KOCKÁZATMENEDZSMENT ÉS INFORMATIKAI ALKALMAZÁSOK MENEDZSMENTJÉNEK A KAPCSOLATA

THE RELATIONSHIP BETWEEN APPLICATION AND COMPLIANCE MANAGEMENT

MOZSÁR LÍVIA ALICE PhD-hallgató
Óbudai Egyetem

Abstract

The approach of the article is to show the relationship between compliance management and application portfolio management in large companies. Analyzing of the two areas a new management model is created which means the secure information application management. The methodology provides a guideline for large organizations for example how they can increase the success of different audits.

The secure information application management is a new framework where the different security standards are integrated into application and architectural management. The question is how to create a security management framework that supports the safe management of information applications? Architectural, application portfolio and compliance management integration can define the principles to assess the different risks, and monitor them. A safety application management can support the organization. The management can reduce costs, risks and helps the secure and stable operation in long term.

1. Bevezetés

A tanulmány első részében definiálja a két területet, milyen lépések, módszerek állnak a rendelkezésre, majd ajánlást ad a két terület összehangolására, kapcsolódási pontok feltárására. A módszertan egy vezérvonalat ad, nem teljes körű, a szervezet sajátosságait figyelembe véve bővíthető és szűkíthető is.

A tanulmánynak nem célja részletesen bemutatni az alkalmazás portfólió és compliance menedzsmentet. Az informatikai alkalmazás menedzsment jelentősége főleg globális nagyvállalatoknál napjainkban egyre nő, hisz az üzleti folyamatok támogatottságát az informatikai rendszerek segítik elő. Nagyvállalatoknál az adatok informatikai rendszerekben vannak tárolva, informatikai rendszerek, folyamatok nélkül a szervezetek működésképtelenek. Az informatikai folyamatok, szolgáltatások biztonságos menedzselése egyre kritikusabbá válik. Alapvető követelmény kell, hogy legyen minden szervezetben, hogy információk álljanak rendelkezésre az informatikai rendszerek működési biztonságáról.

Az informatikai alkalmazás racionalizáció lépéseinek felsorolása, jelentősége egyes kockázati tényezők csökkentésének lehetőségével a szervezetben az egyik legfontosabb tényező. Ilyen lépések például a redundáns applikációk elemzése, redundanciák csökkentése például alkalmazások lekapcsolásával, vagy integrálásával. Következő fontos elem a dokumentációk megléte az alkalmazásokról, s ezen dokumentációk tárolhatóságának, frissíthetőségének a követelményei. Az informatikai auditok és az informatikai alkalmazások dokumentációjának a meglétének az elemzése, valamint az informatikai alkalmazásme-

nedzsment kapcsolata a kockázat menedzsmenttel egyre nagyobb hangsúlyt kap a külső adutiáló szervezetek (KPMG, PwC) által. Az informatikai alkalmazás portfolió létrehozásának az egyes lépéseinél már figyelembe kell venni az alkalmazásokra vonatkozó dokumentációs követelményeket, compliance előírásokat.

SANS felmérése alapján kimutatták, hogy a vállalatoknak közel az egyharmadának nincsen kialakított alkalmazás biztonsági programja.

A legtöbb vállalatnak, főleg a nagyvállalatoknak, ahol az alkalmazások száma meghaladja a több százat, nincs pontos lista az alkalmazásokról, így nem is lehet a szervezet, s a vállalat menedzsmentje meggyőződve arról, hogy biztonságosan működnek az alkalmazások. A nagyvállalatoknál alkalmazás portfolió menedzsment nélkül az informatikai rendszerek biztonságos menedzselése sem lehetséges.

Ahhoz, hogy a biztonsági menedzsment program, szabályok, keretrendszerek megfelelően legyenek alkalmazva, ahhoz szükséges lenne ismerni a nagyvállalatoknak az üzleti folyamatokat támogató informatikai rendszereket teljesen.

2. Alkalmazás portfolió menedzsment

A nagyvállalatok többsége a különböző és több százezres üzleti folyamatok támogatására több száz vagy akár több ezer informatikai alkalmazást használnak. Ennek eredménye, hogy az informatikai organizáció, a benne lévő szabályrendszerek is egyre komplexek, átláthatatlanokká váltak. Az alkalmazás portfolió menedzsment segít egy széleskörű átláthatóságot adni a meglévő alkalmazásokról, támogatja az üzleti stratégiai döntéseket. Megoldást nyújt az összetett és sok informatikai rendszereket működtető vállalatoknak az alkalmazások kategorizálása révén a folyamatok, így az alkalmazások optimalizálására, a szervezet hatékony működtetését, valamint azt, hogy az informatikai szolgáltatások az üzleti igényekhez igazodjon.

Az integrált alkalmazás portfolió menedzsment előnyei, hogy az alkalmazások költségeinek (hardver, szoftver, fejlesztési, karbantartási) csökkentése, valamint az alkalmazások folyamattámogatásának egyszerűsítése valósulhat meg a megfelelő keretrendszer kialakításával, folyamatos menedzsmenttel. A költséghatékonysági lépések és intézkedések középpontjában az informatikai alkalmazásokra költött különböző költségek összetétel vizsgálatában adhat segítséget egy megfelelő applikáció portfolió menedzsment. A fejlesztési költségek csökkentése, futtatási költségek csökkentése, a fő változtatások csökkentése az IT összköltségek csökkenéséhez vezet az informatikai részlegekben.

Sok szempontból elemezhetőek az alkalmazások, amit egy alkalmazás portfolió menedzsmentnek figyelembe kell venni, mint például: támogatott üzleti területek, folyamatok, stratégiai célok a szervezetnek, ezáltal az informatikai alkalmazások életciklusának a meghatározása, meglévő és tervezett üzleti és informatikai projektek.

3. Compliance menedzsment

A compliance menedzsment sokrétű terület, az informatika terület szempontjából az informatikai compliance menedzsmentet emelem ki. A compliance-től függetlenül vagy integráltan működhet egy szervezetben a vállalati kockázatmenedzsment, a belső ellenőrzések valamint a külső ellenőrzések (auditok).

A menedzsment része, eleme a célok meghatározása, folyamatok monitorozása a céloknak, ellenőrzési pontok kialakítása, nyomon követése, értékelése, valamint a keretrend-

szer felépítése és a szervezet sajátos működésébe való illesztése. A compliance menedzsment előírásoknak, szabályoknak való megfelelést támogat, stratégiai döntésekhez nyújt segítséget.

A jelenlegi szabványkészletek segítik a nagy méretű szervezetek működését, azonban sok szervezeti sajátosságot nem tud figyelembe venni. Meglévő szabályrendszerek például: SOX, GLBA, HIPAA, FFIEC, ITIL, COBIT, ISO.

A compliance menedzsment rendszer fontossága abban rejlik, hogy a kockázatok menedzselhetőek, új törvényi előírások figyelemmel kísérése és alkalmazása révén a szervezet folyamatos törvényi megfelelősége biztosítható. Támogatja a szervezetben az üzletmenet folytonosságát, teljesítményt növelhet, valamint a szervezet hosszú távú stabil működését támogatja.

A menedzsmentet három területe:

1. Vállalaton belüli előírások, törvényi megfelelések nyomon követése, ellenőrzése, iparági sajátosságok (Basel II, FDA, FERC, FAA)
2. Vállalaton kívüli előírások (SOX, J-SOX)
3. Standardek (ISO, ITIL)

4. Kétirányú megközelítés, kapcsolódási pontok az alkalmazás menedzsment és compliance menedzsment között

Egy 2012 decemberében készült felmérés rávilágít arra a tényre, hogy a vállalatok 23%-ának van kialakított és működőképes biztonsági programja az alkalmazások teljes életciklusára vonatkozóan. A felmérésben részt vevő vállalatoknak több, mint az egynegyede nem tudja pontosan az informatikai alkalmazásainak a számát. A felmérésből kiderül az is, hogy így a biztonságos menedzselés, főleg az üzletkritikus alkalmazások nem menedzselhetőek. A megkérdezettek 23%-a alkalmaz és követ biztonsági előírásokat az informatikai alkalmazás életútjában. Azáltal, hogy a szervezet vezetése, érintett osztályok, felelősök nem tudják, mennyi és milyen informatikai alkalmazásokat használnak, menedzselnek, így a biztonsági előírások betartása, alkalmazása sem kivitelezhető.

A kapcsolódási pontok feltárása kiterjeszthető több terület bevonására is, mint például üzleti folyamatok menedzselése, stratégiai menedzsment, nagyvállalati architekturális menedzsment.

A biztonsági szabályokat be kell tartani egy szervezeten belül, valamint figyelmet kell fordítani az információs rendszerek biztonságának irányítására, szervezésére, koordinálására, a biztonsághoz kapcsolódó folyamatok tervezésére, fenntartására, kontrolálására vonatkozó előírásokat, ajánlásokat.

Ahhoz, hogy a szervezet biztonságos informatikai rendszert működtessen, ismernie kell az informatikai alkalmazásokat, az alkalmazások által támogatott üzleti folyamatokat, a bennük tárolt adatok fontosságát. Az informatikai szabályozásnak illeszkednie kell a vállalat meglévő felépítésébe, folyamatiba. Fontos, hogy a szervezet alkalmazzon valamilyen szabványt. A gazdasági szervezetek informatikai rendszerének és folyamatainak biztonságos, folytonos működését támogató szabványok, ajánlások, COBIT, ISO, ITIL.

A COBIT egy keretrendszer arra, hogy a vezetőknek lehetősége legyen az előírásoknak való megfelelésnek. Egy keretrendszer, aminek a segítségével a szervezeteknek az üzleti céljaik elérésében segíti a vezetőket, az IT tevékenységek, költségek menedzselése is átláthatóvá válik. A COBIT keretrendszer lehetőséget ad arra, hogy az IT kockázatok megfelelően legyenek menedzselve egy szervezetben.

Integrált compliance rendszer megléte fontos a nagyvállalatoknál. Integrált compliance menedzselés előnye, hogy az egyes területeken lévő hiányosságok, s az ezekből eredő kockázatok, folyamathiányosságok, költségek láthatóvá válnak a menedzsment részére. Fókuszálva az informatikai rendszereken végzett auditokra, a sikeressége az ellenőrzéseknek javítható, növelhető, ha a törvényi megfelelőségi keretrendszer illeszkedik az informatikai rendszerek sajátosságaihoz, illetve figyelembe veszi az előírások betartására vonatkozó idő, ember és költségigényt is.

A következőkben az alkalmazás portfolió racionalizálás lépéseit és a compliance összhangba hozásának egy lehetséges megoldását mutatom be. A modell az informatikai alkalmazások törvényi megfelelőségének a biztosítására fókuszál.

Az alkalmazás portfolió lépéseinek az összes lépésénél, tehát már az elejétől fogva be kell hogy kapcsolódjon a compliance menedzsment. A két terület mellett párhuzamosan kell, hogy zajlódjon az architekturális tervezés is, ami összehangolja az üzleti stratégiai célokat a meglévő alkalmazás portfolióval. Az operatív stratégia része a lépéseknek, operatív tervezésbe pedig bele kell vonni a létrehozott integrált lépéseket. A lépések az alábbiak:

1. Alkalmazás menedzsment és compliance menedzsment keretén belül a célok definiálása
2. Célok beilleszthetőségének elemzése a vállalati szervezetbe, keretrendszerbe
3. Ellenőrzési pontok kialakítása, ellenőrzési keretrendszer kiválasztása
4. Személyi, tárgyi feltételek létrehozása
5. Integráció menedzselése, folyamatos fejlesztése

Az alkalmazás portfolió és compliance menedzsment integrálásával, összehangolt működésével az auditok sikeressége is növelhető. Az külső informatikai auditoknak sok típusa van, mint például az alábbiak:

- Információbiztonsági audit
- Üzletfolytonossági audit
- Mobil applikációkra terjedő audit
- Felhő alapú audit
- Program audit
- Software, alkalmazás audit
- Szociális média kockázat audit
- Informatikai kockázatmenedzsment audit
- Adatvesztés és védelmi audit

Az alkalmazás menedzsment első lépése az alkalmazások racionalizációja. A legfontosabb, hogy listát kell készíteni a meglévő a fejlesztés alatt álló, illetve a bevezetésre szánt alkalmazásokról, hiszen látni kell egy nagyvállalatnak, mely akár több régióban van jelen, hogy milyen alkalmazásai vannak. A listakészítésénél sok befolyásoló tényező lehet – például milyen területen működik az adott vállalkozás, milyen üzleti területeket szolgál ki,azok az üzleti egységek milyen országban, régióban vannak jelen.

Néhány elem, amit szükséges a listakészítésénél figyelembe venni. A lista nem teljes körű.

1. Alkalmazás neve
2. Architekturális ábra
2. Üzleti folyamatok, amit támogat

3. Alkalmazáshoz kapcsolódó személyek, kontaktok listája a különböző területekről (üzlet, informatika)
4. Stratégiai támogatottság szintje
5. Felhasználók száma, listája
6. Éves költség, költségek összetevője részletesen
7. Korábbi auditok eredményei
8. Dokumentációk az előírások alapján

A lista készítés után egy integrált adatbázis létrehozásával lehet támogatni az információk tárolhatóságát, könnyen frissíthetőségét. A compliance területnek ennél a lépésnél be kell kapcsolódni, s a szervezeti sajátosságokhoz kell igazítania az előírásokat, szabályokat. Követelményként kell például fogalmazni a lista készítés lépéseit, idejét, felelősöket, nyilvántartásra vonatkozó követelményeket. Ez a lépés segítheti például a szervezetet egy informatikai alkalmazás audit alatt keletkező hibák számának a csökkentését. A dokumentációkra vonatkozó követelményeket meghatározhatja a szervezet a külső előírások alapján, de kialakíthat belső, saját ellenőrzési szabályrendszert is. A dokumentációk létrehozásának, karbantartásának, monitorozásának a részletes lépéseit kell definiálnia a szabályrendszereknek a felelősökkel együtt. Tehát a compliance-nek ki kell térnie az informatikai alkalmazások nyilvántartásának, mindennapi futtatásának a szabályrendszerére, mint például:

– Adatok kategorizálása, menedzselése
– Informatikai és üzleti üzletfolytonossági tervek (BCV)
– Adatvédelem
– Ellenőrzési pontok az üzleti és informatikai folyamatokban

5. Alkalmazás tervezés, architekturális tervezés és a törvényi megfelelés kapcsolatrendszere

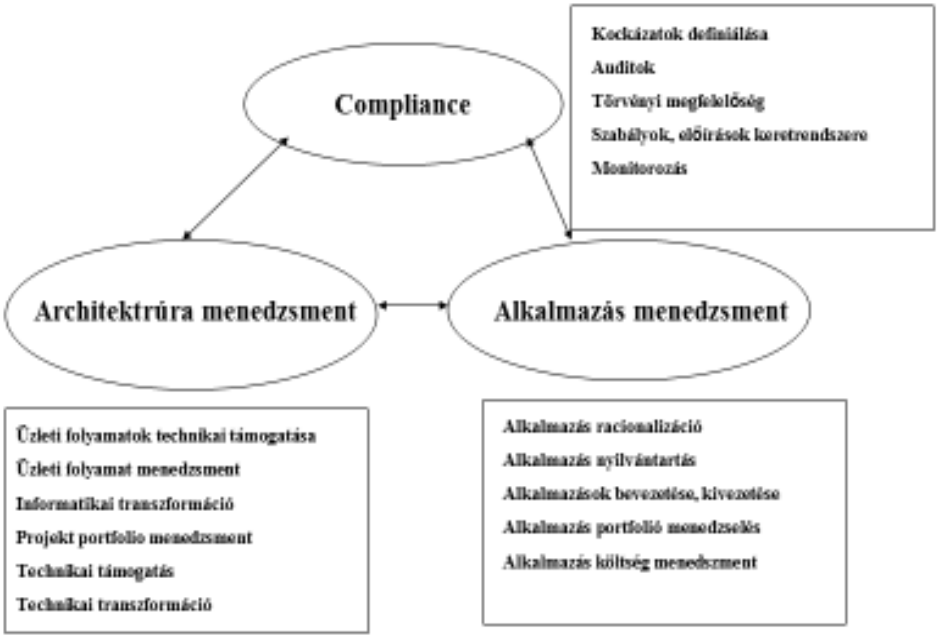
Ebben a lépésben összekapcsolódik az alkalmazásmenedzsment az architekturális tervezéssel. Az architekturális tervezés, menedzsment jelentősége akár olyan szervezetben is fontos, ahol az informatikai alkalmazások száma meghaladja a 40-et. Az architekturális menedzsment struktúrája, felépítése nagyban függ az üzleti folyamatok számától, komplexitásától, informatikai folyamatok meglététől, technikai színvonaltól. Az architektúra menedzsment egy globális nagyvállalatban sok területtel kell, hogy együttműködjön, mint például az üzleti stratégiai menedzsment, változtatás menedzsment, kockázatmenedzsment, pénzügyi stratégiai menedzsment, domain menedzsment, informatikai alkalmazás portfolió menedzsment, és törvényi megfelelőség szempontjából érintett területek-compliance, kockázatmenedzsment. Az informatikai alkalmazások több életciklusában is jelen van az architekturális tervezés, így a törvényi megfelelőségek vizsgálatának is itt kell megtörténnie. Vállalati architektúra képes arra, hogy összehangolja az üzleti, informatikai folyamatokat, személyeket, információs rendszereket az üzleti célokkal és a stratégiai irányítással. Néhány ismertebb vállalati architektúra ajánlás: Zachmann, DODAF (the Department of Defense Architecture Framework), FEAF (Federal Enterprise Architecture Framework), EAP (Enterprise Architecture Planning) TOGAF. Az ADM, vagyis az architekturális fejelsztési módszer részes elemét képezi a TOGAF-nak. TOGAF-nak több fázisa van. A korábban felsorolt architekturális ajánlások lényegében eszközök arra, hogy hogyan fejlesszen egy szervezet vállalati architektúrát. Ezek az eszközök lényegében a sza-

bályrendszerek felett helyezkednek el (ITIL, ISO stb.) de a szervezet koncepcionális kérdéseit fogalmazza meg, míg a különböző szabályrendszerek a felhasználóknak és az ügyfeleknek nyújtanak szolgáltatást. Az ajánlásokat és a szabályrendszereket összekapcsolva az alkalmazás portfolió menedzselésével biztonságosabbá teheti a szervezet a működését.

Az architekturális alkalmazás tervezési eszközök kiváló keretrendszerek arra, hogyan kell informatikai megoldást építeni valamint monitorozni azonban nem ad ajánlást arra, hogyan kell szállítani az informatikai szolgáltatásokat. Az szabályrendszerek pedig részletesen kitérnek az informatikai szolgáltatásokra, anélkül, hogy megfogalmaznák azt, hogy milyen hatása lehet az egyes szabályok gyakorlati alkalmazásának a támogatott üzleti folyamatokra.

Azonban fontos kiemelni a különbségeket, mint például azt, hogy az üzleti architektúra kialakítása az architekturális tervezések keretrendszerén belül valósul meg, ez teljesen hiányzik az szabályzati rendszerekből. Az informatikai szolgáltatások futtatása és szállítási a szabályrendszereken belül vannak definiálva, azonban a az architekturális keretrendszer nem ad semmilyen ajánlást fejlesztési, támogatási, futtatási környezetre.

1. ábra. **Az informatikai alkalmazás, architekturális tervezés és compliance menedzsment**



Forrás: saját szerkesztés

Konklúzió

Globális nagyvállalati környezetben, ahol az informatikai alkalmazások száma világszerte meghaladja a több ezret, kiemelt fontosságú terület az egyéb menedzsment területek mellett az informatikai alkalmazás menedzsment. Az informatikai alkalmazás menedzsmentnek bele kell épülnie az architekturális tervezésbe, menedzsmentbe, valamint a törvényi előírások, megfelelőségek menedzsment területébe is. A három terület menedzsment integrációja biztosíthatja a szervezet számára a biztonságos informatikai alkalmazásme-

nedzsmentet,s így a különböző kockázatok csökkentését is, valamint az informatikai alkalmazás auditok sikerességét. A modell és a kapcsolódási pontok feltárása további kutatásokat, elemzéseket igényel.

Felhasznált irodalom

1. SANS: Survey on Application Security Programs and Practicesdecember 2012, Jim Bird, Frank Kim: https://www.sans.org/reading-room/whitepapers/analyst/survey-application-security-programs-practices-35150

https://www.securityinnovation.com/services/application-risk/application-portfolio-assessment.html

http://www.isaca.org/Groups/Professional-English/po1-6-it-portfolio management/Pages/Overview.aspx

http://www.slideshare.net/RoryMackay1/application-management-framewor

http://www.kpmg.com/CH/en/Library/Articles-Publications/Documents/Advisory/pub-20131106-it-internal-audit-survey-en.pdf

https://www.sans.org/reading-room/whitepapers/analyst/survey-application-security-programs-practices-35150

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

http://www.slideshare.net/RoryMackay1/application-management-framework

http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e2_it_menedzsment_scorm/a_szolgaltatasi_szintek_meghatarozasa_es_kezelese_i241kym9Ks6j0FCd.html

https://www.axelos.com/gempdf/ITIL_and_TOGAF_White_Paper_v0_3.pdf

https://lirias.kuleuven.be/bitstream/123456789/369965/1/KBI_1226.pdf