

1. Útmutató

1.1. Tartalom

- 1.2. Bevezető
- 1.3. Szerzők

2. Aktuális információk

- 2.1. Tartalom
- 2.2. Informatikai biztonsági megfontolások a Sarbanes – Oxley törvény ürügyén
 - 2.2.1. A SOX, a sajt, és a maffia – bevezető
 - 2.2.2. A Sarbanes – Oxley törvény, és az amerikai befektetők érdekei védelmének története
 - 2.2.3. Mi is az pontosan, amiért felelős a vezetőség?
 - 2.2.4. A törvény informatikai vonzatai
 - 2.2.4.1. Az alkalmazói rendszerek funkcionalitási megfeleléséből, és adataik érzékenységéből a törvény szerint eredő követelmények
 - 2.2.4.2. A SOX követelményei az intézményi dokumentációs rendszerre, és az auditorok dokumentumkezelésével kapcsolatban
 - 2.2.4.3. COBIT és COSO elemek felhasználási lehetőségei a Sarbanes – Oxley törvény feltételeinek teljesítésében. Informatikai biztonsági tanulságok
 - 2.2.5. A törvény betartása, felügyeletéből eredő új követelmények – a folyamatos ellenőrzés, a folytonos audit, és lehetőségeik

- 2.2.5.1. Az adatélelciklus vizsgálatának szükségessége
- 2.2.5.2. Külső ellenőri hozzáférés az adatokhoz – ellenvetések
- 2.2.5.3. A folyamatos bizonyítékgyűjtés módjai
- 2.2.6. A vállalati alkalmazások SOX pontjai – részletek egy felkészülésből
 - 2.2.6.1. A felkészülés előzményei, előzetes teendők
 - 2.2.6.2. Az informatikai szakterület SOX feladatainak meghatározása
 - 2.2.6.3. A szakmai legjobb gyakorlat, mint segítség
 - 2.2.7. A neurális hálók alkalmazhatósága a Sarbanes – Oxley törvény szerinti megfélelési vizsgálatokban
- 2.2.8. Irodalomjegyzék, rövidítések
- 2.3. Szabványok és ajánlások
- 2.4. Fogalmak és definíciók
 - 2.4.1. Irodalomjegyzék, rövidítések
- 2.5. A szolgáltatás-orientált architektúrák biztonsági kérdései
 - 2.5.1. A SOA módszertan célja
 - 2.5.2. Magyarázzuk a terminológiánkat – middleware, vagy enterprise service bus helyett „becsomagolunk”
 - 2.5.3. A szolgáltatás-orientált architektúra alapelvei és komponensei
 - 2.5.3.1. A SOA architektúrális és tervezési alapelvei
 - 2.5.3.2. Technikai SOA komponensek
 - 2.5.3.3. Aggályok
 - 2.5.4. A SOA-szerű architektúrák előképei
 - 2.5.5. Rutinveszélyek
 - 2.5.6. Veszély és védelem a SOA koncepció egyes rétegein
 - 2.5.6.1. Legalul: a szolgáltatást megvalósító rendszer
 - 2.5.6.2. A szolgáltatást követő réteg: a becsomagolás. A szolgáltatások becsomagolásából eredő biztonsági előnyök és hátrányok
 - 2.5.7. A kommunikáció formái az architektúrán belül: a szolgáltatások között
 - 2.5.7.1. Az XML-lel kapcsolatos biztonsági problémák

- 2.5.7.2. A web-szolgáltatások kliens-szerver alapú kommunikációja. A SOAP veszélyforrásai és kezelésük
- 2.5.7.3. Egyéb kommunikációs formák
- 2.5.7.4. Az OASIS ajánlásai a web-szolgáltatások együttműködésének biztonságára
- 2.5.8. A kommunikáció közege, az intézményi számítógép-hálózat veszélyei.
A hálózati védelem lehetőségei és korlátai
- 2.5.9. Behívási környezet: az újfajta forgalomirányító, a web-oldal
- 2.5.10. Számítógépes alkalmazásokat fenyegető veszély és védelem
- 2.5.10.1. A mögöttes adatbázisok fokozott védelme
- 2.5.10.2. A web-szolgáltatások programozásának problémái, az ütemezés
- 2.5.10.3. Rugalmasság az üzlet érdekében
- 2.5.10.4. Hardver szintű adatvédelem és adatvesztélyeztetés
- 2.5.10.5. A folytonos audit szükségessége
- 2.5.11. A SOA és a grid
- 2.5.12. Veszélyek az intézmény hatókörén kívül – az egyetemes felelősség, és néhány nemzetközi jellegű megoldásszállítói biztonsági kezdeményezés
- 2.5.13. Rövidítések jegyzéke
- 2.5.14. Irodalomjegyzék

3. Az informatikai biztonság

- 3.1. Tartalom
- 3.2. Az informatikai biztonság kialakulása (CD-ROM-on olvasható)
- 3.3. Az informatikai biztonság meghatározása (CD-ROM-on olvasható)
- 3.4. Az informatikai biztonsággal kapcsolatos törvényekről és rendeletekről
- 3.5. Hazai és nemzetközi biztonsági együttműködések

- 3.5.1. CERT-ek szerepe a hálózatbiztonsági incidensek kezelésében
 - 3.5.1.1. A CERT szervezetek kialakulása
 - 3.5.1.2. A CERT keretrendszer
 - 3.5.1.3. A CERT szolgáltatásai
- 3.5.2. Minősített adatot kezelő elektronikus rendszerek biztonsága a NATO-ban és az Európai Unióban
 - 3.5.2.1. Általános elvek
 - 3.5.2.2. A biztonság alapjai
 - 3.5.2.3. Az információbiztonság védelme
 - 3.5.2.4. Az informatikai rendszerek és a kommunikációbiztonság védelme
 - 3.5.2.5. Személyi biztonság
 - 3.5.2.6. Fizikai biztonság
 - 3.5.2.7. Dokumentum biztonság
 - 3.5.2.8. Minősítési szintek és megfeleltetésük a nemzeti rendszerekben
 - 3.5.2.9. Útmutató az SSRS elkészítéséhez
- 3.5.3. Az Unió csatlakozás és az informatikai biztonság (CD-ROM-on olvasható)
- 3.6. Információs hadviselés – információs terrorizmus – kiber-terrorizmus
 - 3.6.1. A hadviselés új hadszínterei
 - 3.6.1.1. A hadviselés színtérének változásai az emberiség történelme során
 - 3.6.1.2. A kibertér, mint a hadviselés hatodik színtere
 - 3.6.2. Az információs társadalom infrastruktúrái
 - 3.6.2.1. Az információs infrastruktúrák csoportosítása
 - 3.6.3. Információs hadviselés – az információs színtéren folytatott küzdelem alapjai
 - 3.6.3.1. Az információs fölény értelmezése, szintjei
 - 3.6.3.2. Az információs támadás modellje
 - 3.6.3.3. Az információs hadviselés kialakulása
 - 3.6.3.4. Az információs hadviselés fogalma, értelmezése
 - 3.6.3.5. Az információs hadviselés filozófiája
 - 3.6.3.6. Az információs hadviselés fajtái
 - 3.6.3.7. Az információs hadviselés elemei
 - 3.6.4. Információs terrorizmus – kiber-terrorizmus

- 3.6.5. Egy információs támadás forgatókönyve (esettanulmány)
- 3.7. Kritikus információs infrastruktúrák biztonsága
 - 3.7.1. Infrastruktúrák
 - 3.7.1.1. Funkcionális információs infrastruktúrák
 - 3.7.1.2. Támogató információs infrastruktúrák
 - 3.7.2. Kritikus infrastruktúrák
 - 3.7.2.1. Kritikus infrastruktúra meghatározások különböző országokban
 - 3.7.3. Kritikus információs infrastruktúrák
 - 3.7.4. Energiaellátó rendszerek rendszerirányítása
 - 3.7.4.1. Villamosenergia-rendszer
 - 3.7.4.2. Gázellátás és rendszerirányítása
 - 3.7.5. Internet Magyarországon
 - 3.7.5.1. HBONE és IIF
 - 3.7.5.2. Elektronikus Kormányzati Gerinchálózat
 - 3.7.5.3. Kormányzati portál, kormányzati ügyfél-tájékoztató központ, elektronikus ügyfélkapu
 - 3.7.5.4. A Sulinet-hálózat
 - 3.7.5.5. Kereskedelmi internet
 - 3.7.6. Védelmi szféra infrastruktúrák
 - 3.7.6.1. Navigáció
 - 3.7.6.2. Korszerű felderítő rendszerek
 - 3.7.6.3. Térinformatikai alapú katonai információs rendszerek
 - 3.7.6.4. Harcászati internet-hálózatok
 - 3.7.7. Kritikus információs infrastruktúrák elleni fenyegetések
 - 3.7.8. Kritikus információs infrastruktúrák védelme
 - 3.7. Irodalomjegyzék

4. Informatikai biztonsági követelmények

- 4.1. Tartalom
- 4.2. A kommunikáció kérdései
 - 4.2.1. A szteganográfia alkalmazási lehetőségei és módszertana az információvédelemben
 - 4.2.1.1. Az adatrejtés múltja

- 4.2.1.2. Az információrejtés technikája és eszközei
- 4.2.1.3. Szteganalízis
- 4.2.1.4. Gyakorlati szteganalízis
- 4.2.1.5. Függelék
- 4.2.1.6. Irodalomjegyzék
- 4.3. Adatfeldolgozási és biztonsági események naplózása
 - 4.3.1. A naplózási tevékenység célja
 - 4.3.1.1. A naplózás történetének áttekintése
 - 4.3.1.2. Kihívások és válaszok
 - 4.3.1.3. Az infrastruktúra
 - 4.3.2. Tervezés
 - 4.3.3. A naplózás szabályozási és ellenőrző környezete
 - 4.3.3.1. Koncepció
 - 4.3.3.2. Szabályozás
 - 4.3.3.3. Példa szabályozókörnyezetekre
 - 4.3.3.4. GAP analízis – a hiányosságok vizsgálata
 - 4.3.4. Eljárásrend és üzemeltetés
- 4.4. A hálózatbiztonsági incidens menedzsment folyamata
 - 4.4.1. Az incidens
 - 4.4.2. Számítógépes hálózatok védelme
 - 4.4.3. Az incidens menedzsment
 - 4.4.3.1. Az incidens menedzsment követelményei
 - 4.4.3.2. Az incidens menedzsment folyamat áttekintése
 - 4.4.4. Az incidens kezelés
 - 4.4.4.1. Az incidens kezelési szolgáltatás meghatározása
 - 4.4.4.2. Az incidens kezelési szolgáltatás funkciói
 - 4.4.4.3. A sorrendbe állítás funkció
 - 4.4.4.4. A kezelési funkció
 - 4.4.4.5. A közzétételi funkció
 - 4.4.4.6. A visszajelzési funkció
 - 4.4.4.7. Együttműködések
 - 4.4.4.8. Információkezelés
- 4.5. A Sérülékenységek Egységes Értékelési Rendszere, azaz a Common Vulnerability Scoring System

- 4.5.1. Bevezetés
- 4.5.2. Mi a CVSS?
- 4.5.3. Metrikus csoportok
 - 4.5.3.1. Bázis metrika
 - 4.5.3.2. Az időbeliség metrikái
 - 4.5.3.3. A környezet metrikái
 - 4.5.3.4. Bázis, időbeli és környezeti vektorok
- 4.5.4. Mérőszámok
 - 4.5.4.1. Irányelvek
 - 4.5.4.2. Egyenletek
 - 4.5.4.3. Példák a CVSS használatára
- 4.5.5. További források
- 4.5.6. Irodalomjegyzék

5. A védelem megvalósítása

- 5.1. Tartalom
- 5.2. Bevezetés
- 5.3. Számítógéphálózatok
 - 5.3.1. A számítógéphálózatok biztonságának felülvizsgálata
 - 5.3.2. A számítógéphálózatok biztonságának alapfogalmai
 - 5.3.2.1. Rétegszemlélet
 - 5.3.2.2. Hálózatbiztonsági megközelítés
 - 5.3.2.3. Az információt hordozó üzenet elleni támadások hálózatokban
 - 5.3.2.4. A fizikai réteg információinak biztonsági problémái
 - 5.3.2.5. Az adatkapcsolati réteg információinak biztonsági problémái
 - 5.3.2.6. A hálózati réteg információinak biztonsági problémái
 - 5.3.2.7. A szállítási réteg információinak biztonsági problémái
 - 5.3.3. A vezetékes távközlő rendszerek áttekintése
 - 5.3.4. A mobil cellás rádiótelefon rendszerek áttekintése és néhány gyakorlati alkalmazás

- 5.3.4.1. A biztonsági megfontolások helye a GSM rendszerek áttekintésében
- 5.3.4.2. A GSM hálózatok felépítésének sémája
- 5.3.4.3. A GSM hálózatok elleni lehetséges támadások áttekintése
- 5.3.4.4. Védekezés a támadásokkal szemben, biztonság a GSM hálózatokban
- 5.3.4.5. Rövidítések az 5.3.4.1. – 5.3.4.4. szakaszokhoz
- 5.3.4.6. Irodalomjegyzék az 5.3.4.1. – 5.3.4.4. szakaszokhoz
- 5.3.5. Műholdas Távközlési Rendszerek
- 5.4. A szabályozás kérdései (CD-ROM-on olvasható)
- 5.5. Az emberi tényező jelentősége az informatikai biztonságban (CD-ROM-on olvasható)
- 5.6. Az informatikai helyiségek fizikai védelme (CD-ROM-on olvasható)
- 5.7. Dokumentumkezelés, ügyvitel (CD-ROM-on olvasható)
- 5.8. Logikai védelem az infrastrukturális elemek szintjén
 - 5.8.1. Operációs rendszerek
 - 5.8.1.1. DOS alapú operációs rendszerek
 - 5.8.1.2. Windows 95 operációs rendszer
 - 5.8.1.3. Windows 98 operációs rendszer
 - 5.8.1.4. További Windows informatikai biztonsági információk
 - 5.8.1.5. VMS (CD-ROM-on olvasható)
 - 5.8.1.6. IBM OS/390 (CD-ROM-on olvasható)
 - 5.8.1.7. UNIX (CD-ROM-on olvasható)
 - 5.8.1.8. Novell hálózati operációs rendszer (CD-ROM-on olvasható)
 - 5.8.1.9. OS/400 (CD-ROM-on olvasható)
 - 5.8.1.10. Linux (CD-ROM-on olvasható)
 - 5.8.1.11. Windows 2000 operációs rendszer (CD-ROM-on olvasható)
 - 5.8.1.12. FreeBSD (CD-ROM-on olvasható)
 - 5.8.1.13. Hozzáférés-védelem az MS Windows operációs rendszerekben (CD-ROM-on olvasható)

- 5.8.2. Hálózatok
- 5.8.3. Oracle adatbázis alapú rendszerek biztonsága

6. Napjaink problémái

- 6.1. Tartalom
- 6.2. IDS/IPS és ami mögötte van...
 - 6.2.1. Bevezetés
 - 6.2.2. Az IDS áttekintése és története
 - 6.2.3. Mi az a behatolás érzékelés?
 - 6.2.4. Miért szükséges az IDS használata?
 - 6.2.4.1. A kockázat növekedés megelőzésének problémái
 - 6.2.4.2. Érzékelési problémák, melyek nem kiküszöbölhetők más biztonsági fogásokkal
 - 6.2.4.3. A támadási módok detektálása
 - 6.2.4.4. A meglévő fenyegetettség dokumentálása
 - 6.2.4.5. Hasznos információk az aktuális támadásokról
 - 6.3. E-business (CD-ROM-on olvasható)
 - 6.4. A rejtjelzés, az elektronikus dokumentumok azonosítása és a digitális aláírás (CD-ROM-on olvasható)
- 6.5. Az Internet – hackerek és crackerek (CD-ROM-on olvasható)
- 6.6. Vírusok, férgek, trójai programok
 - 6.6.1. Bevezetés
 - 6.6.2. Történeti áttekintés
 - 6.6.3. Víruselméleti kérdések
 - 6.6.4. A PC-k (noteszgép, asztali gép, kiszolgáló, okostelefon és PDA) fertőzési lehetőségei
 - 6.6.5. A nem PC alapú és vékony kliens architektúrák támadhatósága
 - 6.6.6. Férgék
 - 6.6.7. Trójai jellegű programok
 - 6.6.8. Egyéb, a programokkal kapcsolatos veszélyek
 - 6.6.9. Mai jellemző veszélyforrások, trendek, várható új támadástípusok
 - 6.6.10. Védekezési lehetőségek a PC vírusai ellen, szoftvertípusok és eszközök

- 6.6.11. Vírusvédelmi megvalósítások
- 6.6.12. Nem (tisztán) program jellegű támadók
- 6.7. Pénzüntézeti informatikai rendszerek néhány biztonsági aspektusa
 - 6.7.1. Pénzüntézeti információ biztonság
 - 6.7.2. Speciális körülmények, követelmények
 - 6.7.3. Humán kockázatok
 - 6.7.4. Rendszerek rendelkezésre állása
 - 6.7.5. Hibatűrő hardware eszközök és megoldások alkalmazása
 - 6.7.6. Üzletmenet-folytonosság, katasztrófa helyreállítás
 - 6.7.7. Megbízható azonosítás, hitelesítés, bizalmasság
 - 6.7.8. Pénzüntézeti informatikai rendszerek határvédelme
 - 6.7.9. Informatikai rendszer biztonsági menedzsment
- 6.8. Az integrált vállalatirányítási információs rendszerek biztonsága
 - 6.8.1. Az integrált vállalatirányítási rendszerek kialakulása és jelentősége
 - 6.8.1.1. Az információs rendszerek fejlődés-története és az integrált rendszerek megjelenése
 - 6.8.1.2. Az üzleti folyamatok támogatása vállalati erőforrás tervező rendszerekkel
 - 6.8.1.3. A vállalati információcserét támogató informatikai megoldás létesítésének lehetőségei
 - 6.8.1.4. A vállalati erőforrás tervező rendszerektől elvárt alapvető szolgáltatások
 - 6.9. Szoftvertermékek és folyamatok minősége és az informatikai biztonság
 - 6.9.1. Bevezetés
 - 6.9.2. A szoftver termékek és folyamatok értékelésére és tanúsításra vonatkozó, nemzetközileg elfogadott módszertanok áttekintése
 - 6.9.2.1. ISO/IEC 9126, ISO/IEC 14598, ISO/IEC 25000
 - 6.9.2.2. ISO 9000
 - 6.9.2.3. CMM
 - 6.9.2.4. CMMI
 - 6.9.2.5. ISO/IEC 15504 (SPICE)

- 6.9.3. Szoftvertermékek és folyamatok minőségének szerepe az informatikai biztonság növelésében
- 6.10. Az Informatikai szolgáltatások biztonsága
 - 6.10.1. Az ITSM és az ITIL
 - 6.10.2. Az ITIL rövid története
 - 6.10.2.1. ITIL V1
 - 6.10.2.2. ITIL V2
 - 6.10.2.3. ITIL V3
 - 6.10.3. ITIL és a benne rejlő biztonsági szempontok
 - 6.10.3.1. Az Információbiztonság elhelyezése a témában
 - 6.10.3.2. Információbiztonság menedzsment folyamat
 - 6.10.3.3. Informatikai szolgáltatások biztonsága
 - 6.10.4. Definíciók
 - 6.10.4.1. Mi az a szolgáltatás
 - 6.10.4.2. Mi a szolgáltatás menedzsment
 - 6.10.4.3. A jó és a legjobb szakmai gyakorlat
 - 6.10.4.4. Funkciók
 - 6.10.4.5. Folyamatok
 - 6.10.4.6. Szerepkörök
 - 6.10.4.7. Változás
 - 6.10.4.8. Kiadás
 - 6.10.4.9. Esemény
 - 6.10.4.10. Incidenskezelés
 - 6.10.4.11. Problémakezelés
 - 6.10.4.12. Hozzáférés menedzsment
 - 6.10.4.13. Életciklus
 - 6.10.5. Szolgáltatás-stratégia
 - 6.10.6. Szolgáltatás-tervezés
 - 6.10.7. Szolgáltatás-létesítés és -változtatás
 - 6.10.8. Szolgáltatás-üzemeltetés
 - 6.10.9. Szolgáltatások folyamatos fejlesztése

7. Az irányítás és a stratégia támogatása informatikai biztonsági eszközökkel

Mottó

1.1. Tartalom

Az informatikai biztonság kézikönyve

- 7.2. Az ISACA auditálási alapelvei, és a COBIT® módszertan bemutatása
 - 7.2.1. Bevezetés
 - 7.2.2. A COBIT® célja, fejlődése, és alapvető komponensei
 - 7.2.2.1. A COBIT® indító alapfogalmai
 - 7.2.2.2. Az informatikai irányítás hangolása a kiegyensúlyozott mutatószámrendszer, és a képesség érettségi modell egyes fogalmainak bevezetésével
 - 7.2.3. A COBIT® alkalmazása informatikai biztonsági döntésekben, és ellenőrzési irányelvei
 - 7.2.4. Példa ellenőrzési feladat lépéseire – a COBIT® és a CISA Review Technical Information Manual alapján
 - 7.2.5. Példa biztonsági ellenőrzési lista kialakítására a COBIT® segítségével
 - 7.2.6. Néhány, a COBIT® példának megfelelő ellenőrzési cél, ellenőrzési intézkedés és eljárás az ISO/IEC 17799, és az ISO/IEC 27001 szabvány szerint
- 7.3. A COBIT 4.0 és 4.1 újdonságai
 - 7.3.1. Előszó új COBIT fejezetünkhöz
 - 7.3.2. A COBIT® 4 alapelvei
 - 7.3.2.1. Az informatikai irányítás fogalmának fejlődése
 - 7.3.2.2. Ellenőrzési célok alkalmazói rendszerekhez
 - 7.3.2.3. Az irányítási és szervezeti érettség vizsgálatának újdonságaiból

8. Mellékletek

- 8.1. Tartalom
- 8.2. Az elektronikus aláírás (CD-ROM-on olvasható)
- 8.3. Számítógépes bűnözés (CD-ROM-on olvasható)
- 8.4. Az elektronikus kereskedelem (CD-ROM-on olvasható)
- 8.5. Informatikai Biztonsági Szabályzat (ajánlás) (CD-ROM-on olvasható)

- 8.6. Kockázatkezelés szempontrendszerrel irányított értékelési módszerrel
 - 8.6.1. A kockázat, mint stratégiai ellenőrzési cél
 - 8.6.2. A kockázatkezelés a biztonsági és az informatikai biztonsági rendszerben
 - 8.6.3. Egy kockázatkezelési módszertan
 - 8.6.3.1. A kockázatkezelési ciklus
 - 8.6.3.2. Kockázatbecslés
 - 8.6.3.3. Üzleti folyamatok és folyamatrendszerek vizsgálata és értékelése
 - 8.6.4. Egy kiinduló követelmény szempontrendszer kockázatkezelési példaprojekthez
 - 8.6.5. A kockázatkezelés gyakorlata
 - 8.6.5.1. A COBIT® alkalmazása a szempontrendszerrel irányított értékelési módszerrel együtt
 - 8.6.5.2. Gyakorlati megfontolások
- 8.7. Domain nevek regisztrációja (CD-ROM-on olvasható)
- 8.8. Az EU Tanácsának határozata a Tanács biztonsági szabályzatának elfogadásáról (2001/264/EK) (CD-ROM-on olvasható)
- 8.9. Az informatikai ellenőrzés feladatai
 - 8.9.1. Az informatikai ellenőrök feladatai
 - 8.9.2. IT biztonsági kockázatmenedzselés
 - 8.9.2.1. Kockázatértékelés
 - 8.9.2.2. A kockázatértékelés eredménye
 - 8.9.2.3. A kockázatok kezelése – „kockázattal arányos” védelem kialakítása
 - 8.9.3. Az IT szabályozás szerepe
 - 8.9.3.1. A vonatkozó szabályozás áttekintése, struktúrája
 - 8.9.3.2. Szükséges IT – biztonsági – szabályozások tartalma
 - 8.9.4. A feladatok és felelőségek elhatárolásának áttekintése
 - 8.9.4.1. Feladatok és felelősségi körök meghatározása
 - 8.9.4.2. Legfontosabb összeférhetlenségek
 - 8.9.5. Informatikai nyilvántartások vizsgálata

- 8.9.5.1. A nyilvántartásokkal kapcsolatos feladatok vizsgálata
- 8.9.5.2. A nyilvántartások tartalma
- 8.9.6. Biztonsági dokumentációkkal szembeni elvárások
- 8.9.7. Az intézmény jogosultságkezelésének vizsgálata
- 8.9.7.1. Általános elvárások
- 8.9.7.2. A központi jogosultságkezelés
- 8.9.7.3. Vonatkozó szabályozások
- 8.9.7.4. Igénylések dokumentálása és nyilvántartása
- 8.9.8. Az IT és IT Biztonsági stratégia vizsgálata
- 8.9.9. Az alkalmazásfejlesztés ellenőrzése
- 8.9.9.1. Specifikációs szakasz
- 8.9.9.2. Fejlesztési szakasz vizsgálata
- 8.9.9.3. Tesztelési szakasz vizsgálata
- 8.9.9.4. Az üzembe helyezés és az utógondozási szakasz vizsgálata
- 8.9.9.5. Vizsgálat adatmigráció esetében
- 8.9.10. Változáskezelés
- 8.9.11. Rendkívüli helyzetek kezelése
- 8.9.11.1. Az üzletmenet-folytonosság menedzselése
- 8.9.11.2. Az üzletmenet-folytonossági tervek ellenőrzése
- 8.9.11.3. A BCP/DRP tervek tesztelése
- 8.9.11.4. A BCP/DRP tervek aktualizálása
- 8.9.12. A naplózás ellenőrzése
- 8.9.12.1. Naplózási koncepció
- 8.9.12.2. Naplózási beállítások
- 8.9.12.3. Naplóállomány elemzések
- 8.9.10.4. ...és egy példa (a Hpt. 13/B. § értelmezése)
- 8.9.13. Oktatás és IT biztonság-tudatosság
- 8.9.14. További informatikai biztonsági ellenőrzési célok és ellenőrzési intézkedések
- 8.9.14.1. Adatátvitel és adathordozók szállítása
- 8.9.14.2. Vírusvédelem
- 8.9.14.3. Logikai védelmi eszközök
- 8.9.14.4. Fizikai védelem
- 8.9.14.5. Internetes és elektronikus bankolás
- 8.9.14.6. A tűzfalak menedzselése
- 8.9.14.7. A mozgatható adathordozók, perifériák védelme

- 8.10. Az informatikai erőforrás-kihelyezés auditálási szempontjai
- 8.10.1. Összefoglaló áttekintés
Az erőforrás-kihelyezés tervezése

