Hunguard Kft. Tanúsítási Divízió
1123 Budapest, Kékgolyó u. 6. 5. em. 4.
Honlap: http://www.hunguard.hu
Telefon: (+36) 1 225-87-96
Telefax: (+36) 1 225-87-97
E-mail: iroda@hunguard.hu

ELEKTRONIKUS BESZÁMOLÓ RENDSZER v_2013.04.16

TANÚSÍTÁSI JELENTÉS

HUNG-TJ-MIBÉTS-07-2013

Fájlnév: HUNG-TJ-MIBETS-07-20130430
Verzió: v_2013.04.16
Minősítés: Nyilvános
Oldalak: 14

A Tanúsítási jelentés a Hunguard Kft. Tanúsítási Divíziójának, mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezetnek a vizsgálatai alapján készült.

Tartalomjegyzék

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2013.04.11.	A szerkezet felállítása
v0.02	2013.04.26.	A tanúsítás eredményeit tartalmazó első teljes változat
v0.05	2013.04.29.	Egyeztetett változat
v1.0	**2013.04.30.**	**Végleges változat**

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft
Tanúsítási Divízió

A tanúsítási jelentést ellenőrizte:

Staub Klára
Hunguard Kft.
Minőségbiztosítási vezető

1 Bevezetés

1.1 Azonosító adatok

A tanúsítás tárgyának neve	Elektronikus beszámoló rendszer (eBESZ rendszer)
A tanúsítás tárgyának verziója	v_2013.04.16: 2013.04.16-i állapot
A tanúsítás tárgyának integrátora	WSH Számítástechnikai Oktató és Szolgáltató Kft.
A rendszer üzemeltetője	Közigazgatási és Igazságügyi Minisztérium
A tanúsítás megrendelője	Közigazgatási és Igazságügyi Minisztérium
A tanúsítás típusa	Informatikai biztonsági funkciókat megvalósító informatikai rendszer tanúsítása MIBÉTS módszertan alapján, a NAT kijelölési okirat szerint
A tanúsítás alapjául szolgáló Értékelési jelentés azonosítója	eBESZ_fv_rendszer_ertekelesi_jelentes_v1.1.doc
A tanúsítás alapjául szolgáló Értékelési jelentés készítője	Hunguard Kft. Értékelési Divízió 1123. Budapest, Kékgolyó u. 6. 5. em. 6.
A tanúsítás alapjául szolgáló Rendszer biztonsági előirányzat azonosítója	eBESZ_v1.1_rendszer_biztonsagi_eloiranyzat.doc
A tanúsítás végrehajtója	Hunguard Kft. Tanúsítási Divízió 1123. Budapest, Kékgolyó u. 6. 5. em. 4.

1. Táblázat: Azonosító adatok

1.2 A tanúsítás jellemzése

Az eBESZ rendszer tanúsítása egy működő, tanúsított rendszer újratanúsítása.

Az eBESZ rendszer kezdeti tanúsítványa 2011.12.20-i keltezéssel, HUNG-T-223-01-2011 nyilvántartási számon az elektronikus közszolgáltatás biztonságáról szóló 223/2009 (X.14.) kormányrendelet előírásainak megfeleléséről került kiállításra, érvényességi idejének megjelölése a Tanúsítvány kiállításakor: 2014.12.20. (a működtetett rendszerekben történő folyamatos változtatások miatt) évenkénti felülvizsgálat mellett.

Időközben a 223/2009. kormányrendelet visszavonásra került, lényeges továbbfejlesztések is történtek (pl. a fizetési portálhoz illesztés), ezért jelen Tanúsítvány – felhasználva a korábbi értékeléseken alapuló HUNG-T-223-01-2011 Tanúsítvány és kapcsolódó Tanúsítási jelentés állításait – már nem a 223/2009 (X.14.) kormányrendelet előírásainak megfelelését, hanem a részben megújított Rendszer biztonsági előirányzatban meghatározott követelményeknek való megfelelést állítja.

A tanúsítás alapjául szolgáló felülvizsgálati rendszer értékelése a korábbi értékelés eredményeinek fenntarthatóságára koncentrálva az alábbi területeket értékelte:

a) a korábbi értékelések óta elvégzett módosítások dokumentáltsága, értékelése, beleértve a Rendszer biztonsági előirányzat aktualizálását;
b) a legutolsó rendszer értékelés óta a rendszeren végrehajtott módosítások, valamint a technológia fejlődése következtében hogyan változtak a maradvány kockázatok (sikerült-e megszüntetni/csökkenteni ezek közül néhányat, merültek-e fel újabbak), az értékelési bizonyítékok aktualizálásával továbbra is biztosított-e a rendszer üzemeltethetősége, egyúttal átláthatósága és elemezhetősége is;

c) a műszaki és üzemeltetési biztonsági intézkedések összességében jól működtek-e a gyakorlatban, nem vetődtek-e fel ezzel kapcsolatban új, kiegészítő intézkedéseket igénylő maradvány kockázatok;
d) a legutolsó rendszer értékelés óta bejelentett vagy feltárt biztonsági hibák, illetve a felülvizsgálati értékelés során a biztonsági napló vizsgálata nem tárt-e fel új, kiegészítő intézkedéseket igénylő maradvány kockázatokat.

1.3 A tanúsítás tárgya, a rendszer biztonsági környezete és elvárásai

A tanúsítás tárgya az eBESZ rendszer, amely egy elektronikus közszolgáltatást megvalósító informatikai rendszer.

A vizsgálandó rendszer környezetét, funkcióit és határait az Elektronikus beszámoló rendszer - rendszerbiztonsági előirányzat (SST: System Security Target) [D4] dokumentum részletesen azonosítja.

1.3.1. Az eBESZ rendszer szolgáltatásai

Az eBESZ rendszer az alábbi közszolgáltatásokat biztosítja:

1. **Beküldés**: Kettős könyvvitelt vezető vállalkozók (az adózás rendjéről szóló 2003. évi XCII. törvény 7. §-ának (2) bekezdése szerinti) képviselői számára biztosítja, hogy eleget tehessenek a számvitelről szóló 2000. évi C. törvényben meghatározott, éves beszámoló letétbe helyezésére és közzétételére vonatkozó kötelezettségüknek. Ezen ügyfeleknek (a továbbiakban beküldők) az eBESZ rendszer lehetővé teszi, hogy a kormányzati portál útján a céginformációs szolgálatnak elektronikusan beküldhessék a cégükre vonatkozó mérleget, eredmény-kimutatást és a jogszabály által előírt egyéb kötelezően benyújtandó céges dokumentumokat (pl. kiegészítő melléklet, könyvvizsgálói jelentés), a jogszabály szerinti elektronikus űrlappal együtt.

2. **Letöltés**: Bárki (a továbbiakban **letöltők**) számára biztosítja a további szolgáltatások igénybe vételéhez szükséges tájékoztató és egyéb nyilvános információk (Nyomtatvány kitöltő program, Elektronikus űrlap, Beszámolóséma, MÁK igazolás, IFP igazolás, stb.) letölthetőségét az eBESZ rendszer honlapjáról.

3. **Nyilvános lekérdezés**: Bárki számára biztosítja, hogy a közzététel céljából megküldött beszámolókat haladéktalanul és ingyenesen megismerhesse. Ezen ügyfelek (a továbbiakban **lekérdezők**) az eBESZ rendszer honlapján cégnév, cégjegyzékszám vagy adószám alapján megkereshetik és megtekinthetik a beszámolókat.

4. **Ellenőrzés**: Bárki (a továbbiakban **ellenőrzők**) számára biztosítja az eBESZ rendszer által küldött elektronikus számlák aláírásának webes felületen történő ellenőrzési lehetőségét.

5. **Költségtérítés megfizetése**: A beküldők számára lehető teszi az erre vonatkozó költségtérítés (3000 Ft-os közzétételi díj) elektronikus úton történő megfizetését, az alábbi módokon:
    - a Magyar Államkincstártól (MÁK) lekért utalványminta lekérésével,
    - az Igazságügyi Fizetési Portál (IFP) útján.

Az Elektronikus beszámoló rendszer - rendszerbiztonsági előirányzat (SST: System Security Target) [D4] dokumentumban részletesen ismertetésre kerül, hogy az alábbi szerepköri felhasználók hogyan használhatják a rendszert:

- beküldők (akiknek rendelkezniük kell Ügyfélkapuval);
- letöltők;
- lekérdezők;
- (az elektronikus számla aláírásának érvényességét a webes felületen) ellenőrzők;
- a költségtérítést megfizetése közszolgáltatást igénybevevők.

Az eBESZ rendszer közszolgáltatásain kívül az alábbi kiegészítő szolgáltatásokat is biztosítja:

1. **Belső lekérdezés**: Az eBESZ rendszert működtető KIM egyes munkatársai (a továbbiakban **belső felhasználók**) számára egy külön alkalmazáson keresztül speciális lekérdezési lehetőséget biztosít az adatbázisba szervezett cégadatokról.
2. **Zártkörű külső lekérdezés**: A törvény által meghatározott közfeladatot ellátó szervek/szervezetek egyes munkatársai (a továbbiakban **külső felhasználók**) számára egy külön alkalmazáson keresztül speciális lekérdezési lehetőséget biztosít az adatbázisba szervezett cégadatokról.

Az eBESZ rendszer a köz- és kiegészítő szolgáltatásának biztosítása érdekében az alábbi háttér szolgáltatásokat veszi igénybe más informatikai rendszertől, illetve biztosítja ezen rendszer számára:

3. **NAV felhasználás**: Az eBESZ a fogadott űrlapok és csatolmányok egy részét továbbítja a NAV informatikai rendszere számára, illetve fogadja és feldolgozza a válaszokat. A szolgáltatást a **NAV rendszer** veszi igénybe.
4. **CKT felhasználás**: Az eBESZ rendszer egy külön az erre a célra kifejlesztett web szolgáltatáson keresztül számlázási adatokat továbbít a Cégközzétételi rendszer számára, illetve fogadja az elkészült elektronikusan aláírt számlákat és az ezekhez tartozó kiegészítő adatokat. A CKT (Forrás) informatikai rendszer az eBESZ rendszer tartományában helyezkedik el, illetve elérhető a minisztérium felhasználókat kezelő tartományból is. A szolgáltatást a **CKT rendszer** veszi igénybe.
5. **Microsec felhasználás**: **A** 2001-2008 közötti beszámolókra vonatkozó kérésekre az eBESZ rendszer saját adatbázisából megadja a választ az OCCR részére, egy erre a célra kifejlesztett web szolgáltatáson keresztül. A szolgáltatást az **OCCR rendszer** veszi igénybe.
6. **Rendszerfelügyelet:** A rendszer valamennyi alrendszerét felügyelni (konfigurálni, üzemeltetni, karbantartani, frissíteni) kizárólag tartományi, illetve helyi adminisztrátori jogosultsággal lehet. A rendszerfelügyelet a **Rendszeradminisztrátor** részére biztosított.

1.3.2. Az informatikai rendszer főbb jellemzői

Az informatikai rendszer jól dokumentált, a hatalmas számú dokumentációja a Rendszer biztonsági előirányzatban és az Értékelési jelentésben került részletesen összegzésre. A legfontosabb elemek tanúsítási szempontból:

- az eBESZ rendszer két központi telephellyel rendelkezik, melyek védett és nagysebességű kapcsolattal folyamatos összeköttetésben állnak egymással;
- mindkét telephelyen nagy számban kereskedelmi termékek a rendszerhez fejlesztett alkalmazások, szolgáltatások integrált rendszere működik (nagy teljesítményű hardver elemek: szerverek, mentési rendszerek stb., szoftverek: operációs rendszerek, adatbázis-kezelők, vírusvédelmi és tűzfal rendszerek, felügyeleti rendszer stb.).

1.3.3. Az eBESZ rendszer legfontosabb biztonsági tulajdonságai

Kiemelt szintű rendelkezésre állás

- Az eBESZ rendszer szolgáltatásaihoz folyamatosan biztosítja a hozzáférést.

Integritás védelem

- Az eBESZ rendszer megőrzi és megvédi az általa kezelt felhasználói adatok sértetlenségét.
- Az eBESZ rendszer garantálja a szolgáltatások nyújtásához szükséges rendszer adatok és szoftver elemek sértetlenségét.

Hozzáférés védelem

- Az eBESZ rendszer a *Beküldés* szolgáltatáshoz elfogadja a *beküldők* Ügyfélkapu által végrehajtott azonosítását és hitelesítését.
- Az eBESZ rendszer a *Lekérdezés* szolgáltatást a *lekérdezők* azonosítása és hitelesítése nélkül biztosítja.
- Az eBESZ rendszer a *Belső lekérdezés* szolgáltatást csak azonosított és hitelesített *belső felhasználók* számára biztosítja.
- Az eBESZ rendszer a *Zártkörű külső lekérdezés* szolgáltatást csak a meghatározott IP címmel rendelkező végpontokról bejelentkezett, azonosított és hitelesített *külső felhasználók* számára biztosítja.

Bizalmasság

- Az eBESZ rendszerben a kezelt ügyféladatok nyilvánosak, erre vonatkozóan bizalmassági követelmény nincs.

2 A rendszer értékelt főbb biztonsági funkciói

A Rendszer biztonsági előirányzat az alábbi főbb biztonsági funkciókat határozta meg, melyek elvárásoknak megfelelő funkcionalitását az értékelő szervezet az értékelés során igazolta:

- Azonosítás és hitelesítés;
- Hozzáférés ellenőrzés;
- Naplózás és elszámoltathatóság;
- Rendszer és kommunikáció védelem;
- Rendszer és információ sértetlenség;
- A folyamatos működés (üzletmenet folytonosság);
- Konfiguráció kezelés.

Az értékelés során az értékelési garanciaszint: fokozott (SAP-F) garanciacsomagnak felelt meg.

A választás kompromisszumos, költségkímélő megoldásként született, figyelembe véve azt a tényt (részletes indokolása megtalálható a Rendszer biztonsági előirányzatban), hogy az eBESZ által kezelt információ rendszer szintű kihatása:

- a bizalmasság szempontjából nem értelmezhető (nem kezelendő bizalmasan),
- a sértetlenség és a rendelkezésre állás szempontjából viszont kiemelt.

3 Az Értékelési jelentés főbb megállapításai

Mivel az értékelés egy felülvizsgálati rendszer értékelés volt, ezért ennek sajátosságai alapján az Értékelési jelentés a következő főbb megállapításokat tette (melyek a tanúsítás alapjául szolgálnak):

3.1 A rendszeren végrehajtott módosítások értékelése

A helyszíni szemlén áttekintetésre kerültek a kezdeti rendszer értékelés óta az üzemeltetett rendszerben történt változtatásokat.

A változáskövetésről megállapításra került, hogy az üzemeltetés során betartják a Rendszerszintű Informatikai Biztonsági Szabályzat változáskezelési rendjében meghatározottakat (RIBSZ 6.12 alfejezet és M-7 melléklet), ezen belül az alábbiakat:

- a változtatás igénylése, jóváhagyása és előkészítése;
- a változások éles üzemi környezetbe történő átvezetése;
- a változáskezeléssel kapcsolatos felelősségek.

A megvizsgált elektronikus nyilvántartásban (eBESZ_Változás kezelési nyilvántartás.xls) összesen 15 változás szerepelt, valamennyihez megtalálható volt a változásra vonatkozó kitöltött és jóváhagyott Változáskezelési űrlap.

Az elmúlt másfél évben az informatikai rendszerben a biztonságot érintő alapvető változtatások nem történtek.

3.1.1 Módosítások a korábban feltárt maradvány kockázatok megszüntetésére

A változtatások egy része a kezdeti értékelési jelentésben meghatározott maradvány kockázatok megszüntetésére irányult, a változtatásokkal sikerült a maradványkockázatot kiküszöbölni, vagy kockázati szintjét érdemben csökkenteni.

.

3.1.2 Módosítások a funkcionalitás bővítésére

A rendszer funkcionalitását érintő jelentősebb változtatás az alábbi volt:

- A rendszer adatbázisát és üzleti logikáját felkészítették az IFP (Igazságügyi Fizetési Portál) által kibocsájtott fizetési igazolás kezelésére is, így a beküldők számára lehető vált az erre vonatkozó költségtérítés (3000 Ft-os közzétételi díj) elektronikus úton történő megfizetése (az EFER rendszerhez kapcsolódva, VPOS fizetési móddal).

A bővített funkcionalitás az IFP (biztonságot is érintő) szoftver minőségi vizsgálatával került ellenőrzésre. Ennek eredményei külön dokumentumban (Igazságügyi Fizetési Portál (IFP) a mérlegbeszámoló költségtérítéséhez - Értékelési jelentés) találhatók.

Jelen Tanúsítvány hatóköre nem terjed ki az IFP biztonsági tulajdonságaira, de a szoftver minőségi vizsgálat az eBESZ rendszerre nem tárt fel biztonsági problémát.

3.2 A műszaki biztonsági intézkedések hatékonyságának értékelése

Az elmúlt másfél év üzemeltetésének biztonsága az alábbi területen került ellenőrzésre:

- a kezdeti rendszer értékelés óta jelentett szoftverműködési zavarok és biztonsági problémák áttekintése.
- Visszamenőleg megvizsgálásra kerültek a telepített szoftverek biztonsági frissítéseinek listája, felmérve ezzel a szerverek aktuális (és múltbeli) biztonsági állapotát a nyilvánosságra hozott és kijavított biztonsági hibák elméleti kihasználhatósága szempontjából.
- Bekövetkezett biztonsági események nyomainak keresése a naplókban, az esetlegesen gyakorlatilag is kihasznált biztonsági hibák megállapítása érdekében.

3.2.1 A kezdeti rendszer értékelés óta jelentett biztonsági problémák vizsgálata

A kezdeti rendszer értékelés óta a szoftverműködési zavarok és a biztonsági problémák bejelentését megfelelően, a RIBSz 3.8 alfejezetében, illetve az M-13 és M-14 mellékleteiben meghatározottaknak megfelelően végezték.

Az elmúlt másfél évben két komolyabb működési hiba lépett fel, melyeket az értékelők elemeztek.

Az elmúlt másfél évben biztonsági eseményt, sérülékenység kihasználását nem észleltek.

3.2.2 A biztonsági frissítések telepítéseinek visszamenőleges ellenőrzése

A biztonsági frissítéseket alapvetően a RIBSz 6.8 alfejezetében meghatározottaknak megfelelően végezték.

3.2.3 Bekövetkezett biztonsági események nyomainak keresése

Helyszíni szemle során az értékelők a kezdeti rendszer értékelés óta az üzemeltetett rendszerben történt biztonsági események nyomait vizsgálták a naplóállományok, pásztázó eszközök nyomai, vírus-incidens lista elemzésével.

Az értékelés biztonságot veszélyeztető eseményt nem tárt fel.

3.3 Az üzemeltetési környezetre vonatkozó feltételezések teljesülésének vizsgálata

A felülvizsgálati rendszer értékelés során a műszaki (döntően szoftver-hardver által megvalósított) ellenintézkedések mellett, sor került a menedzsment és üzemeltetési (döntően ember által megvalósított) ellenintézkedések hatékonyságának a felmérésére is.

A rendszer biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételek (melyek tehát nem műszaki, hanem menedzsment és üzemeltetési ellenintézkedéseket igényelnek) teljesülését a Rendszer értékelési jelentés részletesen elemezte és elfogadta.

4 A biztonság érvényre juttatásához szükséges – rendszeren kívüli – feltételek

Az értékelések következtetései a Rendszer biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén is múlnak. Ezen feltételeket (melyek teljesítése nem műszaki, hanem menedzsment és üzemeltetési ellenintézkedéseket igényel, és a szabályozási értékelés a megfelelőséget megállapította) a folyamatos működtetés során biztosítani szükséges.

F1_Kockázatfelmérés

A rendszer működtetője rendszeres időnként, illetve jelentős változások alkalmával felméri a szervezeti működés során jelen lévő, a rendszer működéséből és kapcsolódó információ feldolgozó, tároló vagy átviteli műveletekből származó biztonsági kockázatokat és a rendszer értékeit.

F2_Biztonsági_értékelés_és_auditálás

A rendszer működtetője:

a) rendszeres időközönként értékeli az IT rendszer biztonsági intézkedéseit, annak megállapításához, hogy az intézkedéseket hatékonyan alkalmazzák-e;
b) intézkedési tervet készít és hajt végre a hiányosságok korrigálására, a rendszerekben meglévő sebezhetőségek csökkentésére vagy kiküszöbölésére;
c) engedélyezteti (akkreditáltatja) az informatikai rendszer működését és bármilyen rendszerkapcsolatot, kapcsolódást;
d) folyamatosan felügyeli, ellenőrizi a biztonsági intézkedések betartását a hatékonyság folytonosságának biztosítása érdekében.

F3_Fizikai_biztonság

Az eBESZ rendszer működtetője és üzemeltetője:

a) a jogosult felhasználókra korlátozza az eBESZ rendszerhez, berendezéseihez és kapcsolódó üzemeltetési környezetéhez való fizikai hozzáférést;
b) védi a fizikai létesítményt, biztosítja az eBESZ rendszerhez szükséges infrastruktúrát;
c) biztosítja az eBESZ rendszerhez szükséges háttér és kiegészítő szolgáltatásokat;
d) védi az eBESZ informatikai rendszert a környezeti veszélyektől;
e) megfelelő környezeti intézkedésekről gondoskodik az eBESZ rendszernek helyt adó létesítményekben.

F4_Adathordozók_védelme

Az eBESZ rendszer működtetője és üzemeltetője:

a) védi a rendszer papír alapú vagy digitális adathordozóin lévő információit;
b) jogosult felhasználókra korlátozza a hozzáférést a nyomtatott vagy digitális információkhoz;
c) a digitális adathordozóról biztonságosan törli a rajtuk lévő információt azok eltávolítása vagy újra használata előtt.

F5_Üzletmenet_folytonosság_tervezése

Az eBESZ rendszer működtetője és üzemeltetője terveket készít, ezeket karbantartja és hatékonyan megvalósítja a rendkívüli helyzetekre való reagálásra, a mentési műveletekre és a katasztrófák utáni helyreállításra, annak biztosítása érdekében, hogy a kritikus információs erőforrások rendelkezésre álljanak és rendkívüli helyzetekben is megvalósuljon a folyamatos működés követelménye.

F6_Reagálás_biztonsági_eseményekre

Az eBESZ rendszer működtetője és üzemeltetője

a) biztonsági események kezelésére alkalmas képességet alakít ki az eBESZ rendszerre,
b) nyomon követi, dokumentálja és jelenti az eseményeket a szervezetben erre kijelölt illetékes személynek és/vagy szervezetnek, hatóságnak.

5. Megfelelőségi összegzés

Minden informatikai rendszerben természetesen keletkeznek és maradnak is nem kivédett kockázatok a kialakítás, használat, továbbfejlesztés és üzemeltetés során.

Az informatikai biztonság az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos /ld. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 1.§ 15. pont /.

Ennek megfelelően a fenti definícióba nem beleértendő azon kockázatokat tekintjük maradvány kockázatoknak, amely az adott rendszerben sem technológiai eszközökkel, sem szervezési, szabályozási eszközökkel nincsenek kivédve, de a veszélyek kockázatai, károkozásai, az esetleges támadók motivációi oldaláról – bár kis valószínűségű események – mégis kivédendő kockázatoknak minősíthetőek.

> A technológiai értékelés is feltárhat ilyen, ki nem védett maradvány kockázatokat.
>
> Általában a szervezet biztonságért felelős vezetőségének felelőssége, hogy milyen szintű kockázatot vállalnak fel.
>
> A döntések leggyakrabban (leírt, vagy csak átgondolt) költség-haszon elemzésen, valamint kockázatbecslésen alapulnak. /Lehet a maradványkockázatokat áthárítani is (pl. biztosításokkal), vagy tudatosan, megfelelő elemzések alapján felvállalni./

A Rendszer biztonsági előirányzat már egy kockázatelemzés utáni szükséges intézkedés-sorozatot ír elő. A Rendszer értékelési jelentés felsorol olyan maradványkockázatokat – kis valószínűségű, vagy kis kárértékű eseteket -, amelyek ha nem nagy kockázati szintűnek is minősíthetőek, akkor is javító intézkedések egy soron következő változtatásig (pl. az informatikai rendszer továbbfejlesztése), de mindenképpen a következő audit időpontjáig célszerű megtenni.

A fentek figyelembe vételével a tanúsítás megállapítása a következő:

Az eBESZ rendszer és dokumentációja megfelel a Rendszer biztonsági előirányzatban meghatározott biztonsági és garanciális követelményeknek, az abban kitűzött biztonsági célok, elvárások konzisztensek, megfelelnek az elektronikus információbiztonsági elvárásoknak és teljesülnek, a rendszer biztonságosan üzemeltethető.

Az eBESZ rendszer biztonsági elvárásoknak megfelelőségére a Tanúsítvány kiállítható.

6. Hivatkozások

6.1 Módszertani hivatkozások

[M1]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v4 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M2]: Útmutató rendszer értékelőknek (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M3]: Útmutató tanúsítók számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[M4]: National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, December 2007

6.2 A tanúsításhoz felhasznált dokumentumok hivatkozásai

[D1]: eBESZ Tanúsítási jelentés HUNG-TJ-223-01/2011

[D2]: eBESZ Tanúsítvány HUNG-T-223-01/2011

[D3]: ELEKTRONIKUS BESZÁMOLÓ RENDSZER Rendszer értékelési jelentés

[D4]: Elektronikus beszámoló rendszer - Rendszer biztonsági előirányzat, v1.1