Informatikai kockázat-kezelési szolgáltatások

KPMG Technology Assurance

Információ-biztonsági tanácsadás

Felhasználó- és hozzáférés-kezelés

A KPMG felhasználó- és hozzáférés-kezelési (IAM) szolgáltatásai segítenek összegyűjteni a társaságuknál használatban lévő felhasználói azonosítókat, kialakítani azt a stratégiát és azokat az üzleti folyamatokat, amelyekkel a felhasználói jogosultságok és az információhoz való hozzáférés hatékonyan kezelhető. Ezen túlmenően az általunk nyújtott szolgáltatások része az IAM folyamatokat támogató rendszerek megtervezése és felépítése is.

Információbiztonsági szabályzatok készítése, felülvizsgálata

A nemzetközi szabványok és ajánlások (ISO 27000-es szabványcsalád, COBIT) mentén kialakított módszertanunk segít társaságának olyan információbiztonsági politika, szabályzatok és támogató eljárások kidolgozásában, valamint bevezetésében, amelyek megteremtik az információbiztonság korszerű dokumentációs hátterét.

Üzletmenet-folytonosság kezelés

Az üzletmenet-folytonosság kezelési szolgáltatásunk keretében segítünk, hogy társasága csökkenteni tudja az időkritikus folyamatok elérhetetlenségének kockázatát, valamint biztosítsa a kapcsolódó erőforrások gyors helyreállítását vagy pótlását egy esetleges katasztrófahelyzet után. A KPMG segít társaságának az üzletfolytonossági keretrendszerük és terveik kidolgozásában, bevezetésében és karbantartásában.

Naplóállomány-kezelés

Ezen szolgáltatásunk elősegíti, hogy társaságuk naplóállomány-kezelésbe és -elemzésbe fektetett idő- és pénzbeli ráfordításai a lehető legalacsonyabb szinten tartva is folyamatosan értéket teremtsenek a társaság számára, az alkalmazott naplóállománykezelési eljárások megfeleljenek a változó és egyre szigorúbbá váló szabályozásoknak, valamint, hogy a társaságnál semmilyen a szokásostól eltérő tevékenység ne maradhasson felderítetlen.

Adatszivárgás elleni védelem kialakítása (DLP)

A KPMG adatszivárgás elleni védelmet támogató szolgáltatásai elősegítik az Önök adatvédelmi fejlesztési igényeinek azonosítását és kielégítését. Adatvagyonleltár készítésével meghatározzuk a védendő adatok körét, felmérjük az adatszivárgásra alkalmas csatornákat, illetve társaságuk adatszivárgás elleni védelmének aktuális érettségi szintjét, majd ennek eredményeire alapozva kijelöljük a szükséges fejlesztési irányokat. Támogatást biztosítunk az igényeiknek leginkább megfelelő, az adatszivárgást megelőző informatikai megoldások kiválasztásában és bevezetésében.

Adatkezelési és adatvédelmi tanácsadás

A KPMG adatkezelést és adatvédelmet támogató szolgáltatásai segítséget nyújtanak ahhoz, hogy társaságuk képes legyen a különleges védelmet igénylő munkavállalói és ügyféladatok kezelését hatékonyan és a törvényi előírásoknak megfelelően ellátni. Szakértőink közreműködnek adatosztályozási rendszerük továbbfejlesztésében, adatkezelési megoldásaik törvényi és informatikai biztonsági megfelelőségének ellenőrzésében, az adatszivárgások eredményes menedzselését szolgáló megoldások bevezetésében, továbbá a már bekövetkezett incidensek költséghatékony kezelésében is.

Szoftvereszköz-menedzsment és licencoptimalizálás

A szoftvereszköz-menedzsment kritikus tényezője a korszerű IT-környezet kialakításának. A megfelelő stratégia hozzájárul az informatikai költségek, valamint a szoftverek birtoklásához és használatához kapcsolódó kockázatok csökkentéséhez, továbbá növeli társaságánál az informatikai terület és a

végfelhasználók hatékonyságát. A KPMG segít társaságának a szoftvereszköz-menedzsment körébe tartozó folyamatok, szabályzatok és eszközök érettségének értékelésében, valamint támogatást nyújt azok optimalizáláshoz.

ITIL szerinti működés kialakításának támogatása

A KPMG szakértői támogatást nyújtanak ITIL alapú szolgáltatásmenedzsment-rendszer bevezetéséhez, ezen keresztül az informatikai szolgáltatások transzparens és mérhető működésének megalapozásához. Megoldásunkkal javítható a szervezeti hatékonyság, növelhető a szervezeti egységek közötti együttműködés. A beszállítók teljesítései ellenőrizhetővé és elszámoltathatóvá válnak. A hatékony eszköz- és konfigurációmenedzsmenttel megvalósítjuk a támogatási szerződések, illetve a külső és belső szolgáltatások összhangját. A kialakított rendszer segítségével optimalizálható az IT-üzemeltetésre és -fejlesztésre fordított pénzeszközök felhasználása.

Információbiztonsági kockázatelemzés

Átfogó információbiztonsági kockázatelemzésünk segít a társaságára ható kockázatok pontos megismerésében, kezelésében és a védekezésre való felkészülésben. Az eszköz- és információvagyon felmérése után feltérképezzük a jellemző fenyegetéseket, üzletihatás-elemzéssel előre jelezzük a fenyegetések bekövetkezése esetén a társaságot érő kár jellegét, valamint a historikus adatok, korábbi tapasztalataink és interjúk alapján meghatározzuk e fenyegetések jövőbeli bekövetkezési valószínűségét. Az így szerzett információk alapján rangsoroljuk a társaság számára releváns valamennyi információbiztonsági kockázatot, és intézkedési tervet készítünk.

Informatikai audit típusú szolgáltatások

Adatmigráció auditja és támogatása

Migráció-minőségbiztosítási és -validációs szolgáltatásunk segíti ügyfeleinket a migráció megtervezésében, végrehajtásában, valamint a migráció utólagos ellenőrzésében. A validációt, azaz a forrás- és a célrendszerből nyert adatok – akár teljes körű – összehasonlítását szoftveres elemző eszközök segítségével végezzük, ezáltal a vizsgálandó adatok nagy mennyisége nem jelent akadályt, vizsgálatunkat kérésre pozitív bizonyosságot adó igazolással zárhatjuk.

Általános informatikai audit

Egy általános vagy fókuszált IT-audit sztenderd eljárások, irányelvek és metodológiák (COBIT, ISO 27001) alapján végzett vizsgálat, amely magában foglalja az informatikai biztonság menedzselésének, szabályozásának és az informatikai környezet általános kontrolljainak vizsgálatát. Segítünk ügyfeleinknek azonosítani és értékelni az információbiztonsági kockázatokat, és kialakítani egy a hazai jogszabályoknak és a nemzetközi szabványoknak egyaránt megfelelő kontrollkörnyezetet.

Informatikai átvilágítás

Az informatikai átvilágítás a megjelölt társaság informatikai szervezetének, folyamatainak, üzletileg kritikusabb informatikai rendszereinek, infrastruktúrájának és kontrollkörnyezetének vizsgálatára terjed ki. Ezen belül is a fontosabb kockázati területekre fókuszál. Ilyen vizsgálatokat jellemzően befektetők vesznek igénybe, hogy megismerjék a felvásárolni kívánt társaság informatikai érettségi szintjét.

IT belső ellenőrzés támogatása

A KPMG az IT belső ellenőrzési rendszerek működtetése, átvilágítása és fejlesztése révén segíti ügyfeleit a vállalati értékek megőrzésében. Szolgáltatásaink közé tartozik az IT belső ellenőrzési folyamatok optimalizálása, a valós idejű IT belső ellenőrzést támogató eszközrendszerek fejlesztése, speciális feladatok szakértői támogatása (például visszaélések felderítése, tömeges adatelemzés terén), továbbá – a társaság igényeihez szabott tréningprogram keretében – az érintett munkatársak felkészítése IT belső ellenőrzési rendszerek alkalmazására.

Kiszervezett tevékenységek feletti kontrollok megfelelőségi auditja (ISAE 3402, SSAE 16)

Az ISAE 3402 és az SSAE 16 olyan auditálási szabványok, amelyek formális jelentésben értékelik a szolgáltató (kiszervezett tevékenységet végző) szervezeteknél kialakított és bevezetett ITkontrollokat, valamint ezek működési hatékonyságát. Az SSAE 16 az Amerikai Egyesült Államokban, míg az ISAE 3402 az egyéb országokban lépett a korábbi SAS 70 szabvány helyébe.

Üzleti rendszerek biztonsági és funkcionális auditja

A biztonsági audit keretében áttekintjük az üzleti rendszerek biztonsági beállításait, feltárjuk az azokban lévő adatok biztonságát veszélyeztető kockázatokat és kontrollhiányosságokat, és szükség esetén javaslatot teszünk a megfelelő védelmi intézkedésekre. A funkcionális audit során megvizsgáljuk, hogy az informatikai rendszerek az előírt üzleti logika szerint működnek-e, és azonosítjuk azokat a területeket, amelyek nem felelnek meg a hatékonysági, valamint az üzleti követelményeknek.

Szerepkör-szétválasztás támogatása és auditja (SoD)

Feltárjuk az üzleti rendszerekben lévő bonyolult jogosultsági struktúrákból és beállításokból fakadó problémákat, különösen a visszaélésekre lehetőséget adó szerepkör-összeférhetetlen¬ségeket, amelyek komoly anyagi veszteséget is okozhatnak. A mai ERP-rendszerek komplex jogosultsági struktúrája már egyszerű módszerekkel nem elemezhető, ezért különböző elemző szoftvereket alkalmazunk vizsgálatunk során. Különösen kiemelkedő szakértelemmel és eszköztárral rendelkezünk SAPjogosultságok elemzése terén.

Rendszer interfészek auditja

A rendszerek közötti interfészek számos kockázatot hordoznak magukban. Az adatok elveszhetnek, módosulhatnak, vagy éppen duplikálódhatnak a rendszerek között, így jelentősen befolyásolhatják más rendszerek működéseit, akár a társaság főkönyvi eredményeit is. Vizsgálataink segítségével feltárjuk az interfészek esetleges hibás működését és biztonsági hiányosságait, majd javaslatot teszünk az elvégzendő javításokra.

Rendszerbevezetést megelőző és követő vizsgálatok

A rendszerbevezetést megelőzően nyújtott szolgáltatásunk segíti a bevezetéssel kapcsolatos részfeladatok megtervezését és elvégzését, például a társaság igényeinek legmegfelelőbb rendszer és szállító kiválasztását. Biztosítjuk, hogy a társaság minden szükséges kontrollt megfelelően alakítson ki, és hatásosan működtessen. A rendszer¬bevezetést követő vizsgálatunk során ellenőrizzük az adatmigráció megfelelőségét, és biztosítjuk, hogy a már élesbe állított rendszer a megfogalmazott funkcionalitásnak megfelelően működjön, vagyis lefedje a specifikációt és a valós üzleti igényeket.

Informatikai törvényi megfelelőség

Az informatikai kontrollkörnyezet kialakítását és működtetését egyre szigorúbban szabályozzák a hírközlési, a pénzügyi (banki, biztosítói, alapkezelői, stb.), valamint az állami és önkormányzati szektorra vonatkozóan is. Ezen túlmenően egyes iparágak esetében a jogalkotó a vizsgált rendszerek funkcionális megfelelési kritériumaira is kitér. Szolgáltatásunk keretében azonosítjuk a társaságukra vonatkozó jogszabályokat, ellenőrizzük az ezeknek való megfelelést, illetve javaslatokat teszünk az esetleges hiányosságok kiküszöbölésére.

Social engineering audit és biztonságtudatossági program

Az alkalmazottak félrevezethetősége az egyik legsúlyosabb nem technikai jellegű információbiztonsági kockázat a szervezetek életében. Előre egyeztetett módszertanra és szabályokra támaszkodva valós social engineering típusú támadásokat szimulálunk, és azok eredményei alapján akciótervet dolgozunk ki a hasonló esetek elkerülése érdekében. Vizsgálatunkhoz oktatás is kapcsolódhat, melynek eredményeként a munkatársak tisztább képet kapnak az őket fenyegető lehetséges támadási technikákról és a betartandó biztonsági előírásokról.

Szabványi megfelelőségi audit

Szolgáltatásunk keretében a nemzetközi szabványokban (pl.: ISO 27001, ISO 20000, ISO 22301, ISAE 3402, PCI DSS) lefektetett követelményeknek való megfelelést vizsgáljuk. Vizsgálatunk eredményei alapján vállaljuk a felkészítést a tanúsító vagy megújító auditokra is, amelyek révén társasága növelheti az érdekelt felek bizalmát, valamint üzleti előnyre tehet szert a versenytársakkal szemben.

Technikai biztonsági vizsgálatok

Betörési tesztek

A betörési tesztek azokat a valós támadásokat és fenyegetéseket szimulálják, amelyek hátterében elégedetlen alkalmazottak, különböző felkészültségű külső támadók vagy akár ipari kémek állhatnak. Azonosítjuk a sérülékenységeket, részletesen ismertetjük ügyfelünkkel a lehetséges támadási szcenáriókat, majd a vezetőség és a technikai szakemberek számára is értelmezhető, illetve hasznosítható javaslatokat teszünk.

Rendszer-sérülékenységi vizsgálat

A sérülékenységi vizsgálat a rendszerek technikai gyengeségeit deríti fel, szisztematikusan megvizsgálva az elérhető szolgáltatásokat ismert hiányosságokat keresve, függetlenül attól, hogy ezek hálózati, operációs rendszer, adatbázis-, üzenetközvetítő, vagy alkalmazás-komponensekben fordulnak elő. A sérülékenységeket beazonosítjuk, teszteket végzünk, majd korrekciós javaslatokat teszünk és ismertetjük ügyfelünkkel a sikeres támadási szcenáriókat.

Konfigurációvizsgálat

A KPMG szakértői által végzett konfiguráció-vizsgálat a kritikus szerverek azonosítása és beállításaik független értékelése révén elősegíti társaságuk informatikai infrastruktúrájának hatékony

fejlesztését. Munkatársaikkal együttműködve azonosítjuk az üzleti folyamatok szempontjából kritikus szervereket, majd a KPMG módszertani előírásai és az iparági sztenderdek alapján felmérjük ezek operációs rendszer szintű (például hozzáférés-kezelési, rendszerfrissítési), valamint azon túlmutató (például vírusvédelmi) beállításait.

Kibervédelem

A KPMG kibervédelmi szolgáltatásai révén társaságuk képessé válik megalapozott döntéseket hozni arról, hogy a megfelelőségi szemléletű ITbiztonsági megoldásokon túl mire célszerű pénzt áldozni a kritikus adatok napjaink kihívásainak megfelelő, felkészült támadók ellen is hatásos védelme érdekében. Mindehhez a kockázati környezet, valamint a rendszereiken elvégzett sérülékenység-vizsgálatok és betörési tesztek eredményeinek komplex kiértékelésén nyugvó megoldások kialakítása szükséges, amelyhez szakértőink teljes körű támogatást biztosítanak.

Mobilalkalmazások vizsgálata

A KPMG az általános alkalmazásbiztonsági vizsgálatok mellett a mobilalkalmazások védelmi szempontú ellenőrzésére irányuló szakértői szolgáltatásokat is kínál ügyfeleinek. Ezek során különös figyelmet fordítunk az adott mobilplatform és a kritikus mobilalkalmazások kliens oldali biztonságára. Kiértékeljük többek között, hogy az egyes hardverkomponensekből az alkalmazások által felhasznált adatok (pl. GPS-koordináták) hitelessége, illetve az alkalmazások kriptográfiai eljárásaihoz használt kulcsok tárolásának, forgalmazásának védelme biztosított-e.

ISO 27002 szerinti állapotfelmérés

A KPMG vállalja társaságuk információbiztonsági helyzetének ISO 27002-es szabvány szerinti felmérését a kontrollkörnyezet hiányosságainak azonosítása, valamint információbiztonsági stratégiájuk erre alapozott ki-, illetve továbbfejlesztése céljából. A társaság munkatársaival együttműködve azonosítjuk az információbiztonság szempontjából releváns folyamatokat, és megvizsgáljuk a kapcsolódó kontrollok kialakítását, működési hatékonyságát. Támogatjuk Önöket az ISO 27002-es szabvány szerinti megfelelőséget biztosító megoldás kialakításában.

Adatvédelmi irányelvek vizsgálata

A társaságuk különböző szervezeti egységei által készített és alkalmazott szabályozók adatvédelmi átvilágítása révén a KPMG komplex támogatást nyújt a törvényi előírásoknak való megfelelőség biztosításához. Megvizsgáljuk többek között adatvédelmi szabályzatukat, az ahhoz kapcsolódó nyilatkozatokat, kézikönyveket, IT-biztonsági szabályzatukat, a kialakított incidensmenedzsment-eljárásaikat, valamint az adatosztályozási és adatselejtezési eljárásaikat. Adatvédelmi szakértőink támogatást biztosítanak a feltárt hiányosságok orvoslásához.

Adatvédelmi irányítási struktúra tervezése

A KPMG informatikai támogató megoldásai elősegítik az adatvédelmi követelmények integrációját a szervezetirányítási struktúrába. Komplex szolgáltatásunk keretében a társaságuk munkatársainak személyes és különleges adatokhoz való hozzáférését szabályozó kritériumok törvényi előírásoknak megfelelő kidolgozásán túl közreműködünk olyan informatikai eszközökkel támogatott eljárások kialakításában is, amelyek révén az adatvédelmi követelmények betartásának valós idejű ellenőrzése a szervezet teljes vertikumában biztosítható.

Amennyiben felkeltettük érdeklődését, a részletekkel kapcsolatosan keressen bennünket az alábbi elérhetőségeinken:

KPMG.hu