Az ISO 27001-es szabvány bevezetése és tanúsítása

Informatikai Kockázatkezelési Tanácsadás

Biztonságban vannak társaságuk adatai? Megbízhat abban, hogy a társaság hatékonyan válaszol napjaink információbiztonsági kihívásaira? Tudja bizonyítani információbiztonsági felkészültségét külső fél számára is?

Minden társaság hírnevének és adatinak védelme kiemelten fontos feladat, hiszen a megbízhatóság a siker egyik feltétele. A felgyorsult infokommunikációs technológia révén egy az adatok biztonságát érintő incidens híre azonnal eljut a versenytársakhoz és az ügyfelekhez, ami jelentős reputációs veszteséget okoz. Tapasztalataink szerint az előírt biztonsági követelményeknek való megfelelés, a hírnév védelme, rendkívül komplex feladat, amelynek hatékony megvalósításához nélkülözhetetlen a társaság sajátosságaihoz illeszkedő, a nemzetközileg elismert ISO 27001-es szabvány átfogó keretrendszerére támaszkodó biztonságirányítási rendszer bevezetése és működtetése.

Ismerősek Önnek az alábbi problémák?

- Társaságuk egyre növekvő mértékben függ az informatikai infrastruktúrától, és akár egy rendszer kiesése is az üzleti folyamatok megbénulásához vezethet, azáltal, hogy nem állnak rendelkezésre a szükséges adatok;
- a társaság üzletmenet-folytonosságát akadályozó hibák száma magas, a hibák megoldása ad hoc jellegű;
- a társaság adatainak sérülése vagy nyilvánosságra kerülése pénzügyi veszteséggel járhat;
- az érdekelt felek igazolást kérnek a vállalat információbiztonságára vonatkozóan;
- a szektorban kialakult versenyhelyzetben a Társaság ügyfeleinek megtartása és az új partnerek szerzése állandó feladat, amelynél a bizalom kiemelt fontosságú;alapos kockázatelemzés hiányában nem állapítható meg egyértelműen, hogy a biztonság növelésére szánt költségeket valóban megtérülő fejlesztésekre fordították-e; a védelmi szint nem számon kérhető;
- a társaság üzleti területen dolgozó munkavállalói nem érzik feladatuknak az információ védelmét, úgy gondolják, ez IT-feladat, így szakadék alakul ki az IT és az üzleti terület között.

Hogyan tudunk a segítségére lenni?

A KPMG alábbi, az ISO 27001-es szabvány bevezetéshez és tanúsításához kapcsolódó szolgáltatásai három szakaszban segítik Társaságukat a biztonságirányítási rendszer kialakításában és a tanúsítvány megszerzésében:

I. szakasz – a jelenlegi állapot felmérése: felmérjük az információbiztonsági érettséget, a legjobb gyakorlattól való eltérés mértékét. A biztonsági kontrolok ellenőrzése kiterjed a társaság technológiájára, folyamataira és munkavállalókra vonatkozó kontrolokra;

II. szakasz – tanúsító auditra való felkészítés:

- **Erőforrás-allokáció:** a jelentős többleterőforrást igényelő szabványbevezetéshez biztosítjuk a megfelelő szakmai tudású munkaerőt; támogatást nyújtunk a szabvány követelményeinek megértésében;
- **Dokumentumrendszer kialakítása:** megvizsgáljuk az ISO 27001-es szabvány hatókörébe tartozó szabályzatokat, majd javaslatokat teszünk a szabályozás fejlesztésére; igény esetén elkészítjük a hiányzó dokumentációt, megírjuk az információbiztonsági politikát;
- **Kockázatelemzés:** segítünk a kockázatelemzési módszertan kidolgozásában, a kockázatelemzés elvégzésében, valamint a társaság vezetősége által elfogadható szintre csökkentjük a megállapított kockázatok mértékét;
- **Alkalmazhatósági nyilatkozat készítése:** az auditra való felkészítés során, a társasággal együttműködve elkészítjük az ISO 27001-es szabvány alkalmazhatósági nyilatkozatát, amelyben a biztonsági kontrolloknak való megfelelést támasztjuk alá;

III. szakasz – ISO 27001-audit lebonyolítása: támogatjuk a minősítés megszerzésének folyamatát, amellyel külső fél számára is igazolhatóvá válik, hogy a társaság az információbiztonság területén megfelel az ISO 27001-es szabvány követelményeinek.

Milyen előnyöket nyújtunk?

- Az ISO 27001 módszertana alapján képesek vagyunk hatékonyan csökkenteni a jogi és szabályozási megfelelés hiányából eredő károkat;
- a segítségünkkel kialakított, szabvány szerinti működés növeli az érdekelt felek bizalmát, a minősítés megszerzése üzleti előnyt jelent a vetélytársakkal szemben;
- csökkentjük az incidensek által okozott kiesési időt, ezáltal minimalizálva a károkat és növelve a folyamatok hatékonyságát;
- a keretrendszer segítségével összehangoljuk az üzleti és az IT-szempontokat, ezáltal biztosítva az eredményes együttműködést, a közös célok elérését;
- az ISO-szabvány szerinti működés esetén a vezetőség biztos lehet afelől, hogy a társaság teljesíti a minőségi elvárásokat;
- A szabvány bevezetése által nő a munkavállalók biztonságtudatossága.

Amennyiben felkeltettük érdeklődését, a részletekkel kapcsolatban keressen bennünket az alábbi elérhetőségeinken.

Kapcsolat:

Kórász Tamás
partner
T.: +(36) 70 333 1507
E.: Tamas.Korasz@kpmg.hu

KPMG.hu

Konrád Péter
menedzser
T.: +(36) 1 887 7343
E.: peter.konrad@kpmg.hu

KPMG.hu