M Ű E G Y E T E M 1 7 8 2
Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék

BIZTONSÁG MENEDZSMENT KUTATÓ CSOPORT és az

ISACA®
IT-Governance Szakemberek Támogatása
Információrendszer Ellenőrök Egyesülete

Dr. Nyiry Géza CISA, CISM
Elnök (Inf.rendszer Ell. Egyesülete)

ERDŐSI PÉTER CISA (BME)

VASVÁRI GYÖRGY CISM (BME)
Tiszteleti egyetemi docens

BIZTONSÁGI VÁLTOZÁSOK A COBIT 4-BEN

1.2 változat

2006

1. Bevezetés

A COBIT alkalmazását könnyítendő, ebben a tanulmányban be kívánjuk mutatni, hogy a COBIT 4, biztonsági szempontból, milyen újdonságokat tartalmaz a COBIT 3-hoz képest. A feladat megoldásához a COBIT 4-ben megadott 214 magas szintű kontroll célt (amelyek tehát egyben követelmények is), három csoportra osztottuk:

a.) Az információ rendszerre vonatkozó kontroll célok, amelyek eseti informatikai biztonsági intézkedést igényelnek.
b.) Az informatikai biztonságra vonatkozó kontroll célok.(például a DS 4, és a DS 5), amelyek folyamatos IT biztonsági intézkedéseket igényelnek.
c.) Mind a kettőre vonatkozó kontroll célok (például PO 7.1, - PO 7.8), amelyek folyamatos IT, és IT biztonsági intézkedéseket igényelnek.

Értelemszerűem a vizsgálatunkat a b) és a c) csoportra végeztük el. Megjegyezzük, hogy a COBIT 4. Appendix V.-ben a COBIT 3, és 4. közötti kereszt referenciák szerepelnek. A COBIT 4-nek a COBIT 3 megfelelősségét az alábbi táblázat első két oszlopában is, ennek alapján adjuk meg. Meggyőződésünk szerint, azonban az informatikai biztonsággal foglalkozók, ennél részletesebb elemzést igényelnek.

A COBIT 4. biztonsági szempontból kiemelendő általános újdonságai:

- A COBIT 3-ban 318, a COBIT 4-ben 214 magas szintű kontroll cél van. Pontosabban a COBIT 4 változatlanul 4 szakterületen (PO, AI, DS, ME domain) belül 34 folyamatot (pl.PO1, AI 4, DS 5 process) ad meg, és ezeken belül a 214 magas szintű ellenőrzési célt (pl. PO2,3 high level control objective) ad meg, amelyek értelemszerűen követelményeket jelentenek az információ rendszer, és a biztonság számára is.
- A kontroll célok mindegyikére alkalmazva van az érettségi modell, így az egyes célok auditálásánál mód van, az érettségi szint megállapítására.
- A kontroll célok mindegyikére mag van adva a cél, és a megvalósulás mértékének megállapításához, annak mérési módszere is.
- Az egyes kontroll célok követelmény jelleggel tartalmazzák azt, hogy a megvalósítás során mit kell tenni, és ennek a megfelelősségét, és megvalósulását kell az auditornak ellenőriznie.

- Megjelent a legjobb informatikai biztonsági gyakorlat felhasználására történő hivatkozás. Így az ISO/IEC 117999-es szabványra, az ITIL-re, és az ISF Good Practice for Information Security 4.1 szabványra való hivatkozás.
- A fizikai biztonság önálló ellenőrzési célként szerepel (DS12), de még mindig nem teljes körűek a fizikai biztonsági célok.
- Az ellenőrzésre vonatkozó fejezet erősen átdolgozásra került (ME1-4) az IT governance, az informatikai irányítás megfelelősségét biztosító eljárások szempontjából. Új, hangsúlyos elemként jelenik meg az informatikai terület átláthatóságát biztosító kommunikációs és jelentéstételi kötelezettségek előírása a top menedzsment és az üzleti területek vezetői felé.

COBIT 4	COBIT 3	ÚJDONSÁG A COBIT 4.-ben biztonsági szempontból
PO 2.3	PO 2.3, 2.4	Meghatározza az adatok, érzékenység, kritikusság alapján, elvégzendő osztályozásának céljait, a biztonsági osztályok tartalmát (adat tulajdonosok, biztonsági szint, és az ennek megfelelő védelmi intézkedés). Az adatok osztályozását az egész vállalatra kell elvégezni.
PO 2.4	ÚJ	Az elektronikusan tárolt adatok sértetlenségének biztosítása.
PO 3.2	Új	Technológiai infrastruktúra terv, az IT stratégia, és taktika alapján. A terv magába foglalja a katasztrófa elrendezést, és a technológiai erőforrások beszerzési utasítását.
PO 4.6	4.4, 4.12	A két pont összevonása
PO 4.7	4.5	Biztonsági szempontból nincs új.
PO 4.8	4.6	A teljes szervezetre vonatkozóan, a biztonságért, a kockázat menedzsmentért, és a megfelelősségért a felelősség kiterjesztése, az üzleti célnak megfelelően.
PO 4.9	4.7, 4.8	Az adatok és az információ rendszer tulajdonosainak kijelölése, és a felelősségük az adatok osztályzásáért, és az osztályba sorolásnak megfelelő védelemért.
PO 4.11	PO 4.10	Biztonsági szempontból nincs új.
PO 7.	PO 7.	Egy új cél van a szerepek betöltésének feltételei. (PO 7.3).
PO 9.1	PO 9.1, PO 9.4	Biztonsági szempontból nincs új.
PO 9.2.	PO 9.1, 9.4	A kockázatok összefüggéseinek kihangsúlyozása
PO 9.3	PO 9.3, 9.4	Biztonsági szempontból nincs új.
PO 9.4	PO 9.1, 9.2, 9.4	Biztonsági szempontból nincs új.
PO 9.5,	PO 9.5, 9.6	A kockázati akcióterv a folyamat gazdák felelőssége
PO 9.6	Új	A költség hatékonyság kiemelése
PO 10.9	PO 10.10	A projekt kockázatokat szisztematikusan, és központosítva kell kezelni
PO 8	PO11	A külső követelmények betartása PO8 nincs a COBIT 4-ben, hanem a PO8 a minőség irányítás, amely a COBIT 3-ban a PO11.
AI 1.2	AI 1.9, 1. 10	A kockázat elemzési jelentés az audit trailek (számon kérhetőség), és a belső ellenőrzés méréseinek felhasználásával kell, készüljön.
AI 2.4	AI 2.12	Az alkalmazások biztonságának (kiemelve rendelkezésre állásásnak) meghatározása az adatok osztályozás alapján kell történjen
AI 2.10	Új	Az alkalmazói sw-ek karbantartása, kezelése, és a vészhelyzet csere szabályozva kell, legyen
AI 3.2	AI 1.18, 3.1, 3.3, 3.4, 3.5, 3.7	Az új infrastruktúra elemek (bármely) implementálása a fejlesztő, és az integrátor számon kérhetősége mellett történhet, az egyéb erőforrás elemek biztonsága érdekében.

COBIT 4	COBIT 3	ÚJDONSÁG A COBIT 4.-ben biztonsági szempontból
AI 6.1,	AI 6.1	Ki kell dolgozni a változás kezelési eljárás szabályait, és dokumentálni kell.
AI 6.3	Ai 6.4	Biztonsági szempontból nincs új.
AI 7.1	AI 5.1	Az AI 7 folyamatba össze lett vonva egyes AI, és PO folyamatok ellenőrzési célja. Így a korábbi szétszórtsággal szemben, a megoldások, és cserék ellenőrzési céljai kiemelésre kerültek, mivel egy folyamatként kezeli a COBIT4 őket,
AI 7.2	PO 11.12, 11.13, 11.14,11.15, AI 5.3	
AI 7.2	AI 5.3	
AI 7.4	PO 11.12, 11.13, 11.14, 11.15, AI 2.15, 5.7	
AI. 7.5	AI 5.4, 5.5	
AI 7.6	AI 5.7	
AI 7.7	Ai 5.9	
AI 7.8	Ai 5.12	
AI 7.9	Ai 6.7	
AI 7.10	AI 6.8	
AI 7.11	Ai 6.3	
Ai 7.12	AI 5.13, 5.14	
DS 1.1.	DS 1.1., 1.3	Az 1.1 és 1.3 pontok összevonásra kerültek. Új elemként megjelent az Operation Level Agreement fogalma, melyet az SLA keretrendszernek kezelnie kell.
DS 1.2	ÚJ	El kell készteni a szolgáltatások alap definícióit a szolgáltatások jellemzőit és az üzleti követelményeket figyelembe véve. A szolgáltatások központi kezeléséhez és tárolásához létre kell hozni a szolgáltatás katalógust vagy portfóliót.
DS 1.3	DS 1.2	Az SLA aspektusait felváltotta az SLA konkrétumait tárgyaló kontroll, mely a hasonló tartalmi előírásokon túl kiegészült az aláíró lehetséges személyének meghatározásával, és a mérési követelmények megjelenítésével is.
Ds 1.4	Új	A DS 1.1 pontban megjelent Operation Level Agreement tartalmának meghatározása került ebbe a pontba bele.
DS 2.3	DS 2.6, 2.7	A 2.6 és 2.7 pontok összevonásra kerültek, és ennek megfelelően összevontan meghatározásra került a kontrol célja is.
DS 3.1	DS 3.1, 3.4	A 3.1 és 3.4 pontok összevonásra kerültek, és új elemként megjelent a költség-alapú megközelítésmód is, mint követelmény.
DS 3.4	DS 3.2, 3.8, 3.9	A 3.2, 3.8 és 3.9 pontok összevonásra és átfogalmazásra kerültek, biztonsági szempontból nincs új..

COBIT 4	COBIT 3	ÚJDONSÁG A COBIT 4.-ben biztonsági szempontból
DS 4.1	DS 4.1, 4.2	A 4.1 és 4.2 pontok összevonásra kerültek. A konzisztenciára való hivatkozás megerősítése mellett kikerült a rövid- és hosszú távú tervekhez való illesztési követelmény.
DS 4.2	DS 4.3	Biztonsági szempontból nincs új.
DS 4.3	DS 4.4,	A pont átdolgozásra került, a minimális megvalósítás elve helyett az üzleti kritikusság szerint kell a folyamatos működéshez szükséges erőforrásokat biztosítani.
DS 4.5	DS 4.6	A pont kiegészítésre került tesztelési megfontolásokkal.
DS 4.7	DS 4.8	Biztonsági szempontból nincs új.
DS 4.8	DS 4.9, 4.11	A pontok összevonásra kerültek. Biztonsági szempontból nincs új.
DS 4.9	DS 4.12, DS 11.25	A pontok összevonásra kerültek, és kiegészült az archív adatok kezelésének követelményeivel.
DS 4.10	DS 4.13	Biztonsági szempontból nincs új.
DS 5.1	DS 5.1, 5.12	Az intézkedések biztonságának menedzselését felváltotta az informatikai biztonság menedzselése megközelítésmód.
DS 5.2	Új	Az üzleti információ követelmények, IT konfiguráció, információ kockázati akcióterv, és informatikai biztonsági kultúra követelményeknek megfelelő IT Biztonsági Tervet kell készíteni, melynek megvalósítása szabályozások és intézkedéseken keresztül történik. A szabályokat kommunikálni kell a stakeholderek és a felhasználók felé.
DS 5.3	DS 5.2, 5.3, 5.9, AI 6.6	A (külső, belső, ideiglenes) felhasználói azonosítási eljárások összefoglalóan kerültek leírásra az Identity Management pontban. Változás, hogy a jogosultságok kérelmezésének, jóváhagyásának és beállításának felelőseit is megnevezi.
DS 5.4	DS 5.4 5.5, 5.6, 10.4	A pontok összevonásra kerültek. Biztonsági szempontból nincs új.
DS 5.5	DS 5.6, 5.7, 5.10	A pontok összevonásra kerültek. A naplózott információkhoz való hozzáférésnek illeszkednie kell az üzleti elvárásokhoz a jogosultság és a megőrzési idők tekintetében.
DS 5.6	DS 5.11	A rendkívüli események kezelésében megjelent új elemként a hatás szintek figyelembe vétele.
DS 5.7	DS 5.17	Biztonsági szempontból nincs új.
DS 5.8	DS 5.18	Biztonsági szempontból nincs új.
DS 5.9	DS 5.19	A pontból kikerült a jelentési kötelezettségre való utalás.
DS 5.10	DS 5.20	Biztonsági szempontból nincs új.
DS 5.11	DS 5.15, 5.16	A bizalmas adatok körének példálózó felsorolása és a digitális aláírásra való utalás nem került át a két pont összevont átdolgozásába, mivel az új pont követelmény-szinten fogalmazza meg az elvárásokat.
DS 8.3	DS 8.2	A felhasználói kérések körének meghatározása bővült (az ITIL folyamatainak megfelelően)

COBIT 4	COBIT 3	ÚJDONSÁG A COBIT 4.-ben biztonsági szempontból
DS 9.3	DS 9.3, 9.4, 9.5	Biztonsági szempontból nincs új.
DS 10.1	DS 8.5	A felhasználói kérdések kezelése beleintegrálódott a probléma-kezelési folyamatba.
DS 10.2	Új	A probléma-kezelésen belül új elemként jelenik meg a problémák nyomon követése és a megoldás követelményének definiálása.
DS 10.3	DS 8.4	A probléma lezárási követelményei közül kikerült a lezáratlan esetek kezelése, átkerült a 10.2-be.
DS 10.4	ÚJ	Új elemként jelenik meg a hatékony probléma- és incidens kezelés érdekében a probléma-, változás- és konfiguráció-menedzsment folyamatainak integrációs követelménye.
DS 11.5	DS 11.23, 11.24	Biztonsági szempontból nincs új.
DS 11.6	DS 11.16, 11.17, 11.27	A bizalmas információk védelmi igényei integrálódtak az adatok kezelésének biztonsági követelményei közé.
DS 12.1	DS 12.1, 12.2	Az informatikai eszközök fizikai elhelyezésének leírása a külső és belső követelményeknek való megfelelőséget hangsúlyozza.
DS 12.2	DS 12.1, 12.2	A fizikai intézkedések megvalósítása, ellenőrzése és az incidensek kezelése új megfogalmazásban jelenik meg, az üzleti szükségletekből kiinduló megközelítésben.
DS 12.3	DS 10.4, 12.3	A fizikai hozzáférés komplex menedzselése jelenik meg itt, tekintet nélkül a fizikai hozzáférést megvalósító kilétére és szervezettel való kapcsolatára.
DS 12.4	DS 12.5	Biztonsági szempontból nincs új.
DS 12.5	DS 12.6	A szünetmentes áramforrás követelménye integrálódott a létesítmények fizikai menedzselése pontba.
DS 13.3	DS 13.6	Megjelenik explicit követelményként az IT infrastruktúra és kapcsolódó eseményeinek figyelése.
DS 13.4	DS 5.21, 13.7	Biztonsági szempontból nincs új.
ME 2.1, 2.3	M 2.1	A hiányosságok értékelése külön pontba került át.
ME 3.3	Új	A törvényi és szabályozási előírásoknak való megfelelősség értékelése új alapokra került, az üzleti és IT menedzsment felügyelete és a belső kontrollok működése alapján.
ME 4.4.	ÚJ	Az erőforrás menedzsment új elemként jelenik meg, mely biztosítja az üzleti célok kielégítéséhez szükséges IT erőforrások meglétét és kihasználásának optimális voltát.
ME 4.5	Új	Új elemként jelenik meg az IT kockázatok kommunikálásának igénye. Az IT kockázatok aktuális értékének minden stakeholder számára átláthatónak kell lennie.

COBIT 4	COBIT 3	ÚJDONSÁG A COBIT 4.-ben biztonsági szempontból
ME 4.6	Új	Az IT működés mérésének újonnan megfogalmazott követelménye jelenik meg, a top menedzsment felé időnként és megfelelő, de különböző módokon riportolni kell az IT eredményeit, problémáit, és azok megoldásait.