broczkó Péter: http://www.tankonyvtar.hu/hu/tartalom/tamop425/0053_ITIL_Alapu_Szolgaltatasmenedzsment/ITIL_alapu_szolgaltatas_menedzsment_1_1.html, Letöltés: 2017. április 07.,TÁMOP 4.2.5, Budapest, 2011.,

[24] Liz Gallacher, Helen Morris: ITIL Foundation Exam Study Guide; John Wiley & sons, London, 2012., pp. 20-21

[25] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[26] Dr. Szabó Lajos: Projekt menedzsment; Pearson Education, Harlow, 2012., pp. 25-27

[27] Görög Mihály: A projektvezetés mestersége; Aula, Budapest, 2003., pp. 27-29

[28] Dr. Szabó Lajos: Projekt menedzsment; Pearson Education, Harlow, 2012., pp. 26-30

[29] Görög Mihály: A projektvezetés mestersége; Aula, Budapest, 2003., p. 28

[30] Project Management Institute: A guide to the project management body of knowledge; Project Management Institute, Pennsylvania, 2008., pp. 64-104

[31] Dr. Szabó Lajos: Projekt menedzsment; Pearson Education, Harlow, 2012., pp. 324-333

[32] Görög Mihály: A projektvezetés mestersége; Aula, Budapest, 2003., pp. 123-129

[33] Dr. Szabó Lajos: Projekt menedzsment; Pearson Education, Harlow, 2012., p. 26

[34] Roger Atkinson: Project management: cost, time and quality, two best guesses and a phenomenon, its time to accept other success criteria; Elsevier Science Ltd., Amsterdam, 1999., p. 341

[35] Dr. Szabó Lajos: Projekt menedzsment; Pearson Education, Harlow, 2012., p. 90-102

[36] The Standish Group Report: Big Bang Boom; The Standish Group, International, 2012., p. 94

[37] Információbiztonság – Túl az informatikán: https://tulazinformatikan.wordpress.com/2012/02/08/a-kontroll-fogalma, Letöltés: 2018. január 11.