



Információbiztonsági szolgáltatások a pénzügyi szektor számára

TANÁCSADÁS

A cégvezetők értékteremtést várnak el az IT-től, mint szervezeti egységtől. Az üzleti igényekkel összehangolt IT-szolgáltatás biztosítása az informatikai vezetők egyik legfontosabb célkitűzése. A KPMG valódi megoldásokat kínál az információkezelés biztonsági kockázataira az üzleti igényeket modellező infrastruktúra kialakításában (Virtualizáció, SOA), az üzleti cél-alkalmazás kiválasztása, bevezetése és fejlesztése területén (SOA, EAI), a kellően kontrollált üzemvitel megteremtésében (ITIL, CoBIT), valamint a törvényi előírásoknak megfelelő kontrollkörnyezet kialakításában.

Az infrastruktúra kialakításában rejlő kockázatok

A szállítók által kínált virtualizált, autonóm infrastruktúra kockázatainak kezeléséhez megfelelő kontrollkörnyezet kialakítására van szükség. A KPMG külön módszertant dolgozott ki a virtualizált architektúra tervezése megváltozott biztonsági aspektusaira, az implementáció minőségbiztosítására és az elkészült architektúra utóellenőrzésére.

Szolgáltatásaink lehetővé teszik, hogy a modern technológia nyújtotta lehetőségeket kellő biztonság mellett használják fel az üzleti igények kielégítésére:

- **Kockázatelemzés és -kezelés** az adatok és informatikai rendszerek strukturált, egységes elemzése azok bizalmasságának, integritásának és rendelkezésre állásának felméréséhez. A kockázatok megállapítása, valamint a kezelés módjának kidolgozása mellett fontos a megvalósítás nyomon követése.
- **Infrastruktúra-audit** az infrastruktúrában rejlő informatikai kockázatok üzleti hatásának csökkentése érdekében. Ezáltal elérhető, hogy az informatikai rendszerek pontos és megbízható

adatokat szolgáltatassanak az üzletnek, betartva a jogszabályi előírásokat.

- **Szabványos biztonsági szabályozó-környezet kialakítása**, amely átfogó és strukturált megközelítést biztosít a gyorsan változó környezetben felmerülő veszélyforrások és fenyegetések, valamint kockázatok kezeléséhez. (ISO 27001, ISO 17799).
- **Kontrollált krízishelyzet-kezelés**, amely a virtualizált infrastruktúra, összetettségében üzemeltetésének komplexitásában és a tőlük való magas függésében rejlő kockázatokra ad hathatós intézkedési tervet.

Az üzleti cél-alkalmazás kiválasztásában, bevezetésében és fejlesztésében rejlő kockázatok

A pénzügyi szektorban fokozott az igény az értékesítési csatornák hatékony és teljes körű kihasználására.

Az üzleti funkciók komponens alapú megközelítésével és a komponensek által biztosított szolgáltatások granulálásával lehetségessé válik a szolgáltatás alapú architektúra (SOA) kialakítása.

A SOA legközismertebb alkalmazási területe a webszolgáltatások és azokra épülő alkalmazásintegráció, alkalmazásfejlesztés. Bár ezen technikák alkalmazása sem különbözik sokban az eddigi módszerektől, viszont a fejlesztési életciklusnak (SDLC) jobban figyelembe kell vennie a kontrollálhatóság megteremtését, a tesztelési szintek és típusok megfelelő alkalmazását, valamint a SOA szabványainak megfelelő használatát. Szolgáltatásainkban kiemelt figyelmet fordítunk a szükséges és kontrollált hozzáférés, valamint az integrált rendszerek adatbiztonságának megteremtésére:

- **SDLC-támogatás** segítségével a fejlesztési ciklusban a kellő kontrollok beépítése, így az elkészült rendszerek a minőség és az üzemeltethetőség mellett auditálhatóvá válnak. Mindezek segítségével és a tesztelési életciklus megfelelő tervezésével a szolgáltatások újrafelhasználását és a tesztelőforrások optimalizálását támogatjuk.
- **Az SOA, EAI biztonsági kontrollok tervezése** által a megváltozott fejlesztési technológiában rejlő kockázatok kézbentartása, fejlesztési, architektúrális és szabványügyi megfontolások alapján.

- **Implementációt követő vizsgálatok**
segítségével a követelmények, minőségi elvárások megvalósulásának utóellenőrzése, valamint biztonsági tesztek végrehatása történik meg.
- **Biztonság tesztelési szolgáltatásaink**
sorában megtalálhatóak a „white box”, „grey box” és „black box” penetrációs tesztek is.
- **Migrációs és interfész-vizsgálatok**
Az informatikai rendszerek cseréje, upgrade-je során fellépő problémák jelentős része a régi és az új rendszerek közötti adatmigrációval kapcsolatos. A KPMG szoftveres elemző eszközökkel biztosítja a független, teljes körű és megbízható tesztelést, segítve a projekt időbeli befejezését és az új rendszerben tárolt adatok integritásának megőrzését.

Az üzemeltetésben rejlő kockázatok

Az üzemeltetés szervezésére létrehozott szabványok és szabályzó rendszerek csak a kereteket jelölik ki, a hatékonyság növelését nem garantálják önmagukban. Szolgáltatásaink kialakításánál különös figyelmet szentelünk:

- **a konfigurációkezelésre**, amely alapját képezi az intézményszintű eszközkezelésnek, hibakezelésnek és szolgáltatásfolytonosság-tervezésnek;
- **a szoftver-eszközkezelésre**, amely a fizikai szintű eszközkezelésen túl (leltározás, licencszámvizsgálat) integrálja a szerződéses és pénzügyi licencadatok kezelését;
- **a verziókezelésre**, amely megoldja a konfigurációs elemek változásából adódó verziók együttes kezelését;
- **szolgáltatásiszint-kezelésre**, amely támogathatja a szolgáltatás folytonosság tervezését és ellenőrzését éppúgy, mint az üzleti területek felé történő elszámoltathatóságot.

Üzletmenetfolytonosság-kezelés (BCM) és katasztrófa-helyreállítás (DRP)

Az információs rendszerek bonyolultsága, összetettsége és a tőlük való magas függés, a kisebb és nagyobb természeti katasztrófák, valamint a sosem elhanyagolható humán kockázat miatt ma már elengedhetetlen az üzletmenet és szolgáltatás folytonosság komplex kezelése. Az üzletfolytonosság-menedzsment lefedi a klasszikus értelemben vett katasztrófa-helyreállítási tevékenységet, az üzleti folyamatok folytonosságának biztosítását és a megelőző intézkedések alkalmazását. Az üzletfolytonosság-menedzsment így beépülhet a napi folyamatokba, biztosítható a kontrollok konzisztens alkalmazása és az elkészült üzletfolytonossági tervek folyamatos karbantartása és tesztelése.

Szabályzatok kialakítása

Az informatikai üzemeltetési, fejlesztési és a mindent átható biztonsági szabályok bevezetése, konzisztens alkalmazása és karbantarthatósága szempontjából kiemelten fontos a szabályok strukturált kialakítása. Az üzleti, informatikai és biztonsági stratégiából támogatásunkkal kialakított szabályzatok lefektetik az informatikai működés alapját, míg az ezeken alapuló eljárások, utasítások és egyéb támogató dokumentumok biztosítják az egyértelmű alkalmazást, a munkafolyamatokba való beépülést és a mérhetőséget.

Törvényi megfelelés vizsgálat

A banki informatikára vonatkozó törvényi szabályozás elég szerteágazó, és számos ajánlás is létezik hozzá. A kitételeknek való megfelelést sokféle módon, tág költséghatárok közt lehet elérni. A releváns törvényi előírások (Tpt, Hpt, PSZÁF, MNB előírások), és a PSZÁF követelményeinek alapos ismeretére építve szakértőink rendszeresen végeznek törvényimegfelelés-vizsgálatot, és javasolnak költségkímélő megoldásokat, amelyeket az illetékes hatóságok minden esetben elfogadtak.

Szerepkör alapú identitáskezelés (EIM)

A vállalati működést szabályozó szervezetek egyre nagyobb nyomást gyakorolnak az intézményekre a transzparens

identitáskezelés biztosítása érdekében.

Fontos átláthatóan és egyértelműen összerendelni a vállalati adatokat, erőforrásokat, a felhasználásra jogosult entitásokkal (legyen szó külső felhasználóról, üzleti partnerről vagy beszállítóról). A KPMG Identitáskezelési szolgáltatása segíti a szervezeteket a megfelelő szerepkörök és azok kezelési stratégiájának kialakításában, konszolidálhatóvá, irányíthatóvá és implementálhatóvá téve a szükséges folyamatokat és eljárásokat.

Jogosultság és feladatkör szétválasztási (Segregation of duties) vizsgálatok

Komplex, sokrendszeres környezetben, vagy nagyszámú felhasználó esetén szolgáltatásunk segít a jogosultságokat úgy kialakítani, hogy minimálisra csökkenjen az illetéktelen hozzáférések, és ezáltal a csalás kockázata, valamint a folyamatos adminisztráció és karbantartás is hatékonyan és megbízhatóan működhessen. Társaságunk nagy tapasztalattal rendelkezik a feladatkörök szétválasztása (segregation of duties) terén is.

Központosított naplóállomány kezelés

Pénzügyintézeteknél és nagyvállalatoknál végzett információbiztonsági munkáink során egyre gyakrabban merül fel az igény a biztonsági és üzemeltetési naplóbejegyzések központi gyűjtésére és azok elemzésére. Az informatikai kockázatok csökkentése érdekében, valamint a HPT 13/B. §5 d. bekezdésének, így a felügyeleti szervek előírásainak eleget téve, az informatikai rendszerek naplóállományainak kezelésére olyan szolgáltatást fejlesztettünk ki, amely integrálja az események kezelését, valamint azok valósidejű és retrospektív kiértékelését.

Kapcsolat:

KPMG Tanácsadó Kft.

1139 Budapest, Váci út 99.

Gaidosch Tamás, partner

Tel.: (+36 1) 887-7139

e-mail: tamas.gaidosch@kpmg.hu

Sallai György, senior menedzser

Tel. (+36 1) 887-6620

e-mail: gyorgy.sallai@kpmg.hu

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

© 2008 KPMG Tanácsadó Kft., a Hungarian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.