MŰEGYETEM 1782

Villamosmérnöki és Informatikai Kar

Dr. Kondorosi Károly
egyetemi docens

A COBIT szabványról

Bemutatkozik az SQI
„A szoftverminőség komplex kérdésköre”
2005. április 15.

iit

MŰEGYETEM 1782

Villamosmérnöki és Informatikai Kar

iit

Mi köze a minőséghez?

- Mennyire biztonságos egy informatikai rendszer?
- Milyen minőségű egy biztonsági rendszer?

Biztonsági szabványok és ajánlások
CC, COBIT ITIL, BS7799
MIBÉTS

Áttekintő szint, inkább filozófia, fő jellemzők

Villamosmérnöki és Informatikai Kar

Tartalom

- IT biztonság és audit
- Common Criteria
  (a biztonság műszaki aspektusból)
- COBIT
  (a biztonság szervezeti aspektusból)
- IT biztonság itthon

Villamosmérnöki és Informatikai Kar

Mi a biztonság?

Általában: védettség fenyegetések ellen

Alapvető emberi szükséglet

Mik a fenyegetések? Mit tehetünk ellenük?

Mennyire bízhatunk az eredményben?

Független, szakszerű vizsgálat, minősítés, tanúsítás – audit

Magunk felé – mások felé

Villamosmérnöki és Informatikai Kar

Informatikai biztonság

INFORMÁCIÓ - erőforrás, értéke van

Biztosítani kell az információ

- rendelkezésre állását
- sértetlenségét
- bizalmasságát
- hitelességét

mindehhez

- az informatikai, illetve információs rendszer működőképességét

Villamosmérnöki és Informatikai Kar

Mit vizsgáljunk?

MŰEGYETEM 1782 Villamosmérnöki és Informatikai Kar iit

Mit vizsgáljunk?

MŰEGYETEM 1782 Villamosmérnöki és Informatikai Kar iit

Mit vizsgáljunk?

- az informatikai rendszert (?)
- a szervezetet (?)

Természetesen mindkettőt érdemes és kell.

(Az IT károkat legalább 60%-ban emberi mulasztás okozza.)

Villamosmérnöki és Informatikai Kar

Tipikus szereposztás

szerződés
specifikál
érdekellentét a teljesítés szintjében

FELHASZNÁLÓ ↔ **SZÁLLÍTÓ**

- információ-tulajdonos
- felelős az értékért
- hiányzó IT szakértelem
- üzemeltet
- bizonyos akar lenni

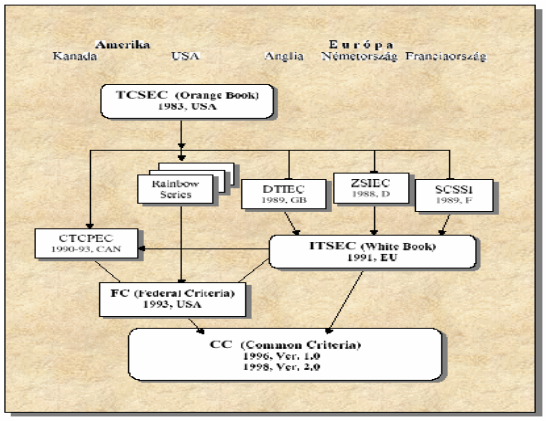
- tervez
- implementál
- átad, követ

AUDITOR

- átvizsgál, mér
- minősít, tanúsít

Villamosmérnöki és Informatikai Kar

Common Criteria



Villamosmérnöki és Informatikai Kar

CC jellemzők

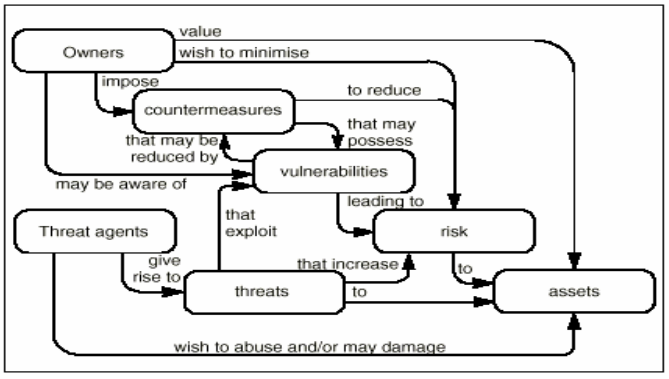
Kiknek szól?
FELHASZNÁLÓ – FEJLESZTŐ – AUDITOR

Műszaki szemlélet
- Környezet, jogi háttér, szervezet:
- Kapcsolatot megmutat, de nem tárgya

MODELL – FUNKCIONÁLIS – GARANCIA
követelmények

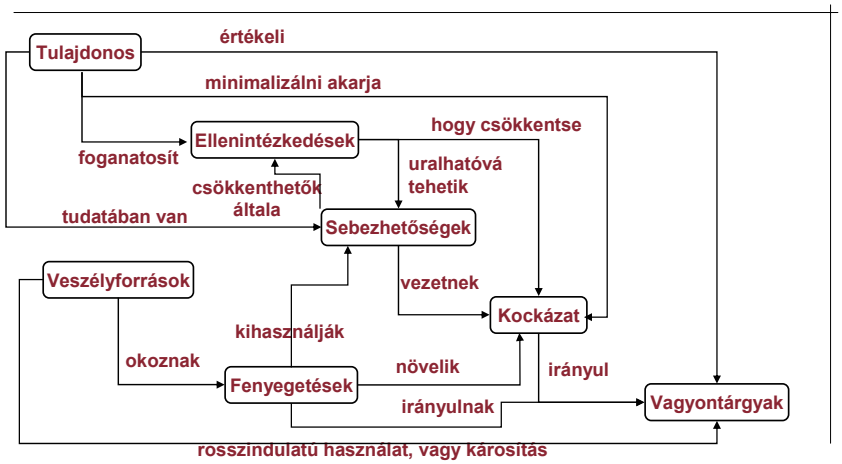
Villamosmérnöki és Informatikai Kar

CC modell



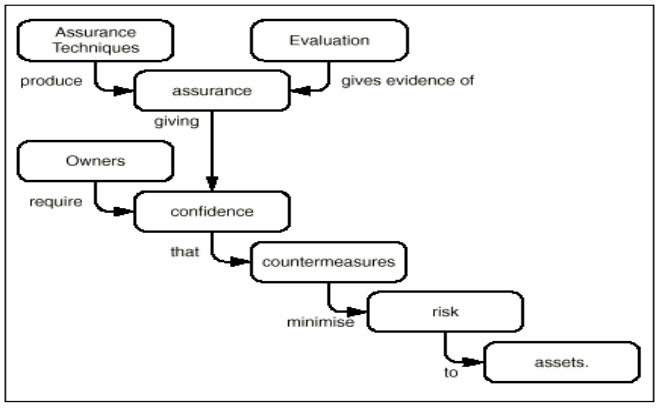
Villamosmérnöki és Informatikai Kar

CC modell



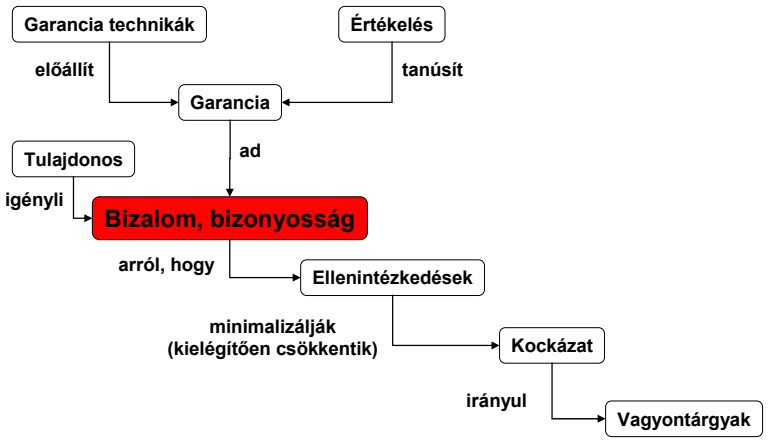
Villamosmérnöki és Informatikai Kar

CC értékelés



Villamosmérnöki és Informatikai Kar

CC értékelés



Villamosmérnöki és Informatikai Kar

Funkcionális követelmények

- **Class FAU:** ***Security audit***
- **Class FCO:** ***Communication***
- **Class FCS:** ***Cryptographic support***
- **Class FDP:** ***User data protection***
- **Class FIA:** ***Identification and authentication***
- **Class FMT:** ***Security management***
- **Class FPR:** ***Privacy***
- **Class FPT:** ***Protection of the TSF***
- **Class FRU:** ***Resource utilisation***
- **Class FTA:** ***TOE access***
- **Class FTP:** ***Trusted path/channels***

Villamosmérnöki és Informatikai Kar

Garancia-követelmények

- **Class ACM:** ***Configuration management***
- **Class ADO:** ***Delivery and operation***
- **Class ADV:** ***Development***
- **Class AGD:** ***Guidance documents***
- **Class ALC:** ***Life cycle support***
- **Class ATE:** ***Tests***
- **Class AVA:** ***Vulnerability assessment***
- **Class AMA:** ***Maintenance of assurance***

Villamosmérnöki és Informatikai Kar

Mit lehet értékelni?

- *Védelmi profil* értékelés
  teljes, konzisztens, technikailag megfelelő
- *Biztonsági specifikáció* értékelés
  - teljes, konzisztens, technikailag megfelelő
  - megfelel a *védelmi profilnak*
- *ÉT* értékelés (értékelés tárgya)
  megfelel a *biztonsági specifikációnak*
- Garancia-karbantartás
  ÉT a módosítások után is megfelel

MŰEGYETEM 1782 Villamosmérnöki és Informatikai Kar iit

Mi adhat erősebb garanciát?

- Több, erősebb (magasabb szintű) követelmény
- Kimerítőbb értékelés
  - terjedelem
  - mélység
  - szigorúság

MŰEGYETEM 1782 Villamosmérnöki és Informatikai Kar iit

Garanciaszintek

1. funkcionálisan tesztelt
2. strukturálisan tesztelt
3. módszeresen tesztelt és bevizsgált
4. módszeresen tervezett, tesztelt és átvizsgált
5. félformálisan tervezett és tesztelt
6. félformálisan verifikált tervezés és tesztelt
7. formálisan verifikált tervezés és tesztelt

Villamosmérnöki és Informatikai Kar

COBIT

- **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology
- **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation (ISACA)
  - 1969: EDP Auditors Association
- Certified Information Systems Auditor (CISA)

Villamosmérnöki és Informatikai Kar

COBIT jellemzők

Kiknek szól?
VEZETŐK – FEKHASZNÁLÓK – AUDITOR

Üzleti szemlélet – pénzügyi szektor

Dokumentum-család

IT része az üzleti stratégiának

Villamosmérnöki és Informatikai Kar

COBIT modell

- Témakörök:
  - PO: Planning and Organisation
  - AI: Acquisition and Implementation
  - DS: Delivery and Support
  - M: Monitoring
- Ezeken belül 34 folyamat

Villamosmérnöki és Informatikai Kar

COBIT család

- Magas szintű => Framework
  - 4 domain – 34 folyamat
- Részletes => Detailed Control Objectives
  - 3-30 részletes intézkedés folyamatonként
  - összesen 318
- Audit => Audit Guidelines
  - ellenőrzési javaslatok a 34 folyamatra
- Vezetői segítség => Management Guidelines
  - célok és mutatók a 34 folyamathoz

Villamosmérnöki és Informatikai Kar

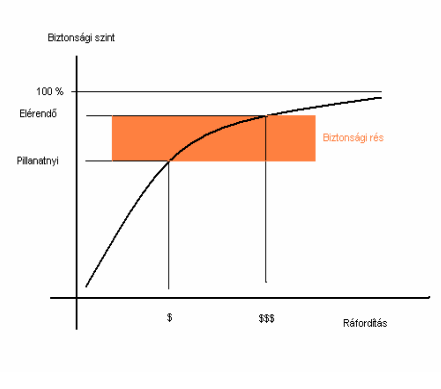
Fontos témakörök

- Kockázatkezelés
- A szervezet és az emberi tényező
- Az infrastruktúra
- Az adat
- A folyamatos üzem

Villamosmérnöki és Informatikai Kar

Kockázat

- A biztonsági rés → „megéri-e?”
- Kockázati elemek:
  - Vagyontárgy (assests)
  - Sebezhetőség (vulnerabilities)
  - Fenyegetettség (threats)
  - Hatás (impacts)
  - Kockázat (risks)
  - Fennmaradó kockázat (residual risk)



Villamosmérnöki és Informatikai Kar

Biztonsági cél

Olyan állapot elérése, amelyben
– a kockázatok
– megvalósítható és értékarányos védelmi intézkedésekkel
– elviselhető mértékűre csökkenthetők.

Az üzleti célok elérhetőségének biztosítása a vezetőség által kívánt mértékben

Villamosmérnöki és Informatikai Kar

Érettségi szintek

- **0 Non-Existent**. Fel sem ismert problémák.
- **1 Initial**. Felismert problémák, de csak ad-hoc módszerek egyéni esetekben. A vezetés szervezetlen.
- **2 Repeatable**. Különböző személyek által végzett, független folyamatok. A felelősség az egyéneké, és a cég függ az egyéntől.
- **3 Defined**. Szabványosított, dokumentált és betanított, de nem ellenőrzött és nem számonkért egyszerű folyamatok, melyek csak a meglévő szokásokat rögzítik.
- **4 Managed**. Lehetséges a folyamatok ellenőrzése és intézkedések történnek eltérés esetén, de nincs automatizmus.
- **5 Optimised**. Integrált és automatizált folyamatok a legjobbnak elismert módszer szerint. Gyors alkalmazkodás a változó igényekhez.

Villamosmérnöki és Informatikai Kar

IT biztonság itthon

- Terminológia (alakul)
- ITB ajánlások
- Több kisebb-nagyobb cég
- MIBÉTS
  (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma)
  http://www.itktb.hu
- COBIT
  ISACA magyar tagozat
  PSZÁF

Villamosmérnöki és Informatikai Kar

Köszönöm a figyelmet.