




Dr. Kondorosi Károly
egyetemi docens


A COBIT szabványról



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



Villamosmérnöki és Informatikai Kar




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
2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 2



Tartalom

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

2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 3



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

2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 4



Informatikai biztonság

INFORMÁCIÓ - erőforrás, értéke van

Biztosítani kell az információ

- rendelkezésre állását
- sértetlenségét
- bizalmasságát
- hitelességét

mindehhez

- az informatikai, illetve információs rendszer működőképességét

2005. április 15.

Bemutató az SQI

KK: A COBIT szabványról - 5



Mit vizsgáljunk?



2005. április 15.

Bemutató az SQI



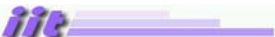
KK: A COBIT szabványról - 6

Mit vizsgáljunk?



2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 7

Mit vizsgáljunk?

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

Természetesen mindkettőt érdemes és kell.

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

2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 8





Villamosmérnöki és Informatikai Kar



Tipikus szereposztás

szervződés
specifikál
érdekelletét a teljesítés szintjében



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


- tervez
- implementál
- átad, követ


AUDITOR

2005. április 15.


Bemutakozik az SQI

KK: A COBIT szabványról - 9

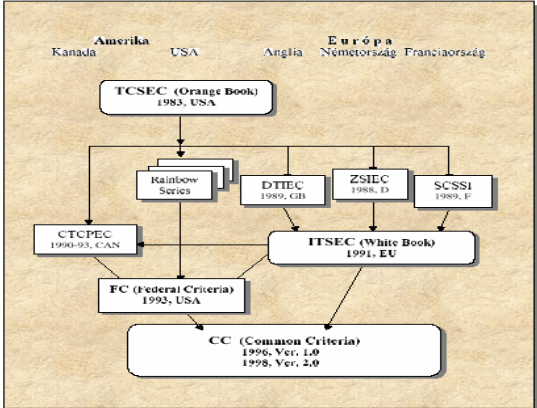




Villamosmérnöki és Informatikai Kar



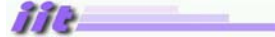
Common Criteria



2005. április 15.

Bemutakozik az SQI

KK: A COBIT szabványról - 10



CC jellemzők

Kiknek szól?

FELHASZNÁLÓ – FEJLESZTŐ – AUDITOR

Műszaki szemlélet

Környezet, jogi háttér, szervezet:

Kapcsolatot megmutat, de nem tárgya

MODELL – FUNKCIONÁLIS – GARANCIA
követelmények

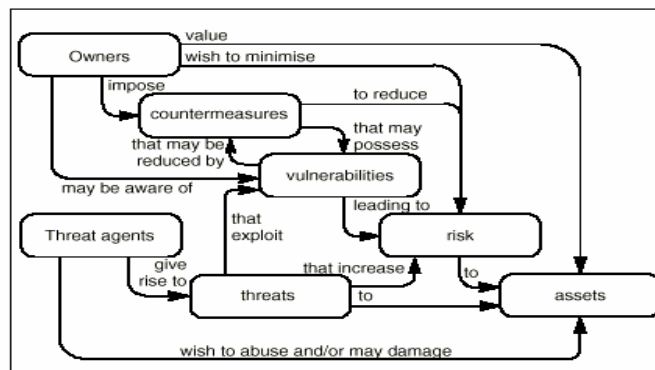
2005. április 15.

Bemutakozik az SQI

KK: A COBIT szabványról -
11



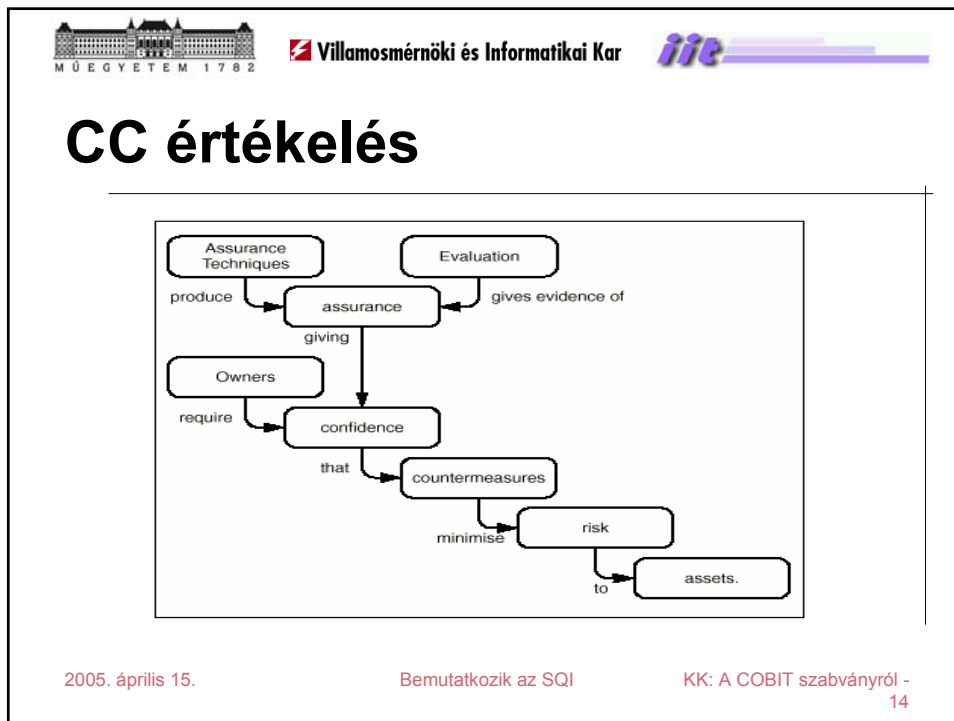
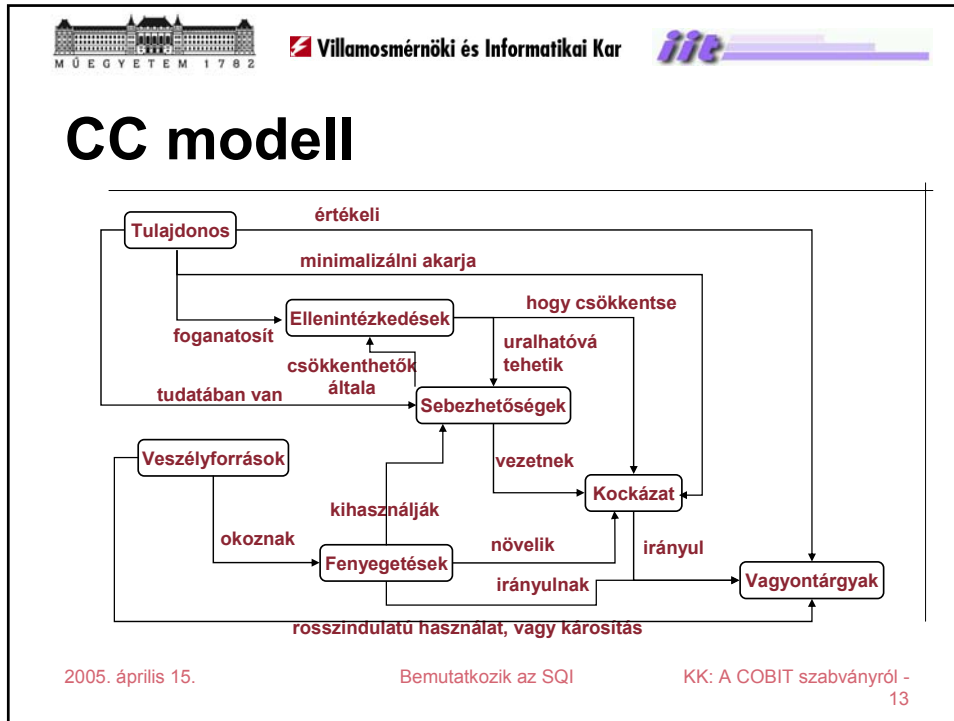
CC modell



2005. április 15.

Bemutakozik az SQI

KK: A COBIT szabványról -
12



MŰEGYETEM 1782 Villamosmérnöki és Informatikai Kar *ite*

CC értékelés

```
graph TD; GT[Garancia technikák] -- előállít --> G[Garancia]; E[Értékelés] -- tanúsít --> G; T[Tulajdonos] -- igényli --> BB[Bizalom, bizonyosság]; G -- ad --> BB; BB -- arról, hogy --> EL[Ellenintézkedések]; EL -- minimalizálják (kielégítően csökkentik) --> K[Kockázat]; K -- irányul --> V[Vagyontárgyak];
```


2005. április 15. Bemutkozik az SQI KK: A COBIT szabványról - 15

MŰEGYETEM 1782 Villamosmérnöki és Informatikai Kar *ite*

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*


2005. április 15. Bemutkozik az SQI KK: A COBIT szabványról - 16



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

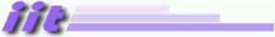
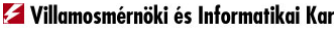

2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 17



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-kezelés**
ÉT a módosítások után is megfelel

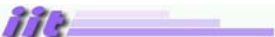


2005. április 15. Bemutató az SQI KK: A COBIT szabványról - 18



Mi adhat erősebb garanciát?

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



2005. április 15.Bemutató az SQIKK: A COBIT szabványról - 19



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


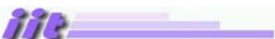
2005. április 15.Bemutató az SQIKK: A COBIT szabványról - 20

**Villamosmérnöki és Informatikai Kar**

COBIT

- **Control Objectives for Information and Related Technology**
- **Information Systems Audit and Control Association (ISACA)**
1969: EDP Auditors Association
- **Certified Information Systems Auditor (CISA)**

2005. április 15.Bemutakozik az SQIKK: A COBIT szabványról -
21

**Villamosmérnöki és Informatikai Kar**

COBIT jellemzők


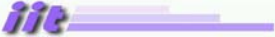
Kiknek szól?
VEZETŐK – FEKHASZNÁLÓK – AUDITOR

Üzleti szemlélet – pénzügyi szektor

Dokumentum-család

IT része az üzleti stratégiának



2005. április 15.Bemutakozik az SQIKK: A COBIT szabványról -
22

**Villamosmérnöki és Informatikai Kar**

COBIT modell

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

2005. április 15.Bemutató az SQIKK: A COBIT szabványról -
23

**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

2005. április 15.Bemutató az SQIKK: A COBIT szabványról -
24

MŰEGYETEM 1782 **Villamosmérnöki és Informatikai Kar** *ite*

Fontos témakörök

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

2005. április 15. Bemutakozik az SQI KK: A COBIT szabványról - 25

MŰEGYETEM 1782 **Villamosmérnöki és Informatikai Kar** *ite*

Kockázat

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

2005. április 15. Bemutakozik az SQI KK: A COBIT szabványról - 26



Biztonsági cél

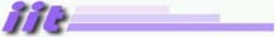
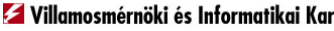

- Olyan állapot elérése, amelyben
- a kockázatok
 - megvalósítható és értékarányos védelmi intézkedésekkel
 - elviselhető mértékűre csökkenthetők.

Az üzleti célok elérhetőségének biztosítása a vezetés által kívánt mértékben



Érettségi szintek


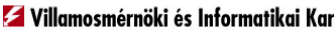

- **0 Non-Existent.** Fel sem ismert problémák.
- **1 Initial.** Felismert problémák, de csak ad-hoc módszerek egyéni esetekben. A vezetés szervezetlen.
- **2 Repeatable.** Különböző személyek által végzett, független folyamatok. A felelősség az egyénké, és a cég függ az egyéntől.
- **3 Defined.** Szabványosított, 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 történnék eltérés esetén, de nincs automatizmus.
- **5 Optimised.** Integrált és automatizált folyamatok a legjobbnak elismert módszer szerint. Gyors alkalmazkodás a változó igényekhez.



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

2005. április 15. Bemutató az SQI KK: A COBIT szabványról -
29



Köszönöm a figyelmet.

2005. április 15. Bemutató az SQI KK: A COBIT szabványról -
30