BIZTONSÁGI AUDIT

Tárgy:	Szolgáltatás menedzsment
Kód:	NIRSM1MMEM
Kredit:	5
Szak:	Mérnök Informatikus MSc (esti)
Óraszám:	Előadás: 2/hét Laborgyakorlat: 2/hét
Számonkérés:	Vizsga, (félévi 1db ZH)

Biztonsági Audit célja

- Az IT Biztonságpolitika (IBP) és az IT Biztonsági Szabályzat (IBSZ) kidolgozása „házon belüli” feladat
  - Megfelelő IBP/IBSZ csak a helyi viszonyok ismeretében készíthető
  - Ehhez azonban lehetséges külső – szakértői – segítség igénybe vétele
- Az IBP/IBSZ kidolgozói „nem gondolhatnak mindenre”, fontos szempontok esetleg megoldás nélkül maradhatnak
- Az IBP/IBSZ belső ellenőrzése mellett ezért külső erők bevonása indokolt

- A „külső erőket” auditoroknak nevezik
- A külsősök által végrehajtott [IBP/IBSZ] vizsgálat = Audit

Informatikai audit módszertanok

- Több IT audit módszertan ismert és használt világszerte
- ISACA – Information System Audit and Control Association
  - CISA – Certified Information System Auditor
  - CISA minősítés komoly vizsgák letételét követeli
    - CISA minősítés Magyarországon is megszerezhető
  - Tudás szinten tartása érdekében éves továbbképzések kötelezők
  - ISACA **NEM bocsát ki** „megfelelt/nem felelt meg” **tanúsítványt**
- ISACA által követett módszertan = COBIT
  - **COBIT** = Governance and **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology –**„csak” ajánlás, NEM szabvány**
  - Többszáz IT rendszer kialakításával kapcsolatos irányelv (control)
  - Mivel **folyamatosan** frissítik, így számos esetben konkrét technikai megoldásokra vonatkozó javaslatokat is tartalmaz

Fontosabb IT biztonsági szabványok

- Az IT biztonság jelentőségének fokozódása tette szükségessé a vonatkozó szabványok kidolgozását
- Kidolgozásuk lehetővé teszi formális auditok végrehajtását

- Első ilyen szabvány = BS 7799 – 1995
  - BSI = British Standards Institution
- ISO 27000 = Nemzetközi szabvány(ok) – 2005
  - Pontosan: ISO/IEC szabványcsalád, mivel mindkét szervezet jegyzi
    - ISO = International Organization for Standardization
    - IEC = International Electrotechnical Commission
- NIST 800-xx National Institute of Standards and Technology
- ISO 15408 – Common Criteria (CC)
- RFC 2196 – Internet Engineering Task Force memorandum

BS 7799 – ISO 17799 (ISO 27000)

- Első elfogadott szabvány = BS7799 (Brit szabvány)
  - Kidolgozója a Department of Trade and Industry (DTI) – 1995
  - Két elkülönült részt tartalmazott
    - Part 1 = Best Practices for Information Security Management
    - Part 2 = „Information Security Management Systems - Specification with guidance for use.”
      - Bevezette a „ Plan-Do-Check-Act” körkörös, folyamatos munkamenetet
- ISO 17799 = BS7799/1 – átdolgozás utáni – átvétele
  - ISO/IEC 17799 = "Information Technology - Code of practice for information security management” – 2000
  - Ez újabb (jelentős) átdolgozás után = ISO 27002 – 2007
- ISO 27001 = BS7799/2 – átdolgozás utáni – átvétele
  - Az ISO 2005-ben fogadta el

ISO 27000 (bővülő) szabványcsalád

- ISO 27001 – biztonsági kontrollok gyűjteménye
  - Pontos neve: ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements
    - Legújabb verzió: ISO 27001:2013 (Szeptember 25.-től)
    - Magyarország is elfogadta: MSZ ISO/IEC 27001:2006
  - normatív felsorolása az egységes elvek szerint kidolgozott különféle betartandó IT biztonsági kontrolloknak, ez alapján audit végezhető
  - 11 témakörben megfogalmazott, rengeteg kontrollt sorol fel
- ISO 27002 – az IT biztonság áttekintő definíciója
  - Fogalom definíciók és magyarázatok halmaza vezetők számára annak érdekében, hogy ismerjék (és értsék) az ISO 27001 szabványra alapuló tanúsítvány megszerzésének követelményeit
  - A tanúsítás az ISO27001 szabványra alapul
  - Megszerzését követően 3 évig érvényes, ezután megújítandó

NIST 800-xx szabványcsalád (USA)

- Kidolgozója az USA szabványügyi hivatal (NIST)
- Formája: tematikus „kötetek” (Special Publication) (-xx)
- Eredetileg a kormányzat céljára, de civil szféra is követi

1. 800-12 – IT biztonság áttekintése, fogalmak magyarázata, IT biztonság fontosságának hangsúlyozása
2. 800-14 – IT biztonsági alapelvek (8db) és módszerek (14db) áttekintő leírása, amelyek betartása fontos lehet az IBP/IBSZ kidolgozásakor.
3. 800-26 – IT biztonsági ajánlások gyűjteménye főképpen a kockázatok elemzésére/kezelésére vonatkozóan
4. 800-37 (2010) – Módszertani útmutató: "Guide for Applying the Risk Management Framework to Federal Information Systems„
5. 800-53 rev3 (2009) – "Guide for Assessing the Security Controls in Federal Information Systems", 194 biztonsági kontroll az IT rendszerek biztonságosabbá tétele érdekében

ISO 15408 – Common Criteria (CC)

- Aktuális változata = Version 3.1 revision 4.
- A CC nem szervezetet, hanem terméket/szolgáltatást minősít
  - A minősítés célja a termék IT biztonsági tulajdonságainak fokozása
  - Nem a végterméket vizsgálja, hanem a tervezés/előállítás folyamatát
  - Egyaránt vizsgálja a HW és SW komponenseket
  - A CC „betartása” (nagyon) megdrágítja a terméket ⇨ lassan terjed
  - Magyarország is elfogadta: MSZ ISO/IEC 15408:2002
- A CC részei (részletek: Wikipedia – Common Criteria !!!)
  - Target Of Evaluation (TOE) – a kifejlesztendő termék meghatározása
  - Protection Profile (PP) – betartandó biztonsági elvek meghatározása
  - Security Target (ST) – a termék biztonsági tulajdonságainak halmaza
  - Security Functional Requirements (SFR) – biztonsági funkciók listája
  - Security Assurance Requirements (SAR) – biztonsági módszerek listája
  - Evaluation Assurance Level (EAL) – biztonság mértéke EAL 1…7 szint

RFC 2196 – IETF memorandum

- RFC 2196 is memorandum published by Internet Engineering Task Force for developing security policies and procedures for information systems connected on the Internet.
- The RFC 2196 provides a general and broad overview of information security including network security, incident response, or security policies.
- The document is very practical and focusing on day-to-day operations.

- 64 oldalas, gyakorlatias megközelítésű memorandum (emlékeztető), amely IBP/IBSZ kidolgozása során figyelembe veendő szempontok, módszerek, szabályok, ajánlások és tanácsok logikusan rendszerezett tárháza…