A NÁDOR RENDSZERHÁZ KFT.

AJÁNLATA

A

Taksonyi Polgármesteri Hivatal részére

Informatikai Biztonsági Feladatok elvégzésére

EREDETI PÉLDÁNY

Ajánlati szám: 15051201129

Tartalomjegyzék

1152 Budapest, Telek u. 7-9. Tel.: +36 (1) 470-5000 Fax: +36 (1) 470-5011
palyazat@nador.hu www.nador.hu

Előzmények

A magyar Országgyűlés 2013. április 15-én fogadta el az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényt (2013. évi L. tv.) (Infobizt. tv./ Ibtv.). A törvény felhatalmazása alapján 2013. decemberében fogadta el a Kormány, illetve hirdették ki a felhatalmazott minisztériumok a törvény végrehajtási rendeleteit.

Határidők

1. A törvény hatályba lépésének időpontja 2013. július 1.
2. Nyilvántartásba vétel szempontjából a Hatóságnak be kell jelenteni 60 napon belül (2013. augusztus 29.):
    a. Szervezet azonosító adatit;
    b. az elektronikus információs rendszer biztonságáért felelős személyét és azonosító adatait, telefon- és telefax számát, e-mail címét, előírt végzettségét;
3. Nyilvántartásba vétel szempontjából a Hatóságnak be kell jelenteni 90 napon belül (2013. szeptember 28. később 2014. február 4-re módosították) a szervezet információ biztonsági szabályzatát. Abban az esetben, ha a szervezet nem rendelkezik Információ Biztonsági Szabályzattal, akkor annak várható elkészülési időpontját kell megadni.
4. A szervezetnek 1 éven belül (**2014. július 1-ig**) el kell végeznie végrehajtási rendeletek alapján:
    a. információs rendszerek biztonsági osztályba sorolását;
    b. szervezet tényleges biztonsági szintbe sorolását;
5. Az elektronikus információs rendszer biztonságáért felelős személynek 5 éven belül (2018. július 1.) az előírt képzési követelménynek eleget kell tennie.

Biztonsági szintbe, osztályba sorolás

Az Ibtv. hatálya alá tartozó elektronikus információs rendszert biztonsági osztályba kell sorolni, bizalmasság, sértetlenség és rendelkezésre állás szempontjából, az Ibtv. 7.§ -ában, valamint a 77/2013. (XII.19.) NFM rendelet 1.§ és 1. számú mellékletben rögzített követelményeknek megfelelően.
A szervezet biztonsági szintje mindig az elektronikus információs rendszereinek a legmagasabb biztonsági osztálynak megfelelő fokozat.
A törvény meghatározza egyes szervezeteknek minimálisan előírt biztonsági szintjét.

Ugyancsak biztonsági szintbe kell sorolni Az Ibtv. hatálya alá tartozó szervezetet is. A biztonsági szintekbe sorolás a 77/2013. (XII.19.) NFM rendelet 2. melléklete alapján történik. Ezen felül meg kell állapítani a szervezet biztonsági szintjét, amely a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de legalább az Ibtv. 9. § (2) bekezdésében meghatározott biztonsági szintű – Ibtv. 9.§.
Ha a szervezet nem éri el a számára előírt biztonsági szintet, úgy az Ibtv. 10. §-a alapján lehetősége van a követelmények fokozatos teljesítésére – Ibtv. 10. § (2)- (7)Ibtv. 10.§.

Az információ biztonságáért felelős személy

Feladatellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést. Személyében felel az információs rendszerek védelméhez kapcsolódó feladatok ellátásáért. Amennyiben a rendszerek mérete, a biztonság szintje, vagy más okból lényeges, akkor az információ biztonságáért felelős személy vezetésével egy külön szervezeti egység hozható létre. Vele szemben támasztott követelmények:

- büntetlen előélet
- feladatellátáshoz szükséges felsőfokú végzettség és szakképzettség (NKE képzés)
- mentesül a szakképzettség alól aki:
    - akkreditált nemzetközi képzettséggel rendelkezik (pl: ISACA minősítések)
    - e szakterületen szerzett 5 év szakmai gyakorlattal rendelkezik.

Az elektronikus információs rendszer biztonságáért felelős személy feladatai az Ibtv. 13.§-a alapján:

- Gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- Elvégzi vagy irányítja a fentiek szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- Előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
- Előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
- Kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal,
- Bármely elektronikus információs rendszerét érintő biztonsági eseményről történő tájékoztatás a 73/2013. (XII.4.) NFM rendeletben meghatározottak szerint tájékoztatni köteles az Ibtv.-ben meghatározott szervet,
- Amennyiben indokolt a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.
- Biztosítja az Ibtv-ben meghatározott követelmények teljesülését az Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő:
    - a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők biztonsággal összefüggő tevékenysége esetén.
    - ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők biztonsággal összefüggő tevékenysége esetén.
- Az Ibtv-ben meghatározott követelmények teljesüléséről jogosult a közreműködőtől tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

- A helyszíni ellenőrzéssel érintett szervezet elektronikus információs rendszer biztonságáért felelős személye az Ibtv. 12. § c) pontja alapján köteles a Hatósággal együttműködni.

Jelen szakmai ajánlatunkkal az első biztonsági szint eléréséhez szükséges feladatokat foglaltuk össze.

Általánosságban elmondhatjuk, hogy a Hivataloknak az alábbi folyamatokat kell bevezetniük, nyilvántartásokat, szabályzatokat és eljárásrendeket kell elkészíteniük a törvényi megfelelés érdekében (1. szint) július 1-ig:

	Adminisztratív védelmi intézkedések	1-es szint	2-es szint
3.1.1.	**Szervezeti szintű alapfeladatok**	**Kötelező**	**Kötelező**
3.1.1.1.	*Informatikai biztonságpolitika*	*Kötelező*	*Kötelező*
3.1.1.2.	*Informatikai biztonsági stratégia*	*Kötelező*	*Kötelező*
3.1.1.3.	*Informatikai biztonsági szabályzat*	*Kötelező*	*Kötelező*
3.1.1.4.	*Az elektronikus információs rendszerek biztonságáért felelős személy*	*Kötelező*	*Kötelező*
3.1.1.5.	*Pénzügyi erőforrások biztosítása*	*Nem kötelező*	*Kötelező*
3.1.1.6.	*Az intézkedési terv és mérföldkövei*	*Nem kötelező*	*Kötelező*
3.1.1.7.	*Az elektronikus információs rendszerek nyilvántartása*	*Kötelező*	*Kötelező*
3.1.1.10.	*Kockázatkezelési stratégia*	*Nem kötelező*	*Kötelező*
3.1.1.11.	*Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás*	*Kötelező*	*Kötelező*
3.1.2.	**Kockázatelemzés**	**Kötelező**	**Kötelező**
3.1.2.1.	*Kockázatelemzési eljárásrend*	*Kötelező*	*Kötelező*
3.1.2.2.	*Biztonsági osztályba sorolás*	*Kötelező*	*Kötelező*
3.1.2.3.	*Kockázatelemzés*	*Kötelező*	*Kötelező*
3.1.3.	**Tervezés**	**Nem kötelező**	**Kötelező**
3.1.3.1.	*Biztonságtervezési eljárásrend*	*Nem kötelező*	*Kötelező*
3.1.3.2.	*Rendszerbiztonsági terv*	*Nem kötelező*	*Kötelező*
3.1.3.3.	*Személyi biztonság*	*Nem kötelező*	*Kötelező*
3.1.3.3.2.	*Viselkedési szabályok az interneten*	*Nem kötelező*	*Kötelező*
3.1.4.	**Rendszer és szolgáltatás beszerzés**	**Nem kötelező**	**Kötelező**
3.1.4.2.	*Beszerzési eljárásrend*	*Nem kötelező*	*Kötelező*
3.1.4.4.	*A rendszer fejlesztési életciklusa*	*Nem kötelező*	*Kötelező*
3.1.4.8.	*Külső elektronikus információs rendszerek szolgáltatásai*	*Nem kötelező*	*Kötelező*
3.1.6.	**Emberi tényezőket figyelembe vevő - személy - biztonság**	**Kötelező**	**Kötelező**
3.1.6.5.	*Eljárás a jogviszony megszűnésekor*	*Kötelező*	*Kötelező*
3.1.6.8.	*Fegyelmi intézkedések*	*Kötelező*	*Kötelező*
3.1.7.	**Tudatosság és képzés**	**Kötelező**	**Kötelező**
3.1.7.1.	*Képzési eljárásrend*	*Kötelező*	*Kötelező*
3.1.7.2.	*Biztonság tudatosság képzés*	*Kötelező*	*Kötelező*

Szakmai ajánlat

A Nádor Rendszerház Kft. sok éves szakmai tapasztalata alapján jelen dokumentumban ajánlatot tesz kiszervezett tevékenység formájában a 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról (a továbbiakban Ibtv.) és a végrehajtási utasításokban foglalt feladatok elvégzésére és az információ biztonsági dokumentációk elkészítésére vonatkozóan Taksony Polgármesteri Hivatal (továbbiakban: Hivatal) részére.

A Hivatalnak a fenti lista és a korábbi egyeztetések valamint ajánlatkérése alapján a törvényi megfelelés érdekében a következő feladatai vannak a 2015. június 30-ai határidőig.

- Informatikai Biztonsági Szabályzat felülvizsgálata
- Informatikai Biztonsági Politika elkészítése és hatályba helyezése
- Informatikai Biztonsági Stratégia elkészítése és hatályba helyezése
- A fenti szabályzatok elküldése a Nemzeti Elektronikus Információbiztonsági Hivatal (továbbiakban: NEIH) részére
- Biztonsági szintbe és osztályba sorolás elvégzése.
- Cselekvési terv elkészítése, hatályba helyezése és elküldése a NEIH részére.
- Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárások: és nyilvántartások úgymint Felhasználói jogosultságok kiosztásának eljárása és nyilvántartása, Eszköznyilvántartás (hardver és szoftver), Változáskezelési eljárásrend kidolgozása.
- Kockázatelemzés elvégzése és kockázatkezelési eljárásrend kidolgozása.
- HR folyamatok felülvizsgálata (fegyelmi és munkaviszony megszűnésekor alkalmazandó eljárások).
- Képzési eljárásrend kidolgozása és a dolgozói képzés időpontjának meghatározása.

1.1. Kockázatelemzés

A biztonsági követelményeket a biztonsági kockázatok módszeres felmérésével szokás megállapítani. Az egyes óvintézkedésekre kiadott költségekkel lehet ellensúlyozni a biztonsági hibákból eredő valószínű üzleti veszteségeket.
A kockázatbecslő eljárásokat alkalmazhatjuk akár az egész szervezetre, akár annak egyes részeire, akár csak egyes egyedi informatikai rendszereire, esetleg olyan sajátos rendszerösszetevőkre vagy szolgáltatásokra, amelyekre az megvalósítható, reális és hasznos.

A ***kockázatelemzés*** annak rendszeres megfontolása, hogy:

a) mi az a kár, amely valószínűleg valamely ügyviteli hiba eredménye, figyelembe véve az információ és más vagyon titkosságának, sértetlenségének és rendelkezésre állásának elvesz(t)ése lehetséges következményeit;
b) milyen a hiba előfordulásának valós valószínűsége az uralkodó fenyegetések és sérülékenységek, valamint a megvalósított óvintézkedések fényében.

Ennek a felmérésnek az eredménye segíteni fog az alkalmas vezetői tevékenységeknek és azoknak a prioritásoknak a meghatározásában, amelyek az informatikai biztonsági kockázatkezeléshez, valamint azoknak az óvintézkedéseknek a megvalósításához szükségesek, amelyeket éppen ezen kockázatok elleni védekezésre választottak ki. Esetleg többször is ajánlatos lehet megismételnünk a kockázatbecslő és az óvintézkedéseket kiválasztó eljárásokat ahhoz, hogy az adott szervezet különböző részegységeit, vagy egyedi informatikai rendszereit is mind áttekintsük.
Azért fontos, hogy a biztonsági kockázatokat és a megvalósított óvintézkedéseket időről időre felülvizsgáljuk, hogy

a) figyelembe vegyük az hivatali követelmények és prioritások változásait,
b) megfontoljuk az új fenyegetéseket és sérülékenységeket,
c) visszaigazoljuk, hogy az óvintézkedések hatékonyak és megfelelőek maradtak.

A felülvizsgálatot különböző mélységben ajánlatos elvégezni, attól a szinttől függően, amely szintet a vezetőség a kockázatok változó szintjeként még el tud fogadni. A kockázatbecslő eljárásokat gyakran előbb a felső szinten hajtják végre, mintegy a felsőbb szintű erőforrásokat elsőbbséggel kezelve, majd csak azután térnek át a részletesebb felmérési szintre, az egyes különleges kockázatokra

ISO 17799/27001 szerinti IT BIZTONSÁGI KOCKÁZATELEMZÉS (KIB 25 ajánlás)

Fázisok:

1. Kockázatelemzési szabályzat és módszertan (KIB 25 alapú)
2. Teljes körű IT sérülékenység és veszélyhányados becslés a Vagyonleltáron, valamint az Információbiztonsági folyamatokon
3. Kockázatelemzés
4. Kockázatkezelési tanácsadás a nagy kockázatú biztonsági rések kiküszöbölésére

Az informatikai rendszer biztonsági kockázatának elemzési módja:
Az informatikai rendszer biztonságát a kockázatelemzés módszerével vizsgáljuk. A meglevő folyamatok, eszközök és szabályzatok megfelelőségét ISO 27001 sztenderdhez viszonyítjuk. A kockázatelemzéshez általánosan Riskman (ITBC/ISO 27001) módszertant használunk.

Kockázati szintek meghatározása:

A kockázati szinteket 1-5-ig terjedő skálával határozzuk meg, ahol az 1 a legalacsonyabb, az 5 a legmagasabb szintet jelenti.

1152 Budapest, Telek u. 7-9. Tel.: +36 (1) 470-5000 Fax: +36 (1) 470-5011
palyazat@nador.hu www.nador.hu

A kockázati szint határokat az informatikai vagyonhoz és az adatállomány értékéhez viszonyítva határozzuk meg. Az összegyűjtött információkat szakembereink elemzik, értékelik, a kapott eredmények alapján készül el a kockázatelemzés.

1.2. Kockázatkezelő intézkedések elkészítése

Ha a kockázatelemzés során a biztonsági követelményeket és kockázatokat már meghatároztuk, ajánlatos lesz megválasztani és megvalósítani azokat az óvintézkedéseket (kockázat kezelő intézkedések), amelyekkel a kockázatot elfogadható szintre akarjuk lecsökkenteni. Az óvintézkedéseket a megvalósítási költségekre tekintettel ajánlatos megválasztani, figyelembe véve azt a kockázatot, amelyet alkalmazásával csökkenteni akarunk, illetve azt a lehetséges veszteséget, amelyet a biztonság megsértése fellépésével okoz. Ugyancsak ajánlatos figyelembe venni a pénzben ki sem fejezhető tényezőket, mint például a jó hírnév elvesztését.
A kockázatkezelő intézkedések dokumentum tartalmazza a rendszer felmérése alapján alkotott képet, megállapításainkat, javaslatainkat a hibák elhárítására, a veszélyek csökkentésére illetve kiküszöbölésére.

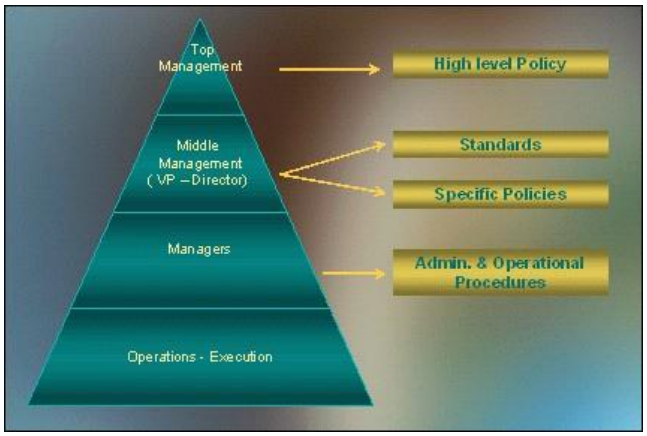
Az intézkedési terv kidolgozásakor figyelembe vesszük az Ibtv. és az Infotv által támasztott követelményeket is.

1.3. Cselekvési terv készítése a következő biztonsági szint elérésére

Az esetben, ha a kockázatelemzés szükségessé teszi, a következő biztonsági szint eléréshez cselekvési tervet készítünk, melynek szerves része az a költségszámítás, amely a cselekvési terv kapcsán előállt beruházások és fejlesztések formájában felmerülhetnek.

1.4. Informatikai biztonsági szabályozó környezet kialakítása

Az informatikai biztonság egyik feltétele a rendszerezett, szabályozott, jól átlátható működés. Ennek elemei, a felelősségi körök és jogosultságok pontos meghatározása, a jogszabályi környezet által megkövetelt szabályzatok, utasítások piramidális strukturáltságának megléte, a biztonsági folyamatok és a teendők dokumentáltsága.



Az Informatikai biztonság keretrendszerének elkészítését (IBIR/IBIK) az ISACA (Információrendszer Audit és Kontrol Egyesület) ajánlásai valamint az KIB 25 - ISO 17799/27001 szabványrendszere (PDCA elv) szerint dolgozzuk ki.
Ennek részei:

a) Informatikai Biztonsági Politika
b) Informatikai Biztonsági Stratégia
c) Informatikai Biztonsági Szabályzat

Mindhárom szabályozási elem a Miniszterelnöki Hivatal által publikált *„KÖZIGAZGATÁSI OPERATÍV PROGRAMOK IT BIZTONSÁGI KÖRNYEZETE”* követelményrendszer specifikációja és leírásai alapján készülnek el.

1.5. Interjúk

A kockázatelemzés elvégzését és a Hivatal IT folyamatainak megismerését interjúk lefolytatásával és a jelenlegi szabályzatok, utasítások, eljárásrendek áttanulmányozásával végezzük el. Az információk hatékony átadására előzetesen egyeztetett időpontban, körülbelül 30-60 perc időtartamban kerülne sor. Természetesen az IT szervezet tagjaival egy hosszabb beszélgetést szeretnénk lefolytatni.

Az interjúkba bevont személyek a következők lennének:

- Irodavezetők
- IT szervezet tagjai

Kereskedelmi ajánlat

Az általunk kínált szolgáltatásokkal a Hivatal biztosítja a teljes törvényi megfelelősséget és a jogszabályban foglalt feladatok és dokumentációk elkésztésének maradéktalan elvégzését a Nádor Rendszerház Kft. szakembereinek iránymutatása mellett.

Munkatársaink a feladatok végrehajtását csak támogatni tudják, azok megvalósítása a Hivatal felelőssége. A szabályzatokat a Hivatal kijelölt munkatársaitól kapott információk alapján, a Hivatal működési rendjéhez igazítják. Az eljárásrendek alapját, alapelveit rögzítik, de a tényleges adatfeltöltéshez elengedhetetlen a hivatali munkatársak, hivatali vezetők, adott területekért felelős csoportvezetők vagy ügyintézők közreműködése, az informatikusok dokumentációs és fejlesztési munkája. A kockázatkezelési eljárások kialakítása szoros együttműködést kíván a Hivatal részéről. A rendelkezésre álló rövid határidőn belül várhatóan számos fejlesztésről kell dönteni, azok eszközigényét biztosítani és bevezetni. A feladatokat abban az estben tudjuk megfelelő minőségben és határidőre elvégezni, amennyiben ez az együttműködés megvalósul.

A fentebb részletezett dokumentációk elkészítését és feladatok ellátását az alábbi áron biztosítjuk a Hivatal részére:

Megnevezés	Ráfordítás (munkanap)	Nettó egységár (Ft)	Nettó összesen (Ft)
Az 1. Biztonsági szint eléréséhez – 2015. június 30-ig			
IT Biztonsági Szabályzat felülvizsgálata	1	75 000 Ft	75 000 Ft
IT Biztonsági Stratégia elkészítése	1	75 000 Ft	75 000 Ft
IT Biztonsági Politika elkészítése	1	75 000 Ft	75 000 Ft
Kockázatelemzés - Kockázatkezelési eljárásrend elkészítése, kockázatelemzés elvégzése	3	75 000 Ft	225 000 Ft
Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárások: Felhasználói jogosultság kiadás –, Eszköznyilvántartás (hardver és szoftver) ellenőrzése és konzultáció azok elkészítésével kapcsolatban,	1	75 000 Ft	75 000 Ft
Informatikai rendszerek biztonsági osztályba sorolása és a szervezet biztonsági szintjének meghatározása	1	75 000 Ft	75 000 Ft
HR folyamatok felülvizsgálata (fegyelmi, eljárás munkaviszony megszűnésekor)	0,5	75 000 Ft	37 500 Ft
Képzési eljárásrend elkészítése	0,5	75 000 Ft	37 500 Ft
IT Biztonságtudatossági képzés – Hivatali dolgozók részére	Dolgozói létszám ismeretében külön ajánlat alapján1		
Cselekvési terv elkészítése	1	75 000 Ft	75 000 Ft
Összesen:			**750 000 Ft**

Egyéb feltételek

Ajánlati kötöttség

Az ajánlati kötöttség az ajánlattételi határidő lejártától számítva **30 napig** tart.

Fizetési feltételek

A fizetés számla ellenében a teljesítés t követően történik, **30 napos banki átutalással** az alábbi számlaszámra:

CIB Bank zRt. 11100104-10507328-01000003

Az ajánlati ár tartalmaz minden olyan költséget, amely az ajánlott feladatok teljesítésével összefügg.

Késedelmes fizetés esetén a Szállító a Ptk 301/A § (1) bek. meghatározott késedelmi kamatot jogosult felszámolni.

Bízunk benne, hogy ajánlatunk maradéktalanul megfelel elvárásaiknak. Amennyiben kérdése merül fel vagy további információra van szüksége, készséggel állunk rendelkezésére megadott elérhetőségeinken.

Budapest, 2015. május 12.

Budai László
IT Biztonságtechnikai üzletágvezető

NÁDOR RENDSZERHÁZ

1152 Budapest, Telek u. 7-9. Tel.: +36 (1) 470-5000 Fax: +36 (1) 470-5011
palyazat@nador.hu www.nador.hu

Referenciák bemutatása

(310/2004. (XII.23.) Korm. rend 15. § (1) bek. a) pont)

Szolgáltatás megnevezése	Megrendelő neve	Teljesítés ideje
IBF pozíció ellátása	Budapest Főváros XVII. kerület Rákosmente Önkormányzatának Polgármesteri Hivatala	2014.
IBF pozíció ellátása	Bajai Polgármesteri Hivatal	2014.
IBF pozíció ellátása, 2013. évi L. tv.	Lechner Lajos Tudásközpont Nonprofit Kft.	2014.
IBF pozíció ellátása	Budapest Főváros IV. kerület Újpest Önkormányzatának Polgármesteri Hivatala	2014.
IBF felkészítés	Soproni Polgármesteri Hivatal	2014.
Ethical Hacking (Black box, belső compliance) és IT biztonság szabályzat audit	Daten-Kontor Számítástechnikai Fejlesztő és Szolgáltató Kft.	2012.
Sérülékenység és IT Biztonsági audit	Károly Róbert Főiskola, Gyöngyös	2010.
IT Biztonsági nyomozás	Károly Róbert Főiskola, Gyöngyös	2010.
IT Biztonsági helyzetfelmérés, és szabályzatok kidolgozása	Pécel Önkormányzati Hivatal	2010.
IT Biztonsági tanácsadás - Kockázatelemzés	Igazságügyi Szakértői Kutató Intézetek	2010.
IT Biztonsági tanácsadás - Kockázatelemzés	ADR Logistics	2010.