Ajánlat

a Magyar Kábelkommunikációs Szövetség részére

Tárgy: Számlázási rendszerrel kapcsolatos felkészítés az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) 142. §-ban előírt követelmények szerinti tanúsításra – átdolgozott indikatív ajánlat

VERITAN Hírközlési és Informatikai Tanúsító Kft.
1043 Budapest, Lórántffy Zs. u. 15/b.
Tel/fax: + 36 1/210-5522 · info@veritan.hu · www.veritan.hu

Tartalomjegyzék

1. BEVEZETÉS 3
2. SZAKMAI AJÁNLAT A SZOLGÁLTATÓK SZÁMLÁZÁSI RENDSZERÉNEK TANÚSÍTÁSRA VALÓ FELKÉSZÍTÉSÉRE 4
2.1. A Szolgáltatók csoportba sorolása 4
2.2. A felkészítés menete 5
2.3. Előzetes felmérés elvégzése 5
2.4. Kockázatelemzés elvégzése és kockázatelemzési eljárásrend készítése 6
2.5. A tanúsításhoz szükséges dokumentumok elkészítése 7
2.5.1 Dokumentáció készítés auditált szoftver alkalmazása esetében 8
2.6. Sérülékenység vizsgálat 9
2.7. Fejlesztés módszertani tanácsadás 9
2.8. Oktatások 9
2.9. Részvétel a tanúsítóval történő egyeztetéseken 10
2.10. Eltérések javítása 10
2.11. Utógondozás 11
3. ÜZLETI AJÁNLAT 11
3.1. Üzleti ajánlat „A" mikrovállalkozási kategória esetén 11
3.2. Üzleti ajánlat „B" kisvállalkozói kategória esetén 11
3.3. Üzleti ajánlat „C" közepes vállalkozói kategória esetén 12
3.4. Határidők 12
3.5. Pénzügyi ajánlat 13
3.6. Ajánlati kedvezmények 14
4.3.1 Kedvezmény több szolgáltató egyidejű megrendelése esetén 14
4.3.2 Kedvezmény Security Operation Center (SOC) szolgáltatás igénybe vétele esetén 15
4. FELELŐSSÉG VÁLLALÁS 16
5. A SZÖVETSÉG RÉSZÉRŐL VÁRT KÖZREMŰKÖDÉS 16
6. AJÁNLATI KÖTÖTTSÉG 17

1. Bevezetés

A Magyar Kábelkommunikációs Szövetség (a továbbiakban: MKSZ) ajánlatot kért tagjai számára a VERITAN Hírközlési és Informatikai Tanúsító Kft.-től (a továbbiakban: VERITAN) számlázási rendszerrel kapcsolatos felkészítés tárgyában az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) 142. §-ban előírt követelmények szerint.

A VERITAN jelenleg IT terméktanúsításra akkreditált tanúsító cég, azonban akkreditációja nem terjed ki a hivatkozott törvényekben meghatározott tanúsítási tevékenységre. Az akkreditáció, illetve a törvényben előírt követelményeknek való felkészülés jelenleg folyamatban van, várhatóan a törvényben előírt időpontra a VERITAN minden szükséges feltétellel rendelkezni fog, hogy az előírt időponttól kezdve tanúsítványt is tudjon kiadni.

Jelen ajánlat szakmai követelményei és módszerei az alapján lettek összeállítva, hogy egy akkreditált tanúsító szervezet számára – legyen ez bármely tanúsító – a felkészített MKSZ tagok (továbbiakban: Szolgáltatók) teljes mértékben megfeleljenek a vonatkozó követelményeknek és az előírt tanúsítás sikeres lehessen.
A VERITAN az ajánlat elkésztésekor már rendelkezik felkészítési referenciával, amelyet a tanúsító szervezet szakértői is megfelelőnek ítéltek, Ez alapján cégünk rendelkezik egy olyan módszertannal, amely alkalmas bármely tanúsító cég tanúsítási követelményeinek teljesítésére.
Jelen ajánlatunk a 2015. február 22-én adott ajánlat átdolgozott változata. Az ajánlat módosítását az MKSZ 13/1/2015. számú levelében megfogalmazott szempontrendszer alapján végeztük el.
Az ajánlatban a Szolgáltatókat a havi kibocsátott számlák darabszáma szerint az MKSZ által kért csoportokba osztottuk, mivel a felkészítéssel kapcsolatos feladatok és dokumentációk a cégek mérete és a számlázási rendszereik bonyolultsága miatt az egyes csoportokban eltérnek.

Jelen ajánlatunk az MKSZ tag Szolgáltatókra érvényes indikatív ajánlat. Az MKSZ saját döntése szerint kiterjesztheti az ajánlatot a Magyar Kábeltelevíziós és Hírközlési Szövetség (MKHSZ) tagjaira is, ez esetben a VERITAN az ajánlatot az MKHSZ szövetség tagjaira is érvényesnek tekinti.

2. Szakmai ajánlat a Szolgáltatók számlázási rendszerének tanúsításra való felkészítésére

A számlázási rendszer tanúsításra való felkészítéséhez a követelményeket az alábbi jogszabályokból származtatjuk:

- 2003. évi C. törvény az elektronikus hírközlésről (a továbbiakban Eht.)
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (a továbbiakban IBTV)
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről (a továbbiakban (NFM rendelet)

A két utóbbi jogszabály alapján kerülnek besorolásra a rendszer védelmi intézkedései.
A besorolást kockázatelemzés alapján kell elvégezni, amely alátámasztja, hogy az adott védelmi szint bizonyíthatóan megfelel a számlázási rendszer zártsági követelményeinek.

A védelmi intézkedéseket első közelítésben az alábbi szinteken vizsgáljuk[1]:

Adminisztratív védelmi intézkedés:	1-es biztonsági szint szerint
Fizikai védelmi intézkedések:	2-es biztonsági szint szerint
Logikai védelmi intézkedések:	
Bizalmasság szempontjából:	3-es biztonsági osztály szerint
Sértetlenség szempontjából:	3-es biztonsági osztály szerint
Rendelkezésre állás szempontjából:	3-es biztonsági osztály szerint

Ettől eltérni abban az esetben lehetséges és szükséges, ha a kockázatelemzés kimutatja, hogy az adott komponens esetében más szintű védelmi intézkedésekre van szükség.
A védelmi szintek kockázatelemzésen alapuló meghatározása kulcstényező abból a szempontból, hogy meghatározzák a védelmi intézkedések számát, jellegét és dokumentációs szintjét, valamint a számlázási rendszer üzemeltetési körülményeivel és biztonsági funkcióival kapcsolatos elvárásait.

2.1. A Szolgáltatók csoportba sorolása

A felkészítéssel kapcsolatos feladatok szerint a Szolgáltatókat 3 csoportba soroltuk:
„A” (mikrovállalkozási kategória) – havi 2.000 kibocsátott számla alatt
„B” (kisvállalkozói kategória) – havi 2.001 – 5.000 kibocsátott számla között
„C” (közepes vállalkozói kategória) – havi 5.001-50.000 kibocsátott számla között

[1] A jelenleg a törvényi előírásoknak megfelelő tanúsító szervezet is ezeket a besorolásokat alkalmazza

A havi 50.000 fölötti számlát kibocsátó Szolgáltatók részére egyedi ajánlatot adunk.

2.2. A felkészítés menete

A felkészítés során a VERITAN a Szolgáltatók részére komplex, a sikeres tanúsításhoz szükséges valamennyi tevékenység elvégzésére adja meg szakmai ajánlatát. Az egyes szakmai felkészítési lépések opcionálisan választhatók a Szolgáltatók felkészültsége és ráfordítható erőforrásainak függvényében. A VERITAN javasolja a teljes felkészítési folyamatra a szolgáltatások igénybe vételét, ebben az esetben teljes körű garanciát vállal a sikeres tanúsításra. Természetesen lehetőség van rész-szolgáltatások igénybe vételére, ebben az esetben a VERITAN a megrendelt szolgáltatásokra a 4. pontban leírt feltételekkel vállalja a garanciát.

A felkészítés az alábbi lépésekben történik:

- Előzetes felmérés
- Kockázatelemzés
- A tanúsításhoz szükséges dokumentáció elkészítése
- Sérülékenység vizsgálat szükség esetén
- Fejlesztés módszertani tanácsadás szükség esetén
- Oktatások
- Részvétel a tanúsítóval történő egyeztetéseken
- Eltérések javítása
- Utógondozás (opcionális)

2.3. Előzetes felmérés elvégzése

Az előzetes felmérés célja a számlázási rendszer üzemeltetési körülményeinek áttekintése, valamint a tanúsításhoz szükséges dokumentációk meglétének felmérése. A felmérés során ismertetésre kerül az a módszertan, amely alapján a VERITAN a felkészítést végzi, így a Szolgáltatók felkészülésben, majd később a tanúsítási folyamatban részt vevő munkatársai megismerik a követelményeket, azok teljesítésének lehetőségeit és a tanúsítók által kért bizonyítékok (dokumentumok) rendszerét. A felmérés módszere kérdőíves, szükség esetén kiegészül helyszíni szemlével.
Kiemelten fontosnak tartjuk, hogy a felmérés egyértelműen tisztázza a számlázási rendszer határait, mert a későbbi folyamatlépések erre fognak kiterjedni, illetve amennyiben a tanúsító ezen túlmenően is követelményeket támaszt vagy vizsgálatokat kíván végezni, akkor ezeket el lehessen hárítani, kerülni.

A felmérés részben kérdőíves, részben az üzemeltetési helyszín bejárását jelenti.

A felmérésről jegyzőkönyv készül, amely előzetesen tartalmazza az elvégzendő feladatokat, a meglévő dokumentumok listáját és az elkészítendő dokumentumok listáját is.

Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), a rendszer architektúráját ismerő vagy tervező szakértő, rendszergazda, kulcsfelhasználó (ha van ilyen), normál felhasználó
A felmérés eredményei: jegyzőkönyv, teendő lista, meglevő dokumentumok listája, elkészítendő dokumentumok listája

2.4. Kockázatelemzés elvégzése és kockázatelemzési eljárásrend készítése

A kockázatelemzés kiterjed a rendszer környezetére, minden olyan elemére (rendszerelem, hardver, szoftver, szervezet) amely a számlázásban részt vesz, és amely az informatikai biztonsági védelem megszervezésben releváns. A kockázatelemzés kitér a rendszer dokumentáltságára is.
A kockázatelemzést egyrészt a NFM rendelet mellékletében leírt tartalmi követelmények figyelembe vételével végezzük el, másrészt felhasználjuk az ISO 27001 szabványban megfogalmazott módszertani leírásokat.
A kockázatelemzésről részletes dokumentáció készül, feltüntetve a számlázási rendszerrel kapcsolatos releváns kockázatokat, azok bekövetkezési valószínűségét, valamint hatását a rendszerre. Ugyancsak felsorolásra kerülnek a rendszerrel kapcsolatba hozható olyan kockázatok is, amelyek a vizsgálatok alapján nem relevánsnak minősíthetők, a minősítés indoklásával együtt.
A hivatkozott NFM rendelet szerint az adott szervezetnek a kockázatelemzésre támaszkodva kell besorolni az informatikai rendszereit - jelen esetben a számlázási rendszert – és ez alapján kell a védelmi intézkedéseket meghozni és dokumentálni.

Szintén a kockázatelemzéshez kapcsolódóan elkészül egy kockázatelemzési eljárásrend, amely tartalmazza, hogy a kockázatelemzést milyen elvek alapján kell elvégezni, mi az érvényesség területe, milyen rendszerességgel kell végezni, illetve melyek azok az esetek, amelyek a kockázatelemzés teljes vagy részleges ismétlődését vonják maguk után.

Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), a rendszer architektúráját ismerő vagy tervező szakértő, rendszergazda, kulcsfelhasználó (ha van ilyen), biztonsági felelős (ha nem az IT biztonsági felelős látja el ezt a szerepkört)
A kockázatelemzés eredményei: Kockázatelemzési dokumentum, Kockázatelemzési eljárásrend

Megjegyzés: Az „A” csoportba besorolt szolgáltatók esetében a kockázatelemzés – lehetőség szerint - a helyszíni felméréssel egy időben készül el.

2.5. A tanúsításhoz szükséges dokumentumok elkészítése

Mind az IT biztonsági szabványok, mind pedig az NFM rendelet előírja, hogy az adott szervezetnek az azonosított és hatályos védelmi intézkedésekkel kapcsolatosan milyen szabályzatokkal, illetve milyen dokumentációkkal kell rendelkeznie.

Az NFM rendelet a szabályzatok tartalmi előírásait tartalmazza, illetve a dokumentáció egy lehetséges struktúráját. Az adminisztratív védelmi intézkedések 1-es, a fizikai védelmi intézkedések 2-es és a logikai védelmi intézkedések vagy 3-as szintjén az alábbi szabályzatok, dokumentációk megléte várható el:

- IT biztonságpolitika
- IT biztonsági szabályzat
- kockázatkezelési eljárásrend
- aktuális kockázatelemzés
- a számlázási rendszerre vonatkozó nyilvántartások
- fizikai biztonsági szabályzat
- képzési eljárásrend
- konfigurációkezelési eljárás
- üzletmenet folytonossági eljárás (beleértve a karbantartásra vonatkozó eljárást)
- hozzáférési szabályzat (beleértve azonosítás és hitelesítés)
- információbiztonsági szabályzat (beleértve az adathordozók védelmét is)
- naplózási és logelemzési eljárásrend
- eseménykezelési eljárásrend

Ezekben a dokumentációkban és eljárásokban kerülnek leírásra azok a szabályok, amelyek az NFM rendelet 1-es és 2-es és 3-as szintjein meghatározott védelmi intézkedéseket tartalmazzák. Kiemelkedő jelentőségű az IT biztonsági szabályzat, amely a rendszer összes elemét tartalmazza, irányelv szinten, és ezek részletes kibontását tartalmazza többi szabályzat vagy eljárásrend.
A dokumentum struktúra végleges meghatározása a kockázatelemzési fázis után történik meg, ekkor határozható meg, hogy mely dokumentumok önállóak, és melyek képezik egy másik dokumentum mellékletét vagy függelékét.
A dokumentáció összeállításakor azokon a területeken, ahol értelmezhető, irányadónak tekintjük az ITIL szabvány ajánlásait.

Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), a rendszer architektúráját ismerő vagy tervező szakértő, rendszergazda, kulcsfelhasználó (ha van ilyen), biztonsági felelős (ha nem az IT biztonsági felelős látja el ezt a szerepkört)
A fázis eredményei: a tanúsításhoz szükséges teljes dokumentáció

Az „A" kategóriába besorolt szolgáltatók esetében a szükséges dokumentációk nagyrészt a felmérés és kockázatelemzés fázisában mintadokumentumok testreszabásával elkészülhetnek. A „B" kategória esetében nagyrészt mintadokumentumok alapján elkészülhet a dokumentáció egy része, azonban szükséges lehet egyedi, a Szolgáltató sajátosságainak megfelelő dokumentumok elkészítésére is. A VERITAN a felkészítés során alapvetően nem mintadokumentumokat ad át a Szolgáltatónak, hanem a mintadokumentumok alapján a felkészítés keretében elkészíti a Szolgáltatóra testreszabott dokumentációt.

Nagyobb szolgáltatók esetében („C" kategóriába sorolt Szolgáltatók) egyedi dokumentáció elkészítését látjuk indokoltnak.

Opcionálisan lehetőség van arra, hogy a Szolgáltatók saját maguk készítsék el a szükséges dokumentumokat, és azok ellenőrzésével bízzák meg a VERITAN-t. A dokumentumok átvizsgálása a formai és tartalmi ellenőrzésre terjed ki, valamint módosítási javaslatok megtételére. A VERITAN ezt az opciót óradíjas konstrukcióban ajánlja, ahol egy óra 6 oldalnyi dokumentum (11-12 pontos betűnagyság, 1.15 sortávolság) átvizsgálását jelenti.

2.5.1 Dokumentáció készítés auditált szoftver alkalmazása esetében

Abban az esetben, ha a Szolgáltató olyan szoftvert használ, amely az Eht. 142. § szerinti akkreditált tanúsító szervezet tanúsítványával rendelkezik, egyszerűsített dokumentációs rendszer elkészítését javasoljuk.
A követelményeket kielégítő dokumentáció ebben az esetben az alábbi dokumentumokkal lefedhető:

- IT biztonságpolitika
- IT biztonsági szabályzat
- kockázatkezelési eljárásrend
- aktuális kockázatelemzés
- képzési eljárásrend
- a tanúsított számlázási rendszerre vonatkozó üzemeltetési szabályzat
- Az üzemeltetési szabályzat a Szolgáltató és a tanúsított számlázási rendszer szállítója által egyeztetett megállapodáson alapuló dokumentum, amely tartalmazza a Szolgáltató és a tanúsított rendszer szállítója közötti feladatmegosztást és felelősségeket a jogszabályi megfelelés tekintetében. Az üzemeltetési szabályzat tartalmilag minimálisan az alábbi szempontokra kell, hogy kiterjedjen:

- incidenskezelés
- változáskezelés
- jogosultság kezelés
- kiadáskezelés
- számlázási rendszer szolgáltatás folytonosság biztosítása
- kommunikáció a felek között

Az így kialakított dokumentációs rendszer abban az esetben is alkalmazható, ha a Szolgáltató a számlázási szoftvert bérli, ASP (Application Service Providing) vagy SaaS (Software as a Service) alapon.

2.6. Sérülékenység vizsgálat

Sérülékenység vizsgálat alatt a számlázási rendszer külső illetéktelen behatolás elleni védettségét értjük. Az NFM rendelet a logikai védelem 2-es szintjén még nem ír elő sérülékenység vizsgálatot, 3-as szinten már ajánlott, ennél fentebbi szinteken ezek elvégzése szükséges.
Abban az esetben, ha a számlázási rendszer szállítója korábban nem végzett sérülékenység vizsgálatot, alapszintű vizsgálat elvégzését a 2-es védelmi szinten is indokoltnak tartjuk.
Az alapszintű sérülékenység vizsgálat alatt a szoftver külső kapcsolódásainak, portjainak ellenőrzését értjük vizsgáló szoftverrel, a szoftver által készített jegyzőkönyv kiértékelésével, az esetleges hiányosságok elhárítására hozott intézkedések meghatározásával.

Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), rendszergazda
A vizsgálat eredményei: jegyzőkönyv, intézkedési terv, hibaelhárítási jegyzőkönyvek

2.7. Fejlesztés módszertani tanácsadás

Az Eht. 142.§ (9) pontja egyedi fejlesztésű szoftverek esetében forráskód szintű elemzést ír elő. A VERITAN a fejlesztés módszertani tanácsadás keretében felkészíti a Szolgáltató fejlesztőit arra, hogy a tanúsító forráskód szintű elemzéséhez a szoftver megfelelő legyen. Ehhez megismerteti azokat a dokumentációs kötelezettségeket és módszereket, amelyeket a fejlesztés során be kell tartani, illetve bemutatja azokat a nem támogatott fejlesztési lépéseket, amelyek egy számlázó rendszer forráskód elemzése során kockázatot jelentenek.

2.8. Oktatások

Az IT biztonsági elvárások egyik legfontosabb követelménye a tudatosság és képzés. A felkészítés során az egyes célcsoportoknak alapképzéseket tartunk a felépített IT biztonsági

védelmi intézkedések, a hozzákapcsolódó dokumentumok, szabályzatok, teendők megismerésére. Az oktatás az alábbi célcsoportokra terjed ki:

- IT biztonsági felelős
- üzemeltetők
- kulcsfelhasználók, felhasználók

Ebben a fázisban oktatási anyagok készülnek, melyek felhasználhatók a későbbiekben a személyzet változásakor, új belépők képzésekor, valamint az ismétlő oktatásoknál.

Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), rendszergazda, felhasználók
Az oktatások eredményei: oktatási jegyzőkönyvek, oktatási anyagok

2.9. Részvétel a tanúsítóval történő egyeztetéseken

A VERITAN a feladatok ütemezése során alkalmazkodik a kiválasztott tanúsító ütemtervéhez. Ennek érdekében szakértőink részt vesznek a tanúsítóval történő egyeztetéseken, annak érdekében, hogy a szükséges tevékenységek és elkészítendő dokumentumok a tanúsítás megfelelő fázisában rendelkezésre tudjanak állni. Ilyen irányú igény esetén a VERITAN szakértői a Szolgáltatók szakértőivel együtt ellátják a cég szakmai képviseletét a tanúsítóval történő megbeszéléseken vagy a tanúsító helyszíni szemléin.

Az ajánlat órakerete az előfizetői szám függvényében:
„A" besorolású Szolgáltatók esetében 1 alkalom, az alapajánlat tartalmazza
„B" és „C" besorolású Szolgáltatók esetében, megrendelés szerint, a tanúsítóval egyidőben„B" besorolású szolgáltatónál 20 óra, „C" besorolású szolgáltatónál 30 óra
Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), vagy által kijelölt személy
Az egyeztetések eredményei: emlékeztetők, jegyzőkönyvek

2.10. Eltérések javítása

A VERITAN a tanúsító által tett észrevételek alapján javítja az elkészített dokumentumokat, illetve elvégzi azokat a tevékenységeket, amelyeket a tanúsító még szükségesnek tart a számlázási rendszer megfelelőségének igazolására.
A javítások határideje: a tanúsító által meghatározott határidő
Szükséges szolgáltatói szakértői részvétel: IT biztonsági felelős (vagy ezzel a feladattal a projekt idejére megbízott személy), rendszergazda, felhasználó
Az egyeztetések eredményei: javított dokumentumok, jegyzőkönyvek

2.11. Utógondozás

A VERITAN a sikeres tanúsítás után vállalja a teljes rendszer dokumentáció nyomon követését, frissítését napra készen tartását. Az utógondozásba az alábbiakat értjük:

- Szervezeti, személyi változások átvezetése a dokumentációkban
- Rendszerelemek változásainak átvezetése a dokumentációkban
- Jogszabály, vagy szabvány változások átvezetése a dokumentációkban
- Oktatások, képzések, új belépők képzése távoktatás keretében
- Tanúsítói felülvizsgálatok előtti frissítő felkészítések
- Kockázatelemzések a Kockázatelemzési eljárásrendnek megfelelően

3. Üzleti ajánlat

Jelen ajánlatunk két részből tevődik össze:

- Az alapajánlat a Szolgáltatóknál való felmérést, és kockázatelemzés elvégzését tartalmazza.
- Ajánlati opciók, amelyeket a Szolgáltatók a továbbiakban részletezettek alapján választhatnak a felkészítéshez, saját felkészültségük és rendelkezésre álló belső erőforrásaik alapján

3.1. Üzleti ajánlat „A" mikrovállalkozási kategória esetén

Az ajánlat szakmai tartalma:

- Alapajánlat: Felmérés, kockázatelemzés, helyszíni ellenőrzések[2],oktatások
- Választható opcionális ajánlatok:
  - A Szolgáltatók által készített dokumentumok ellenőrzése
  - Fejlesztés módszertani tanácsadás
  - Részvétel a tanúsítóval történő egyeztetéseken, eltérések javítása
  - Utógondozás

3.2. Üzleti ajánlat „B" kisvállalkozói kategória esetén

Az ajánlat szakmai tartalma:

- Alapajánlat: Felmérés, kockázatelemzés, helyszíni ellenőrzések[3],oktatások

- [2] „A" besorolású Szolgáltatók esetében az alapajánlat minta dokumentumok alapján a dokumentációk Szolgáltatókra való testreszabását is tartalmazhatja. A fázis tartalmazza a számlázással kapcsolatos helyszínek bejárását, azok elsődleges IT biztonsági ellenőrzését és a teendők dokumentálását.

- Választható opcionális ajánlatok:
  - Dokumentáció készítése
  - Dokumentumok készítése auditált számlázási rendszer esetén
  - A Szolgáltatók által készített dokumentumok ellenőrzése
  - Sérülékenység vizsgálat
  - Fejlesztés módszertani tanácsadás
  - Részvétel a tanúsítóval történő egyeztetéseken, eltérések javítása
  - Utógondozás

3.3. Üzleti ajánlat „C" közepes vállalkozói kategória esetén

Az ajánlat szakmai tartalma:

- Alapajánlat: Felmérés, kockázatelemzés, helyszíni ellenőrzések, oktatások
- Választható opcionális ajánlatok:
  - Dokumentáció készítése
  - Dokumentumok készítése auditált számlázási rendszer esetén
  - A Szolgáltatók által készített dokumentumok ellenőrzése
  - Sérülékenység vizsgálat
  - Fejlesztés módszertani tanácsadás
  - Részvétel a tanúsítóval történő egyeztetéseken, eltérések javítása
  - Utógondozás

3.4. Határidők

A táblázatban szereplő határidők irányadóak a felkészítés elvégzésére. A tényleges határidők a felmérés és kockázatelemzési szakasz után határozhatók meg pontosan.

Határidők az „A" besorolású Szolgáltatók esetében

Projekt fázis	Határidő
Projektindítás	T0
Felmérés, kockázatelemzés, oktatás	T0+ 5 nap
A felmérés, illetve a helyszíni bejárás alatt esetlegesen el nem készült dokumentumok elkészítése	T0 + 30 nap
Sérülékenység vizsgálat szükség esetén	5 nap a dokumentáció készítés időszakában
Eltérések javítása	a tanúsító által megszabott határidő

- [3] „B" besorolású Szolgáltatók esetében az alapajánlat minta dokumentumok alapján a dokumentációk Szolgáltatókra való testreszabását is tartalmazhatja. A fázis tartalmazza a számlázással kapcsolatos helyszínek bejárását, azok elsődleges IT biztonsági ellenőrzését és a teendők dokumentálását.

Határidők a „B” és „C” besorolású Szolgáltatók esetében:

Projekt fázis	Határidő
Projektindítás	T0
Felmérés,	T0+ 5 nap
Kockázatelemzés	T0 + 10 nap
Dokumentáció elkészítés	T0 + 40 nap
Sérülékenység vizsgálat szükség esetén	a dokumentáció készítés időszakában
Fejlesztés módszertani tanácsadás	a dokumentáció készítés időszakában
Oktatások	T0 + 50 nap
Eltérések javítása	a tanúsító által megszabott határidő

3.5. Pénzügyi ajánlat

Az egyes kategóriákra vonatkozó pénzügyi ajánlatot az alábbi táblázat tartalmazza:

Tevékenység	Vállalási ár „A„ besorolású szolgáltatók	Vállalási ár ”B” besorolású szolgáltatók	Vállalási ár ”C” besorolású szolgáltatók
Alapajánlat			
Felmérés, kockázatelemzés, helyszíni ellenőrzések, oktatások	390.000 Ft	690.000 Ft	990.000 Ft
További ajánlati opciók			
Dokumentumok elkészítése	-	1.380.000 Ft	2.490.000 Ft
Dokumentumok készítése auditált számlázási rendszer esetén	Az alapajánlat tartalmazza		
A Szolgáltatók által késztett dokumentumok ellenőrzése	12.000 Ft/óra[4]	12.000 Ft/óra[5]	12.000 Ft/óra[6]
Sérülékenység vizsgálata (szükség esetén)	-	490.000 Ft	490.000 Ft
Fejlesztés módszertani tanácsadás (szükség esetén)	-	240.000 Ft	240.000 Ft
Részvétel a tanúsítóval történő egyeztetéseken, eltérések javítása[7]	Az alapajánlat 1 alkalmat tartalmaz	250.000 Ft	350.000 Ft
Utógondozás	120.000 Ft/év	500.000 Ft/év	750.000 Ft/év

A táblázatban szereplő árak nettó árak, az ÁFÁ-t nem tartalmazzák.

[4] 1 óra 6 oldal dokumentum átvizsgálást jelent
[5] 1 óra 6 oldal dokumentum átvizsgálást jelent
[6] 1 óra 6 oldal dokumentum átvizsgálást jelent
[7] Az eltérések javítását a VERITAN abban a esetben végzi, amennyiben a dokumentumok elkészítésével a Szolgáltató megbízta

A fenti táblázatból kiválasztott portfóliónak megfelelően a Felek megállapodnak a szolgáltatások díjáról. A VERITAN az egyes tevékenységek teljesítése után rész-számla benyújtására jogosult a szerződés szerinti teljes szolgáltatási díj 60 %-a mértékéig. A szolgáltatási díj fennmaradó részének kifizetése a sikeres audit után esedékes.

A fizetési határidő a számla kibocsátást követő 15 nap.

3.6. Ajánlati kedvezmények

A VERITAN Kft. több szolgáltató egyidejű megrendelése esetén, illetve az általunk nyújtott IT Biztonsági felelős (SOC) szolgáltatások igénybevétele esetén a felkészítésből jelentős kedvezményeket ad. A lenti pontokban szereplő kedvezmények nem vonhatók össze.

4.3.1 Kedvezmény több szolgáltató egyidejű megrendelése esetén

A VERITAN Kft. több azonos kategóriába tartozó szolgáltató egyidejű megrendelése esetén az alábbi kedvezményeket nyújtja:

„A" besorolású Szolgáltatók kedvezménye
A kedvezmény nyújtás feltétele, hogy a Szolgáltatók földrajzilag az ország egy régiójában legyenek, ahol az egymástól való átlagos földrajzi távolsága 40 km-nél nem nagyobb. Előnyt jelent, ha ugyanazt, vagy hasonló számlázási rendszert használnak, ebben az esetben a lenti táblázatban megadott kedvezmény növekedhet.

Szolgáltatók száma	Kedvezmény
2	10 %
3-7	25 %
7 fölött	45 %

„B" és „C" besorolású szolgáltatók esetében
A kedvezmény nyújtás feltétele, hogy a Szolgáltatók földrajzilag az ország egy olyan területén legyenek, ahol az egymástól való átlagos földrajzi távolsága 50 km-nél nem nagyobb. Amennyiben az együttesen megrendelő szolgáltatók száma meghaladja az 5-öt, a földrajzi távolság nem releváns a kedvezmény megadásakor. További feltétel, hogy a szolgáltatók ugyanazt a számlázási rendszert használják.
A kedvezmény megadásához különböző besorolásba tartozó Szolgáltatók is megrendelhetik a felkészítést egyidőben.

Szolgáltatók száma	Kedvezmény
2	25 %
3-7	30 %
7 fölött	45 %

4.3.2 Kedvezmény Security Operation Center (SOC) szolgáltatás igénybe vétele esetén

Az IBTV előírja, hogy a Szolgáltatóknak rendelkezni kell kinevezett IT Biztonsági felelőssel. Az IT Biztonsági felelős feladatait az IBTV 13.§ tartalmazza.
A VERITAN Kft. új szolgáltatása (Security Operation Center (SOC)) keretében az ügyfelei számára IT Biztonsági felelőst biztosít, aki megfelel a törvényben előírt feltételeknek, és nevesítetten az igénybe vevő Szolgáltató rendelkezésére áll. A szolgáltatás informatikailag támogatott, a 3. számú melléklet tartalmazza a szolgáltatás leírását.
A szolgáltatás igénybe vétele esetén a felkészítési árakból kedvezményeket biztosítunk. A szolgáltatás igénybevétele esetében nincs szükség utógondozásra, hiszen az az IT Biztonsági felelős szolgáltatás feladata.
Jelen ajánlatunkban szereplő árak „B" és „C" típusú Szolgáltatók esetében kizárólag a számlázási rendszerre és környezetével kapcsolatos feladatok ellátására vonatkoznak, azonban ilyen irányú igény esetében kiterjeszthető a szolgáltató valamennyi IT rendszerére.

A szolgáltatáshoz kapcsolódó kedvezmény igénybevételének feltétele, hogy a szerződő szolgáltató a kedvezményes felkészítés igénybe vételekor szerződést köt a VERITAN-nal az SOC szolgáltatás igénybevételére is. Az SOC szolgáltatás a sikeres tanúsítás után kezdődik. A szolgáltatás igénybevételét a tanúsítvány érvényességének időszakára javasoljuk.

A szolgáltatást a VERITAN havidíjas konstrukcióban nyújtja.

A szolgáltatás tervezett irányárait az alábbi táblázat tartalmazza.

	Szolgáltatási díj Ft/hó	**Kedvezmény a felkészítésből**
„A" besorolású szolgáltató	25.000-30.000	50 %
„B" besorolású szolgáltató	45.000-55.000	35 %
„C" besorolású szolgáltató	60.000-75.000	35 %

A táblázatban szereplő árak nettó árak, az ÁFÁ-t nem tartalmazzák.

A szolgáltatást olyan Szolgáltatók is igénybe vehetik, ahol nem a VERITAN végezte a felkészítést. Ebben az esetben a rendszer bonyolultsága, és dokumentáltsága figyelembe vételével egyszeri felmérési díj kerül a havi díjon kívül felszámításra. A szolgáltatás ebben az esetben is a sikeres tanúsítás után indul.

A szolgáltatás opcionálisan a mentett számlázási állományok tárolását is tartalmazhatja. Ez történhet fizikai adathordozó tárolásával vagy titkosított formában a Szolgáltató részére biztosított tárterületen való biztonságos tárolással.
A VERITAN ezt a szolgáltatást az igénybe vevők számára külön egyedi árazás alapján nyújtja.

4. Felelősség vállalás

A VERITAN a felkészítés során végzett saját tevékenységére teljes körű garanciát vállal az alábbiak szerint:

- amennyiben a tanúsítás bizonyíthatóan a VERITAN tevékenységére visszavezethető okok miatt sikertelen, a felkészítés díjtalan, ha az elkészített vagy átadott dokumentumok részben sem alkalmasak felhasználásra. Felhasználható dokumentumok esetében csak az igazolt költségek kerülnek felszámításra.
- a VERITAN által elkészített dokumentációban az auditor által elvárt módosítások átvezetése díjmentes abban az esetben, ha a VERITAN részt vesz a tanúsítóval történő egyeztetéseken, vagy a módosítási kérések a tanúsító által átadott jegyzőkönyv alapján merül fel igényként.
- nem dokumentum alapú felkészítés esetén – pl, vírusvédelem, tűzfal beállítás stb. – az auditor által feltárt jogos hiányosságok megszüntetése díjmentes.
- a felkészítési díjak kifizetése részben sikerdíjas, azaz a felkészítési díjak 40 %-a a sikeres tanúsítás után esedékes.

A VERITAN kizárja a felelősségét az alábbi esetekben:

- amennyiben a dokumentációt nem a VERITAN készíti vagy nem véleményezi
- amennyiben a Szolgáltató által készített dokumentumokat a VERITAN véleményezi, de az észrevételek a dokumentációban nem, vagy nem úgy kerültek átvezetésre, ahogy a véleményezés szólt, és a tanúsító erre hivatkozva kér újabb módosítást vagy sikertelen a tanúsítás
- amennyiben a VERITAN által korábban, más Szolgáltatónál készített dokumentáció felhasználásával a Szolgáltató maga készítette el a dokumentációt, a VERITAN a tanúsítás sikerességére semmilyen garanciát nem vállal

5. A szövetség részéről várt közreműködés

A VERITAN a szövetség részéről az alábbi területeken vár el segítő/szervező segítséget:

- az ajánlat megfelelőnek minősítése esetén - ha erre igény van - a Szolgáltatók meggyőzéséről a szolgáltatások minél korábbi igénybevételéről, a határidő nyomás csökkentése érdekében,igény esetén a Szolgáltatók - főleg az „A” kategóriájú mikrovállalkozók - minél nagyobb csoportos szolgáltatás igénybe vételében való szervezési tevékenység,
- sikeres felkészítések, illetve a felkészítés alapján sikeres auditok kommunikálása,
- amennyiben a VERITAN által korábban, más Szolgáltatónál készített dokumentáció felhasználásával a Szolgáltató magal készíti el a dokumentációt, és a tanúsítás sikertelen vagy nagyon sok utómunkálatot igényel, annak kommunikálása, hogy a felkészítés nem a VERITAN közreműködésével történt,
- S.O.C szolgáltatás beindítása esetében módszertani konzultációk a szolgáltatás minél jobb bevezetése és testreszabása érdekében,
- a sikeres audit esetén az esetleges fizetési csúszások elhárításában segítségnyújtás.

6. Ajánlati kötöttség

A VERITAN jelen ajánlatát annak megküldését követően számított 40 napig változatlan formában fenntartja. Amennyiben ezen határidőn túl történik meg a megbízásról szóló döntés, a Felek a határidők szempontjából az ajánlatot újra tárgyalják.

A VERITAN jelen ajánlata alapján nem köteles elindítani az SOC szolgáltatást.

Jelen ajánlatunk indikatív ajánlat, amelynek árai és határidői a ténylegesen elvégzendő feladatok szerint változhatnak.
A megrendelt szolgáltatások tekintetében a VERITAN és a Szolgáltatók szerződést kötnek, amelyben pontosan meghatározzák a leszállítandó termék dokumentumokat, az elvégzendő tevékenységeket, valamint határidőket és fizetési feltételeket.

Budapest, 2015. március 17.

Gyursánszky János
ügyvezető igazgató

1. Melléklet: Követelmények számlázási rendszerek IT biztonsági tanúsításához

Adminisztratív védelmi intézkedések

Az 1-es biztonsági szinten elvárt adminisztratív védelmi intézkedések a következők:

- Informatikai biztonságpolitika (3.1.1.1)[8]
- Informatikai biztonsági stratégia (3.1.1.2)
- Informatikai biztonsági szabályzat (3.1.1.3)
- Biztonsági felelős (3.1.1.4)
- Az elektronikus információs rendszerek nyilvántartása (3.1.1.7)
- Információbiztonsággal kapcsolatos engedélyezési eljárás (3.1.1.11)
- Kockázatelemzési eljárásrend (3.1.2.1)
- Kockázatelemzés (3.1.2.3)
- Eljárás a jogviszony megszűnésekor (3.1.6.5)
- Fegyelmi intézkedések (3.1.6.8)
- Képzési eljárásrend (3.1.7.1)
- Biztonság tudatosság képzés (3.1.7.2)

Fizikai, védelmi intézkedések

A 2-es biztonsági szinten elvárt fizikai védelmi intézkedések a következők:

- Fizikai védelmi eljárásrend (3.2.1.2)
- Fizikai belépési engedélyek (3.2.1.3)
- Fizikai belépés ellenőrzése (3.2.1.4)

Logikai védelmi intézkedések

A 3-as biztonsági osztályban elvárt logikai védelmi intézkedések a következők:

Konfigurációkezelés

- Konfigurációkezelési eljárásrend (3.3.1.1)
- Alapkonfiguráció (3.3.1.2)
- A konfigurációváltozások felügyelete (változáskezelés) (3.3.1.3)
- Előzetes tesztelés és megerősítés (3.3.1.3.2)
- Biztonsági hatásvizsgálat (3.3.1.4)
- Konfigurációs beállítások (3.3.1.6)
- Legszűkebb funkcionalitás (3.3.1.7)
- Elektronikus információs rendszerelem leltár (3.3.1.8)
- A szoftverhasználat korlátozásai (3.3.1.10)
- A felhasználó által telepített szoftverek (3.3.1.11)

[8] Zárójelben a 77/2013. (XII.19.) NFM rendelet megfelelő pontjára való hivatkozás

Üzletmenet folytonosság

- Üzletmenet folytonosságra vonatkozó eljárásrend (3.3.2.1)
- Üzletmenet folytonossági terv informatikai erőforrás (3.3.2.2)
- A folyamatos működésre felkészítő képzés (3.3.2.3)
- Az elektronikus információs rendszer mentései (3.3.2.8)
- Az elektronikus információs rendszer helyreállítása és újraindítása (3.3.2.9)

Karbantartás

- Rendszer karbantartási eljárásrend (3.3.3.1)
- Rendszeres karbantartás (3.3.3.2)

Adathordozók védelme

- Adathordozók védelmére vonatkozó eljárásrend (3.3.4.1)
- Hozzáférés az adathordozókhoz (3.3.4.2)
- Adathordozók törlése (3.3.4.6)
- Adathordozók használata (3.3.4.7)

Azonosítási és hitelesítés

- Azonosítási és hitelesítési eljárásrend (3.3.5.1)
- Azonosítási és hitelesítés (belső felhasználók) (3.3.5.2)
- Hálózati hozzáférés privilegizált fiókokhoz (3.3.5.2.2)
- Azonosító kezelés (3.3.5.4)
- A hitelesítésre szolgáló eszközök kezelése (3.3.5.5)
- A hitelesítésre szolgáló eszköz visszacsatolása (3.3.5.6)
- Hitelesítés kriptográfiai modul esetén (3.3.5.7)
- Azonosítás és hitelesítés (szervezeten kívüli felhasználók) (3.3.5.8)
- Hitelesítés szolgáltatók tanúsítványának elfogadása (3.3.5.8.2)

Hozzáférés ellenőrzés

- Hozzáférés ellenőrzési eljárásrend (3.3.6.1)
- Felhasználói fiókok kezelése (3.3.6.2)
- Hozzáférés ellenőrzés érvényesítése (3.3.6.3)
- Sikertelen bejelentkezési kísérletek (3.3.6.7)
- A rendszerhasználat jelzése (3.3.6.8)
- Azonosítás/hitelesítés nélkül engedélyezett tevékenységek (3.3.6.12)
- Távoli hozzáférés (3.3.6.13)
- Vezeték nélküli hozzáférés (3.3.6.14)
- Mobil eszközök hozzáférés ellenőrzése (3.3.6.15)
- Külső elektronikus információs rendszerek használata (3.3.6.16)
- Nyilvánosan elérhető tartalom (3.3.6.18)

Rendszer- és információsértetlenségi

- Rendszer- és információsértetlenségi eljárásrend (3.3.7.2)
- Hibajavítás (3.3.7.3)

- Kártékony kódok elleni védelem (3.3.7.4)
- Az elektronikus információs rendszer felügyelete (3.3.7.5)
- Biztonsági riasztások és tájékoztatások (3.3.7.6)
- A kimeneti információ kezelése és megőrzése (3.3.7.12)

Naplózás

- Naplózási eljárásrend (3.3.8.1)
- Naplózható események (3.3.8.2)
- Naplóbejegyzések tartalma (3.3.8.3)
- Napló tárkapacitás (3.3.8.4)
- Naplózási hiba kezelése (3.3.8.5)
- Naplóvizsgálat és jelentéskészítés (3.3.8.6)
- Időbélyegek (3.3.8.8)
- A naplóinformációk védelme (3.3.8.9)
- A naplóbejegyzések megőrzése (3.3.8.11)
- Naplógenerálás (3.3.8.12)

Rendszer- és kommunikációvédelem

- Rendszer- és kommunikációvédelmi eljárásrend (3.3.9.1)
- Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem (3.3.9.5)
- A határok védelme (3.3.9.6)
- Kriptográfiai kulcs előállítása és kezelése (3.3.9.10)
- Kriptográfiai védelem (3.3.9.11)
- Együttműködésen alapuló számítástechnikai eszközök (3.3.9.12)
- Biztonságos név/cím feloldó szolgáltatások (hiteles forrás) (3.3.9.16)
- Biztonságos név/cím feloldó szolgáltatás (gyorsító táras) (3.3.9.17)
- Architektúra és tartalékok név/cím feloldási szolgáltatás esetén (3.3.9.18)
- A folyamatok elkülönítése (3.3.9.22)

Biztonsági események kezelése

- Biztonsági eseménykezelési eljárásrend (3.3.10.1)
- Képzés a biztonsági események kezelésére (3.3.10.2)
- A biztonsági események kezelése (3.3.10.4)
- A biztonsági események figyelése (3.3.10.5)
- A biztonsági események jelentése (3.3.10.6)
- Segítségnyújtás a biztonsági események kezeléséhez (3.3.10.7)
- Biztonsági eseménykezelési terv (3.3.10.8)

2. Melléklet: IT biztonsági felelős feladatai az IBTV (2013. évi L. tv.) szerint

13. § (1) Az elektronikus információs rendszer **biztonságáért felelős személy feladata** ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az *a)* pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,

d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,

e) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,

f) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

(3) Az elektronikus információs rendszer biztonságáért felelős személy e törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

(4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

(5) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az e törvényben meghatározott követelmények teljesülését

a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők

e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

(6) Az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége az (5) bekezdés szerinti esetekben más személyre nem átruházható.

(7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult az (5) bekezdés szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban 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.

(8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.

(9) A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

(10) Nem kell a (8) bekezdés szerinti képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel vagy e szakterületen szerzett 5 év szakmai gyakorlattal.

(11) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

3. Melléklet: A Security Operation Center (SOC) szolgáltatás összetevői

A megajánlott havidíjas szolgáltatás tervezett tartalma

Dokumentumok karbantartása és frissítése	Dokumentum lista a 2.5 fejezetben (technológiai / jogszabályi változások alapján)
IT biztonsági felelős szerepkör ellátása	Információbiztonsági törvény (2013. évi L. tv.) előírásaival összhangban.
Sérülékenység vizsgálat	Havi rendszerességgel
Egységes, web alapú informatikai rendszer biztosítása a kötelezően előírt nyilvántartások vezetéséhez	**A rendszer az alábbi nyilvántartások vezetését teszi lehetővé:** Elektronikus információs rendszerek IT biztonsággal kapcsolatos engedélyezések Fegyelmi intézkedések Képzések elvégzése Kockázatelemzések Biztonsági hatásvizsgálatok Alapkonfiguráció és változások Elvégzett konfigurációs változtatások Információs rendszerelem leltár Karbantartások (rendszeres / eseti) Karbantartók Hibajavítások Biztonsági események
Biztonsági riasztások és tájékoztatások kiadása	Elektronikus formátumban

Egyedi IT biztonsági szolgáltatás opciók

Fizikai védelmi intézkedésekhez kapcsolódó tanácsadás, beszerzés, üzembeállítás

IT biztonságot érintő hatásvizsgálatok elvégzése

Központi naplózó infrastruktúra

Naplóelemzés és riasztás generálás

Hálózati határvédelmi eszköz biztosítása és üzemeltetése

Behatolás detektálás/megelőzés

Adatszivárgás elleni védelem

Biztonsági események figyelése és jelentése

Segítségnyújtás biztonsági események kezeléséhez

IT biztonság tudatosság képzés (helyszíni, csoportos)