SZÁMÍTÁSTECHNIKAI AUDIT

Common Criteria
1

Mi a biztonság?

Általában: védettség fenyegetések ellen

Alapvető emberi szükséglet

Mik a fenyegetések? Mit tehetünk ellenük?
Mennyire bízhatunk az eredményben?

Specifikusan: informatikai biztonság

Mit vonunk vizsgálat alá?

- ***az informatikai rendszert***
- a szervezetet

Informatikai biztonság - 1

INFORMÁCIÓ - erőforrás, értéke van

Biztosítani kell az információ

- **rendelkezésre állását**
- **sértetlenségét**
- **bizalmasságát**
- **hitelességét**

mindehhez

- a teljes informatikai, illetve információs rendszer működőképességét

Informatikai biztonság - 2

Rendelkezésre állás

- specifikáció szerinti működés
- funkciókra, adatokra értelmezhető

Sértetlenség - integritás

- csak jogosultak változtathatnak, véletlenül sem változik, teljes, korrekt

Bizalmasság

- csak a jogosultak érhetik el - (privacy)

Hitelesség

- források, partnerek, szereplők azonosíthatósága

Informatikai biztonság - 3

A biztonság megteremtése érdekében feladatok határozhatók meg

- a tervezésre
- a bevezetésre
- az üzemeltetésre
- maguknak a feladatoknak a kezelésére

vonatkozóan

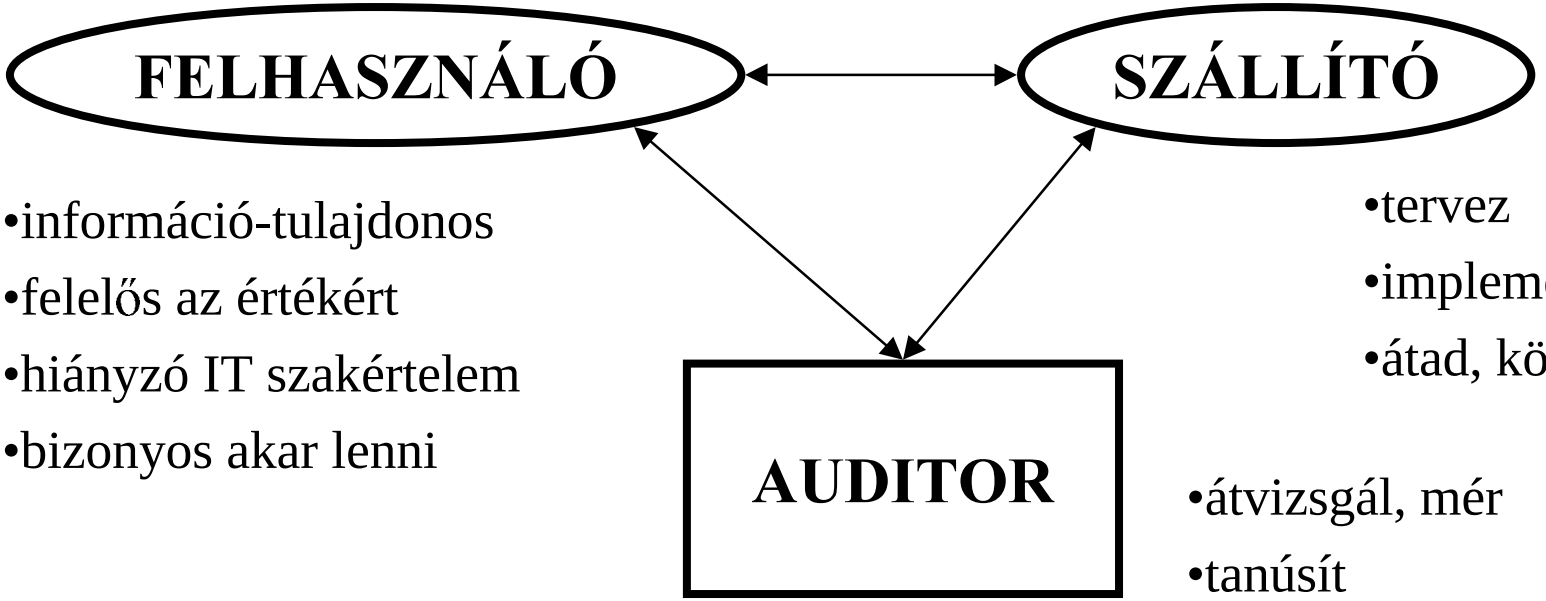
Mennyire vagyunk biztonságban? -1

Tipikus szereposztás

szerződés

•specifikál

•érdekellentét a teljesítés szintjében



•információ-tulajdonos

•felelős az értékért

•hiányzó IT szakértelem

•bizonyos akar lenni

•tervez

•implementál

•átad, követ

•átvizsgál, mér

•tanúsít

Mennyire vagyunk biztonságban?

– Hogyan specifikáljunk (felhasználó)?
– Hogyan tervezzünk (fejlesztő)?
– Hogyan mérjünk (auditor)?

Cél

- összehasonlíthatóság
- megismételhetőség
- objektivitás

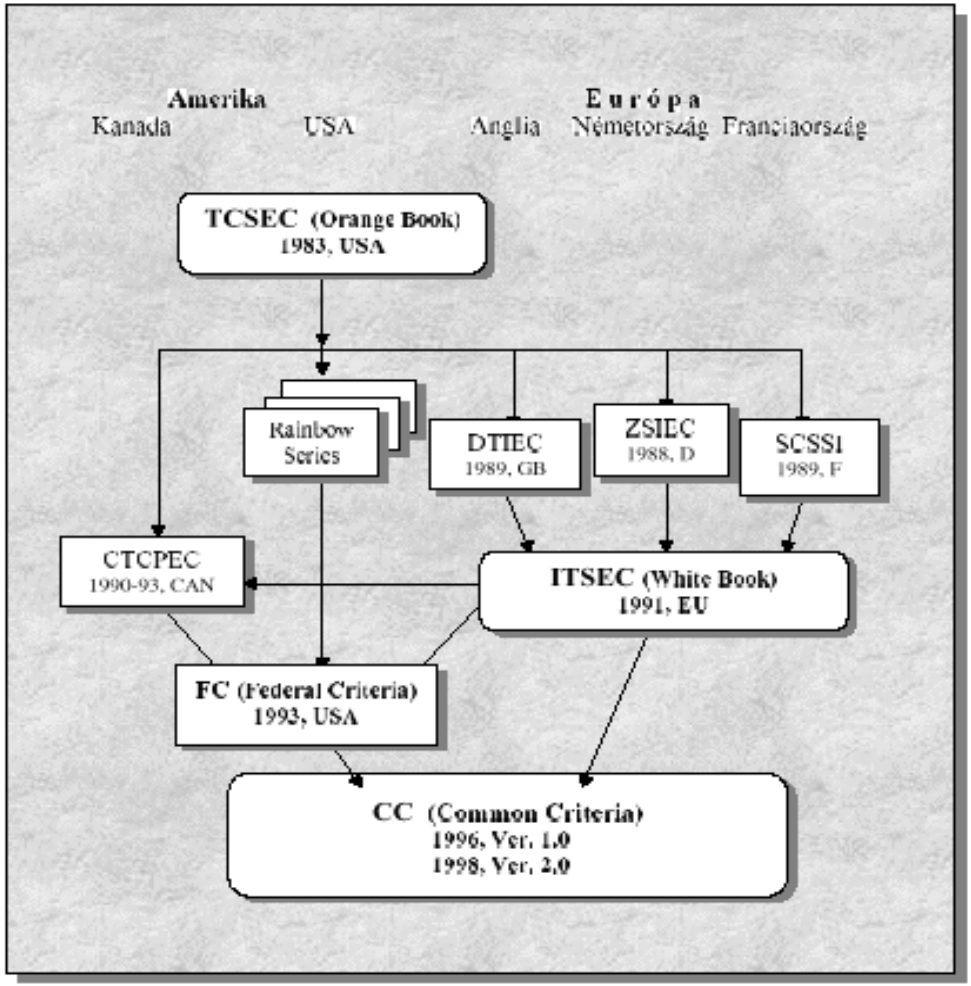
Kellenek

- közös modellek és fogalomrendszer
- mértékek
- minősítési (mérési) eljárások

A minősítés megközelítései

- Trusted Computer System Evaluation Criteria (TCSEC, USA) - 1983
- Information Technology Security Evaluation Criteria (ITSEC, EU) - 1991
- Common Risk Analysis and Management Method (CRAMM - CCTA, UK) - 1991
- Canadian Trusted ... (CTCPEC, Kanada) - 1993
- Federal Criteria for Information Technology Security (FC 1.0, USA) - 1993
- Common Criteria (CC 1.0, közös) - 1996
- ISO/IEC 15408-1 - 1999
- Magyarország: ITB ajánlások (pl. 8. 1994)

A megközelítések származása



Common Criteria

- 1993-tól, jelenleg: CC 2.1

  http://csrc.nist.gov/cc

- Támogatók:

  Kormányzati szervezetek (hatóságok)
  - Egyesült Államok (2 szervezet)
  - Egyesült Királyság
  - Franciaország
  - Hollandia
  - Kanada
  - Németország

  CC Implementation Board (CCIB)

Kiknek szól a CC?

- Felhasználóknak
  - specifikáció
  - termékösszehasonlítás
- Fejlesztőknek (szállítóknak)
  - felkészülés a minősítésre
  - a felhasználóval kölcsönösen elfogadott bázis
  - kellenek az értékelést támogató funkciók is
- Értékelőknek (auditoroknak)
  - ad végrehajtandó lépéseket és biztonsági funkciókat
  - nem ad folyamatot, jogi kereteket

A CC felépítése

3 kötet

- Bevezetés és általános modell
- Funkcionális követelmények
- Garancia (assurance) követelmények

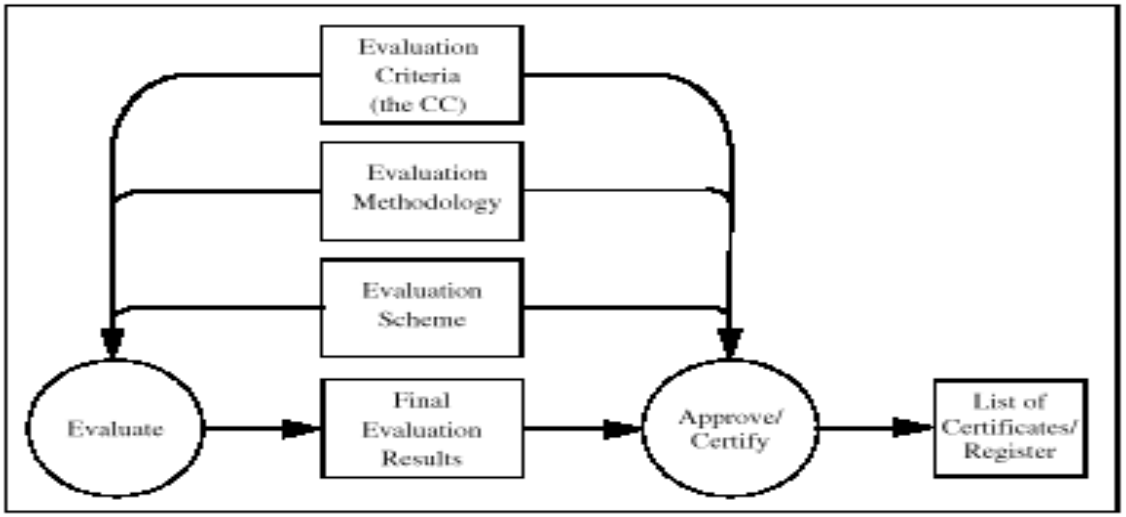
2. és 3. katalógus jellegű - függelékben magyarázatok

Bővítés, származtatás szabályai

Félformális leírás

Ontológiai megközelítés

A biztonság értékelésének kontextusa

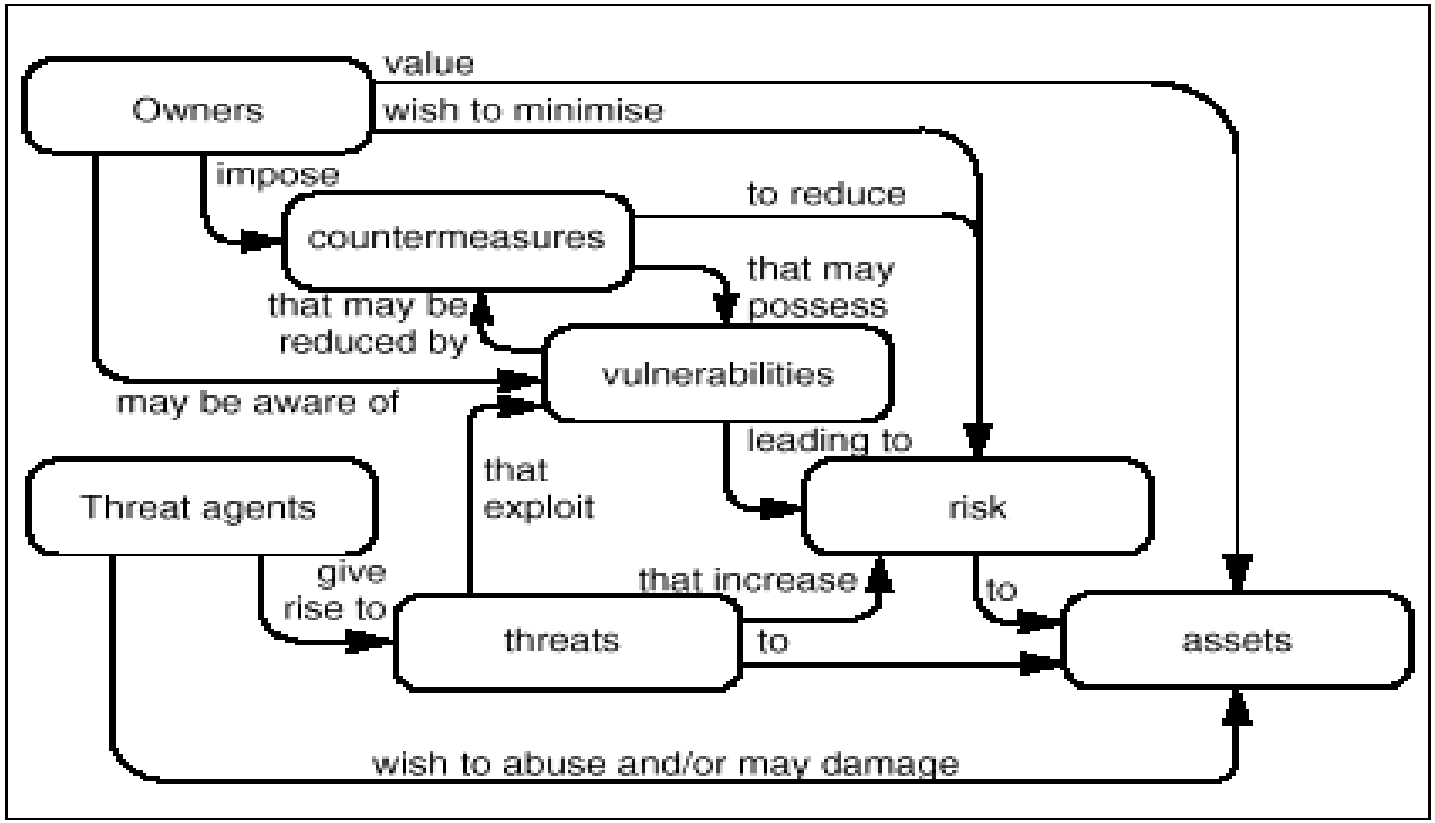


CC a kritériumokat adja

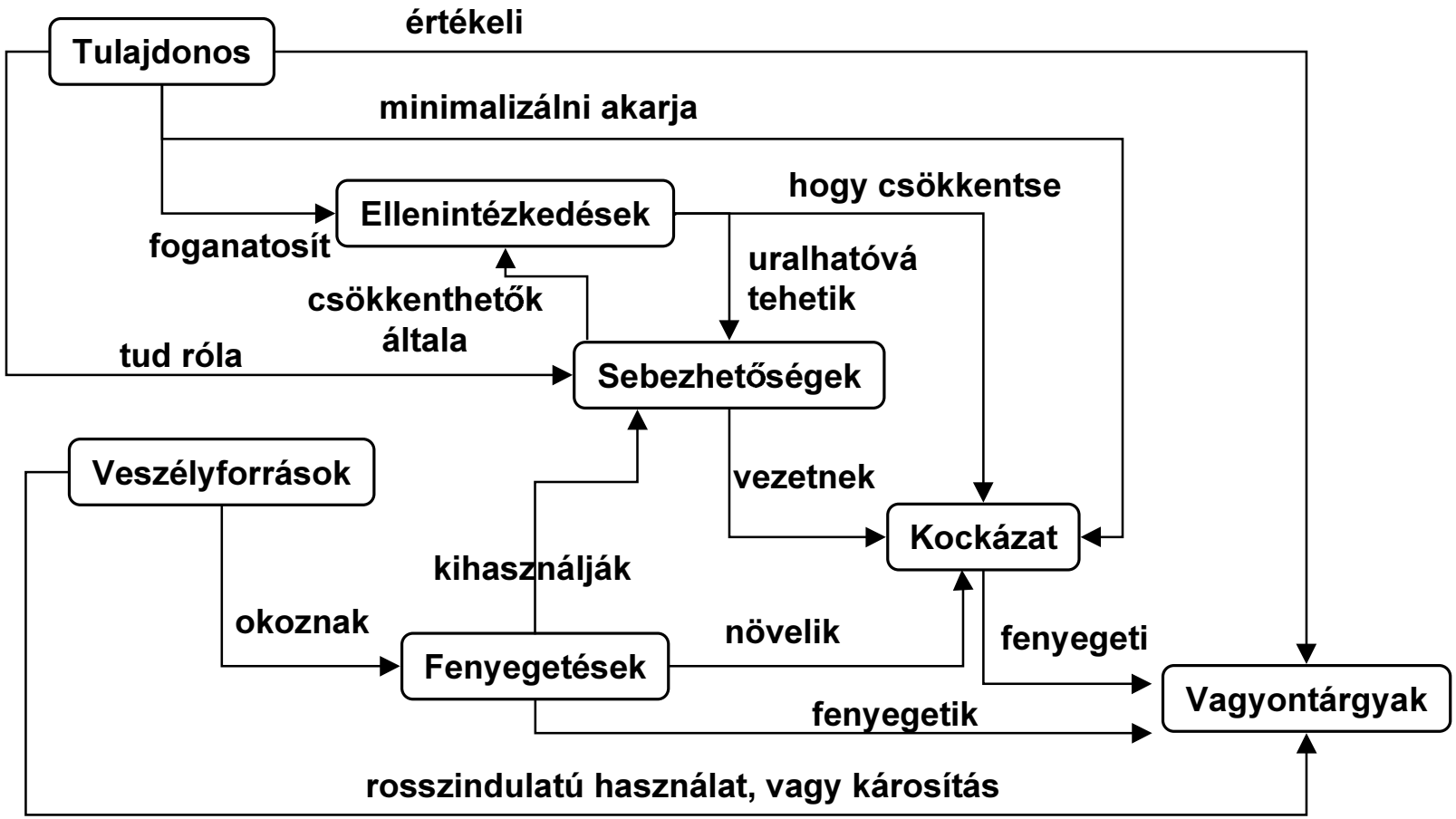
A folyamat és a jogi keretek is kellenek

Maradnak bizonytalanságok - értékelés elfogadása - tanúsítás

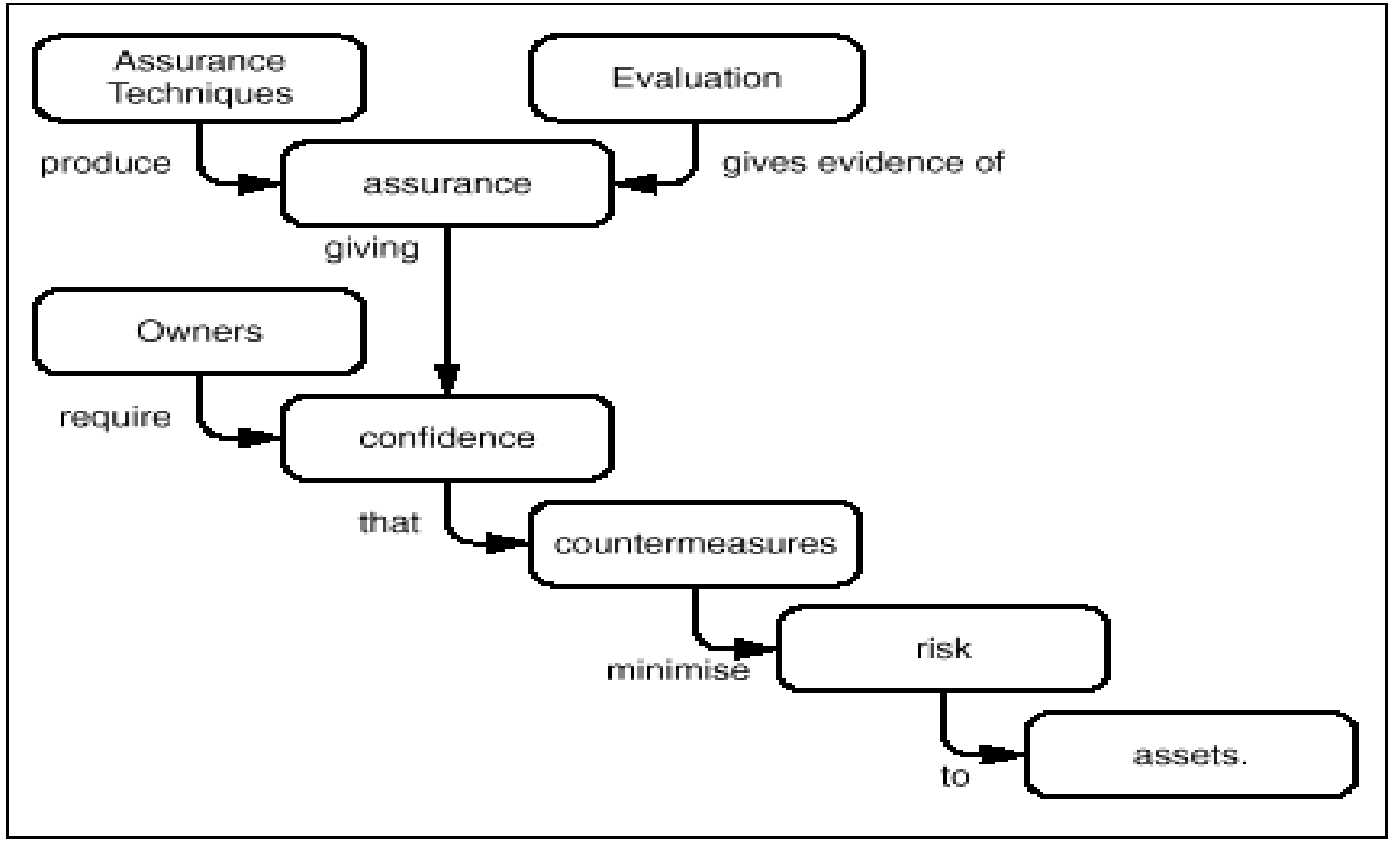
Alapfogalmak és kapcsolataik



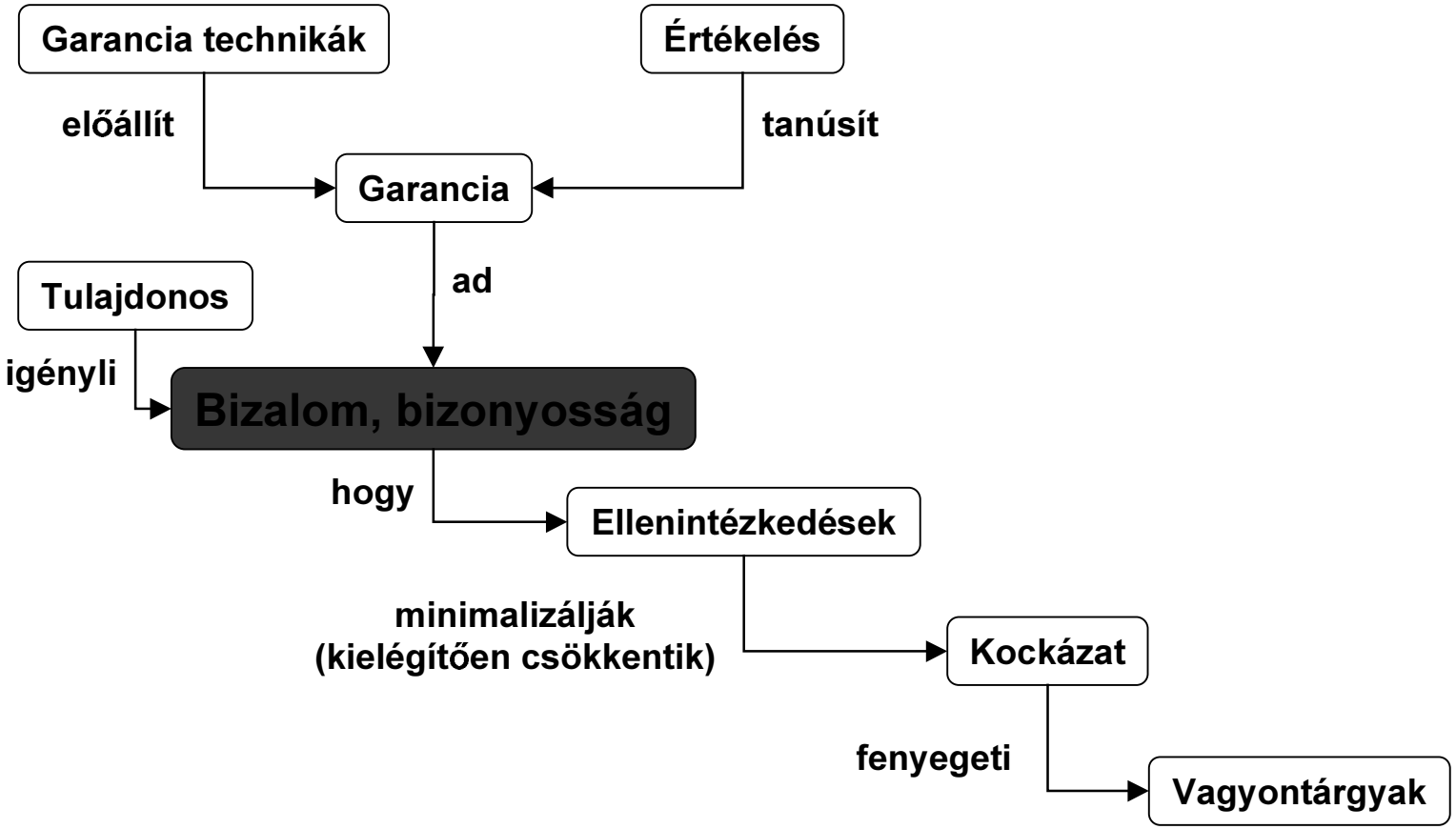
Alapfogalmak és kapcsolataik



Az értékelés fogalmai és kapcsolataik



Az értékelés fogalmai és kapcsolataik



Terminológia

- **CC -** Közös követelményrendszer IT biztonságértékeléshez
- **BF -** Biztonsági funkció
- **(BFP -** Biztonsági funkció politika)
- **BS -** Biztonsági specifikáció
- **ÉGSZ -** Értékelési garanciaszint
- **ÉT -** Értékelés tárgya
- **ÉTBF -** ÉT Biztonsági funkciói
- **ÉTBFH -** ÉTBF hatóköre
- **ÉTBFK -** ÉTBF interfészek
- **ÉTBP -** ÉT biztonságpolitikája
- **IT -** Információtechnológia
- **VP -** Védelmi profil

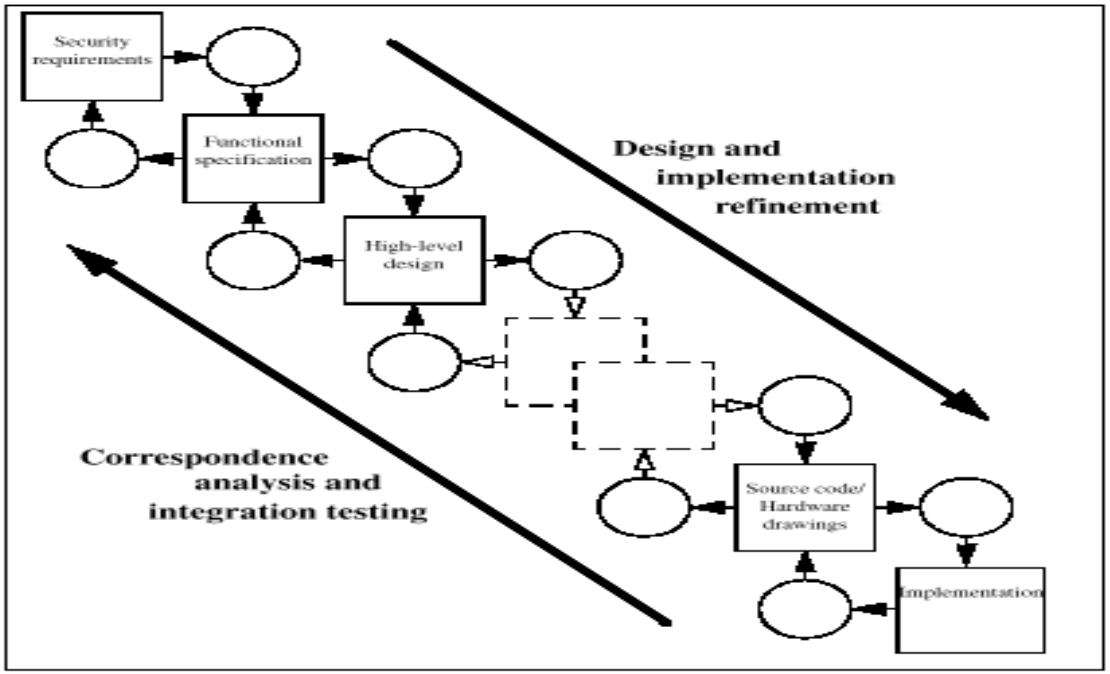
- **CC -** Common Criteria for IT Security Evaluation
- **SF -** Security Function
- **(SFP -** Security Function Policy)
- **ST -** Security Target
- **EAL -** Evaluation Assurance Level
- **TOE -** Target of Evaluation
- **TSF -** TOE Security Function
- **TSC -** TSF Scope of Control
- **TSFI -** TSF Interfaces
- **TSP -** TOE Security Policy
- **IT -** Information Technology
- **PP -** Protection Profile

CC megközelítés

Fázisok a biztonság megteremtése szempontjából

- fejlesztés
- értékelés
- üzemeltetés

Tervezés

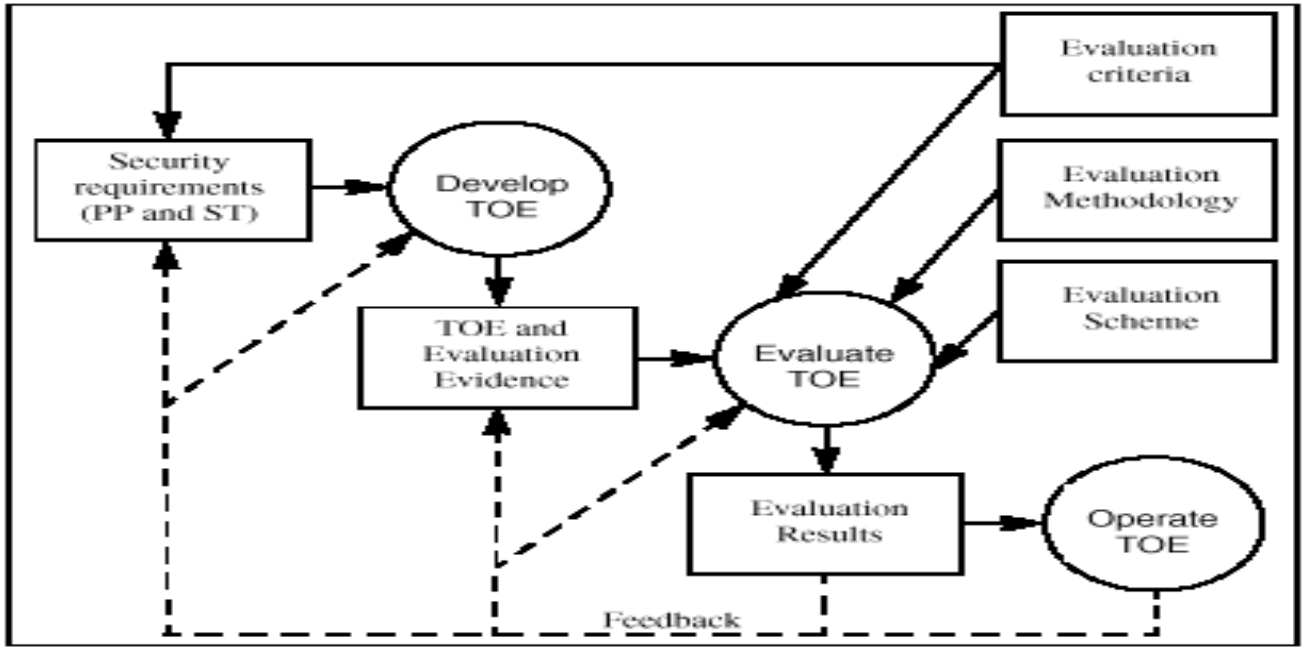


Nincs előírt életciklus modell és tervreprezentáció

Követelmények finomítása

- minden szint implementálja a fölötte lévőt
- nem vezet be új követelményt (szempontot)

Értékelés



Eredmény: értékelési jelentések
megfelelés egy értékelési garancia-szintnek

Az értékelés közvetlen, illetve közvetve visszahat a termékre

Üzemeltetés

- Tapasztalatok (ÉT vagy környezete)
- Visszacsatolás
- Újraértékelést eredményezhet (részleges vagy teljes)
- CC elvárja a garancia-karbantartást, de folyamatait nem részletezi

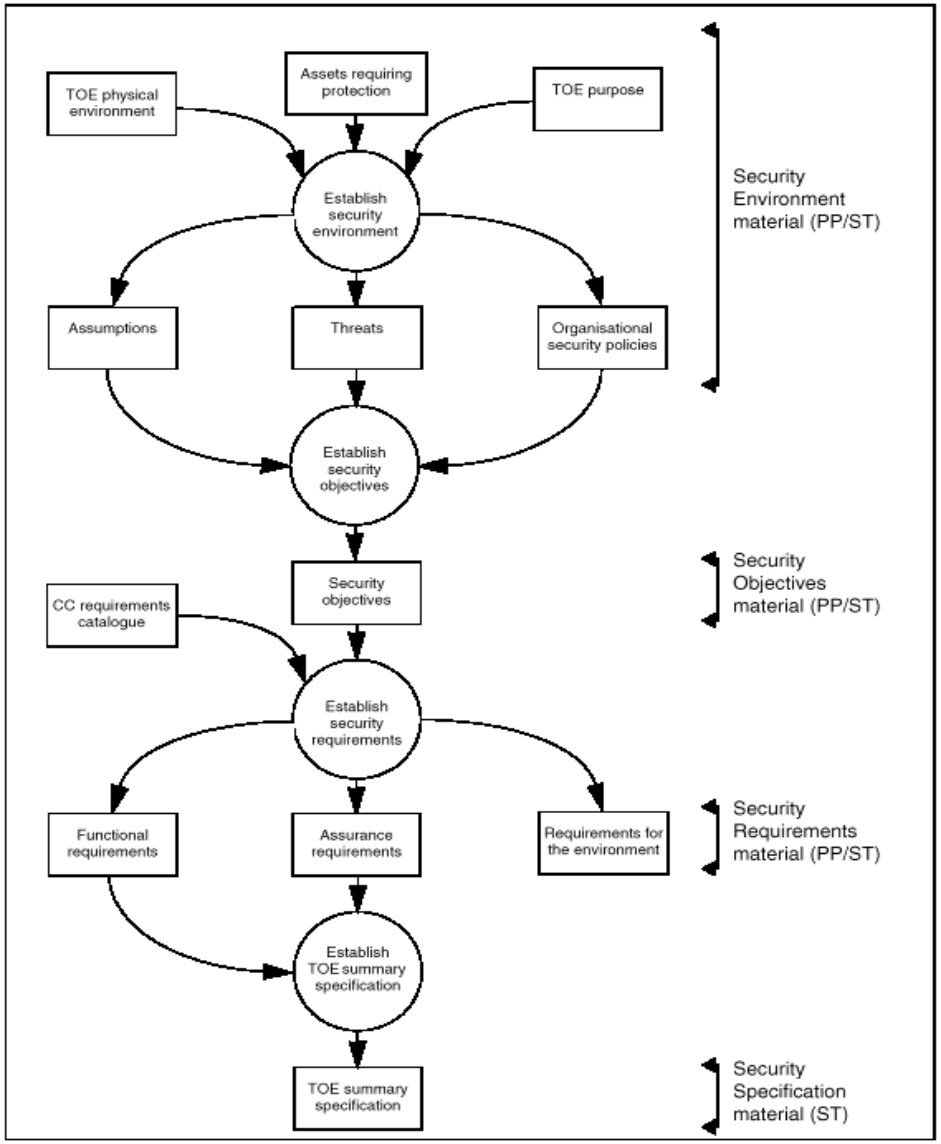
Követelmények és specifikációk származtatása

Rétegmodell

- Környezet
- Célok
- Követelmények
- Specifikáció

Védelmi profil

Biztonsági specifikáció

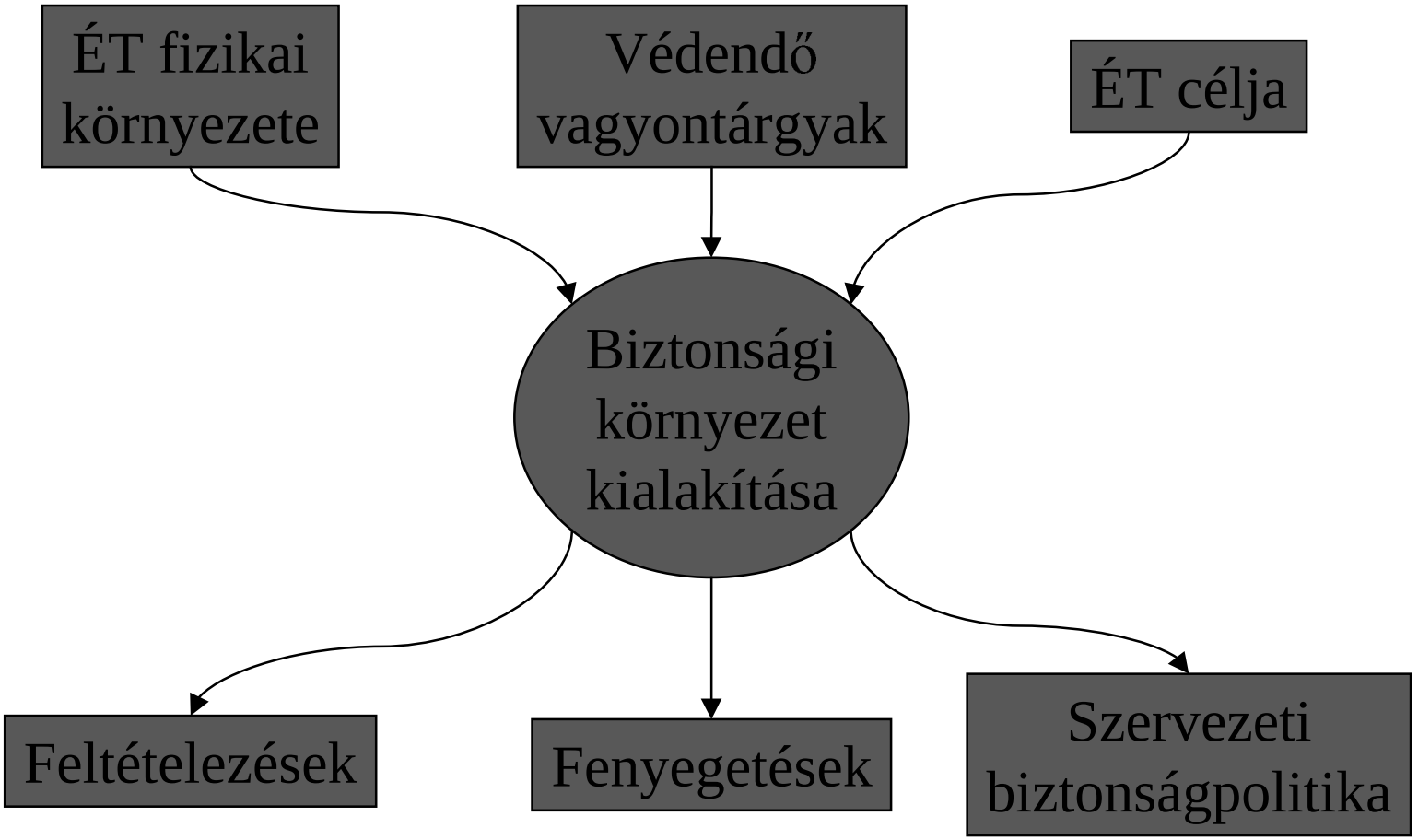


Biztonsági környezet

Tartalmazza:

- az összes releváns törvényt
- szervezeti biztonságpolitikai dokumentumot
- szokást, gyakorlatot és tudást
- az összes veszélyt, ami jelen van, vagy várhatóan jelen lesz a környezetben

Biztonsági környezet



Biztonsági környezet

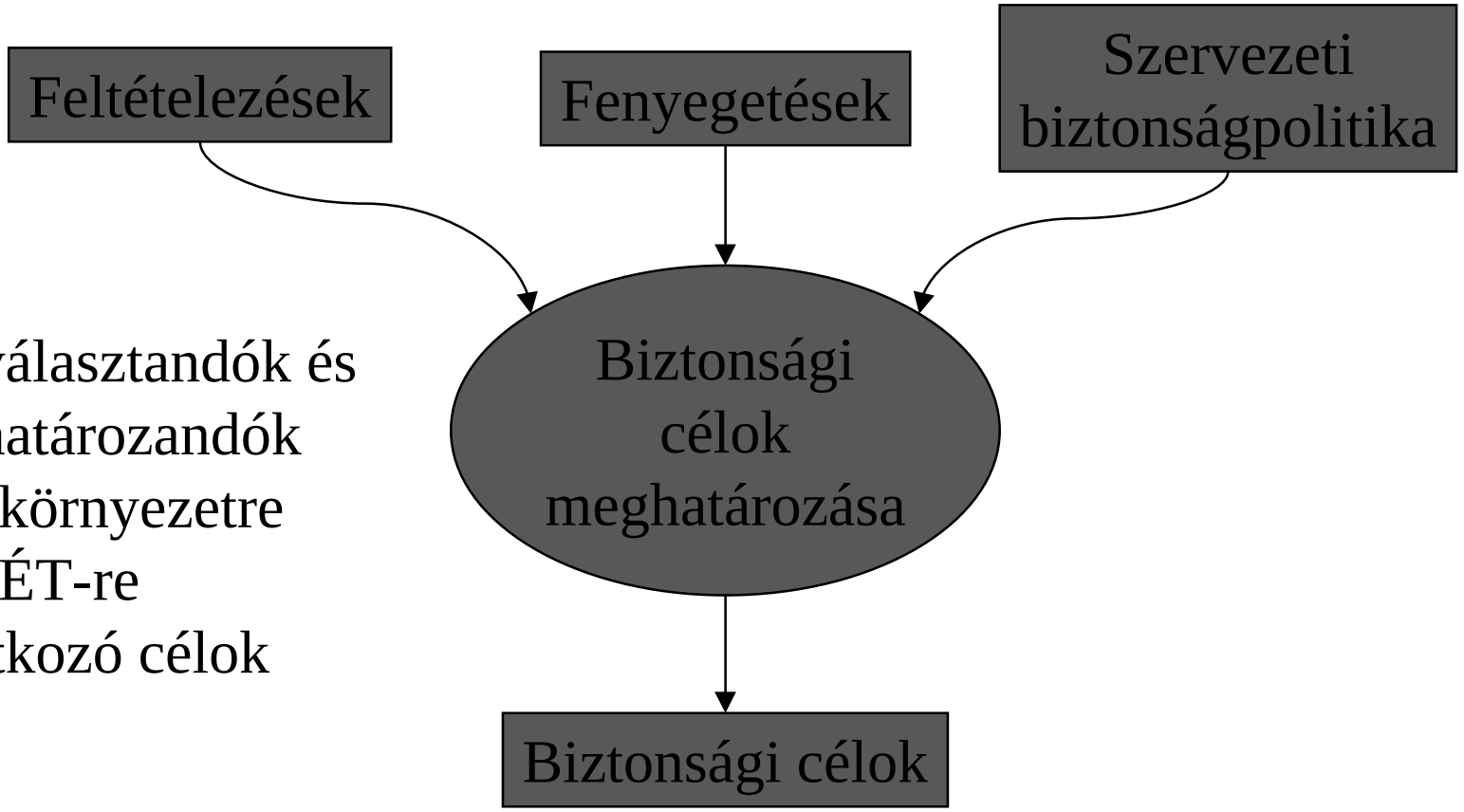
Környezet specifikációjához számbavenni

- az ÉT fizikai környezetét
- védelmet igénylő vagyontárgyakat (közvetlen, pl. adatbázis, ...; közvetett. pl. jogosultságok, ÉT implementáció, ...)
- az ÉT célját, a szándékolt felhasználást

Rögzítendő

- Környezeti feltételek, elvárások
- Feltárt fenyegetések, lehetséges támadások, valószínűségekkel, következményekkel
- Szervezeti biztonságpolitika alkalmazható elemei

Biztonsági célok

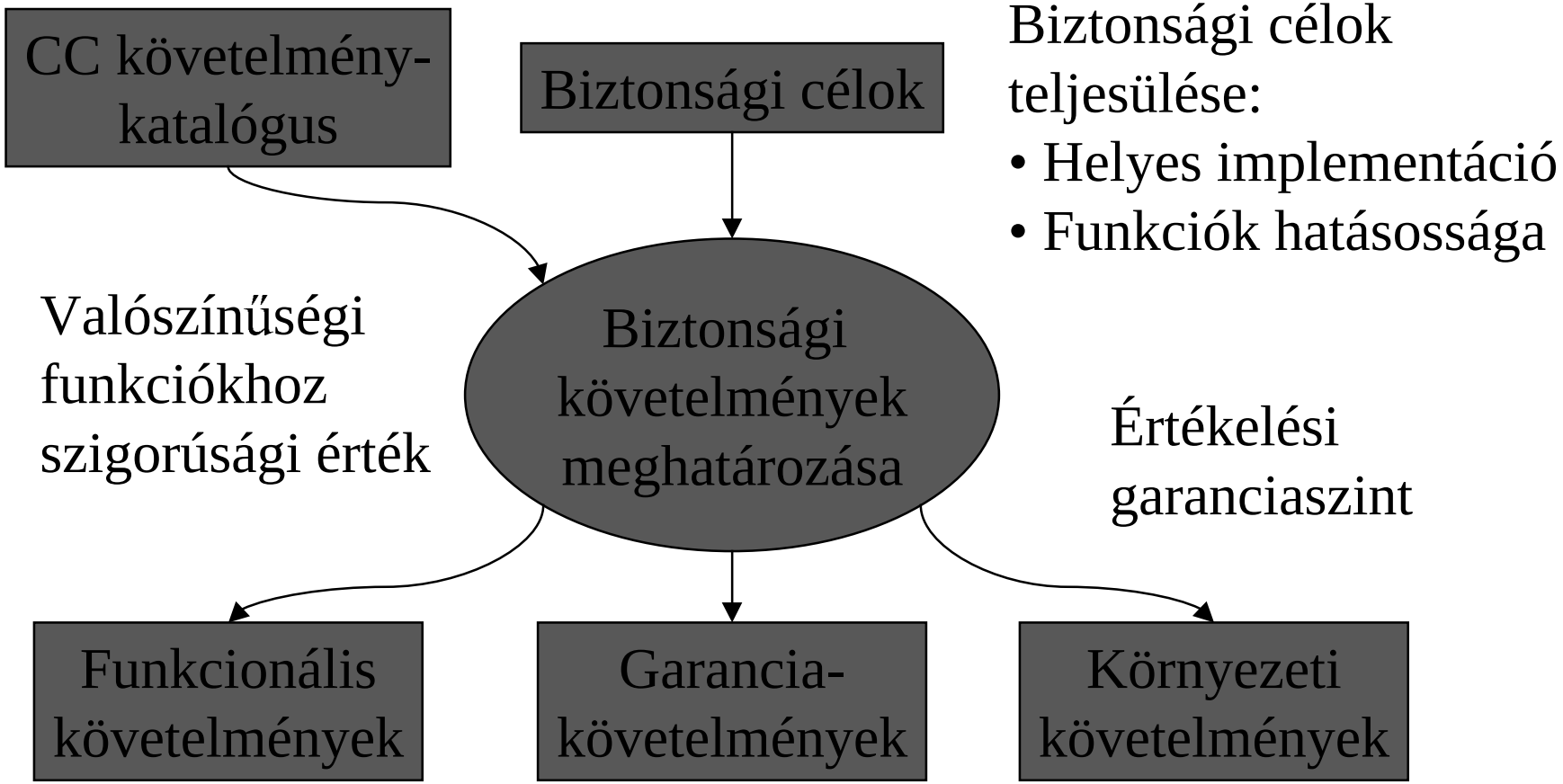


Szétválasztandók és meghatározandók

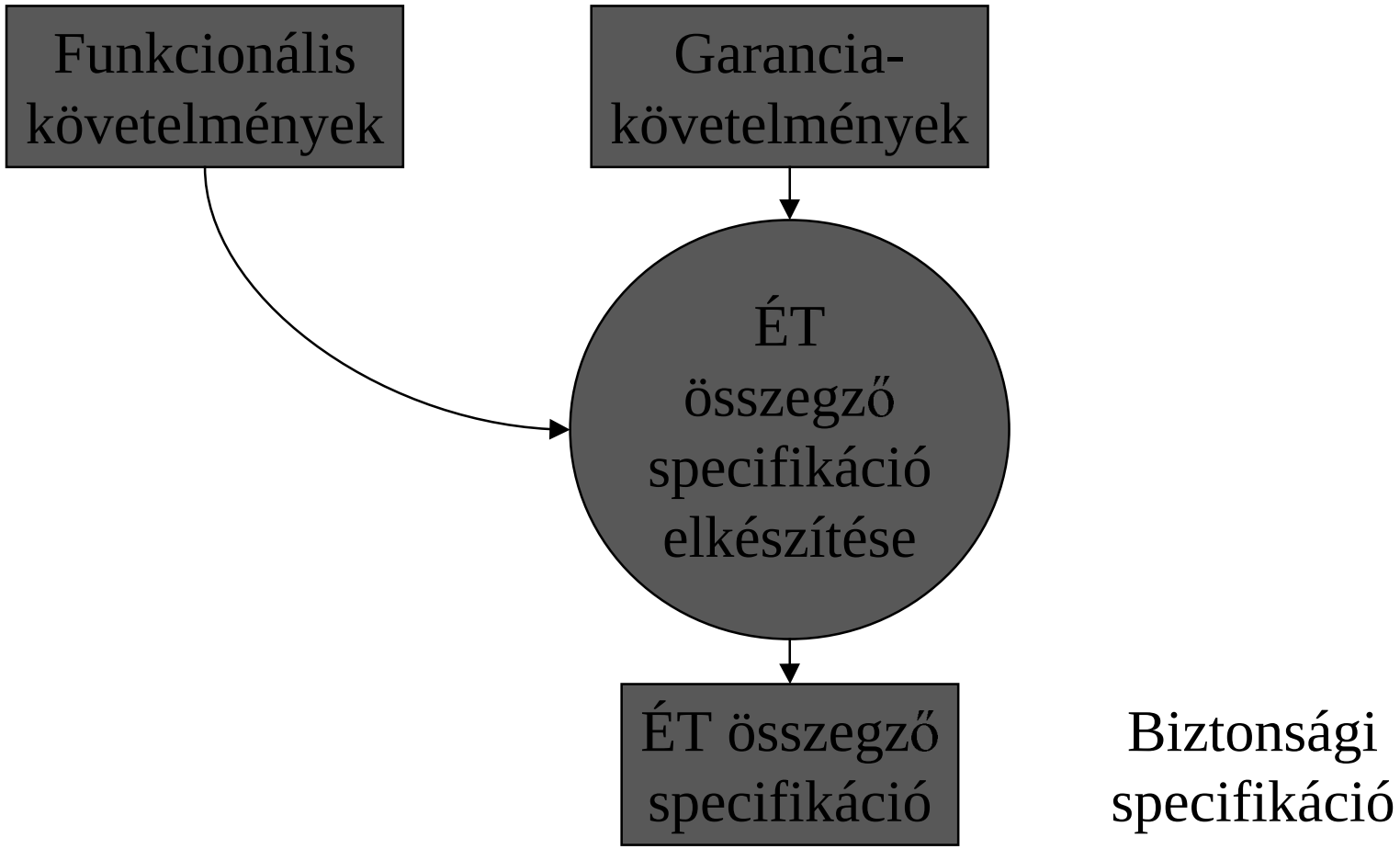
- környezetre
- ÉT-re

vonatkozó célok

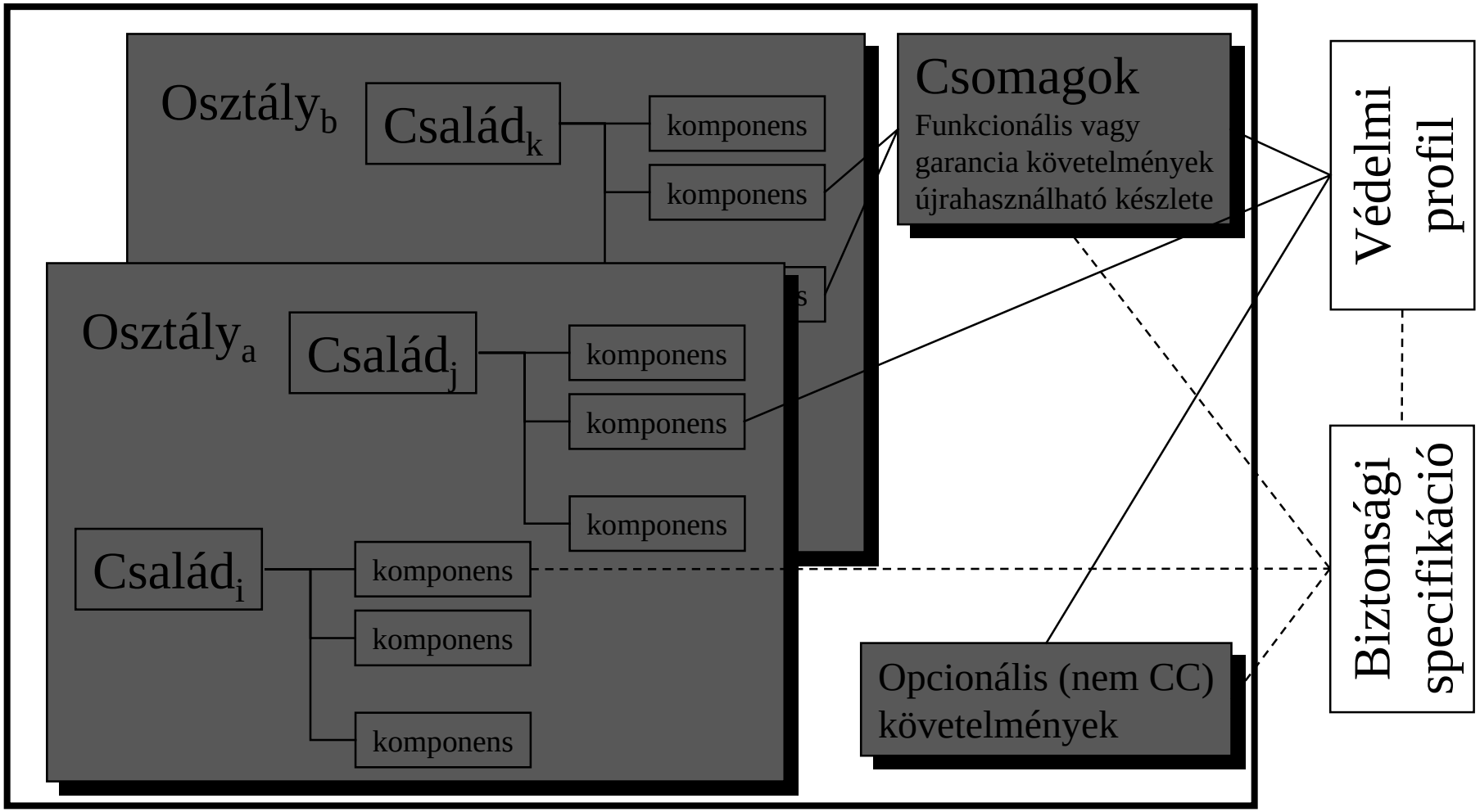
ÉT biztonsági követelményei



ÉT összegző specifikáció



CC leírások


Osztály$_b$
Család$_k$
komponens
komponens
Osztály$_a$
Család$_j$
komponens
komponens
komponens
Család$_i$
komponens
komponens
komponens
Csomagok
Funkcionális vagy garancia követelmények újrahasználható készlete
Opcionális (nem CC) követelmények
Védelmi profil
Biztonsági specifikáció

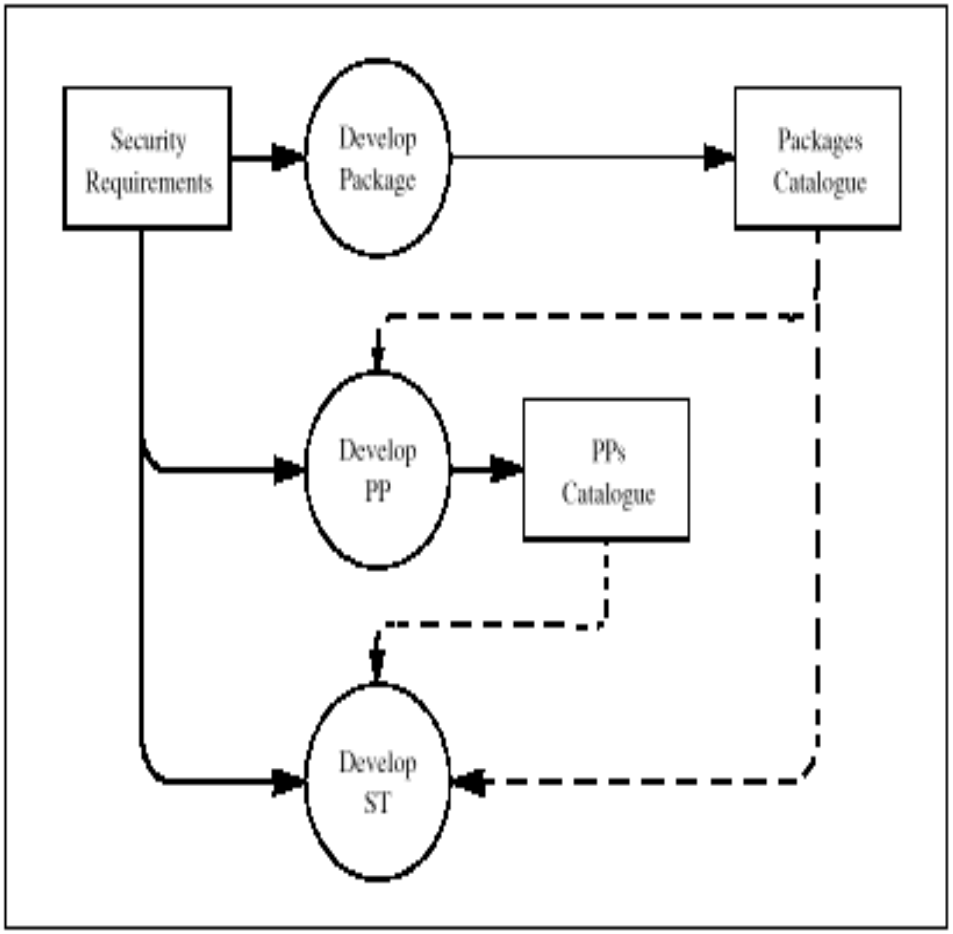
Követelményhierarchia

- Osztály
  Azonos terület, különböző célok
- Család
  Azonos cél, eltérő hangsúly és szigorúság
- Komponens
  Követelmények egy készlete, elemekből áll.
  Családon belül rendezések lehetnek.
  Elem oszthatatlan.

Függőségek (komponenesek között)

Műveletek: iteráció, paraméterezés, kiválasztás, finomítás

Követelmények használata



Csomag
- újrahasználható
- értékelési garancia-szintek is csomagok

Védelmi profil
- újrahasználható
- tartalmaz ÉGSZ-t
- felhasználói csoportok is kialakíthatják

Biztonsági specifikáció
- konkrét

Értékelés-típusok

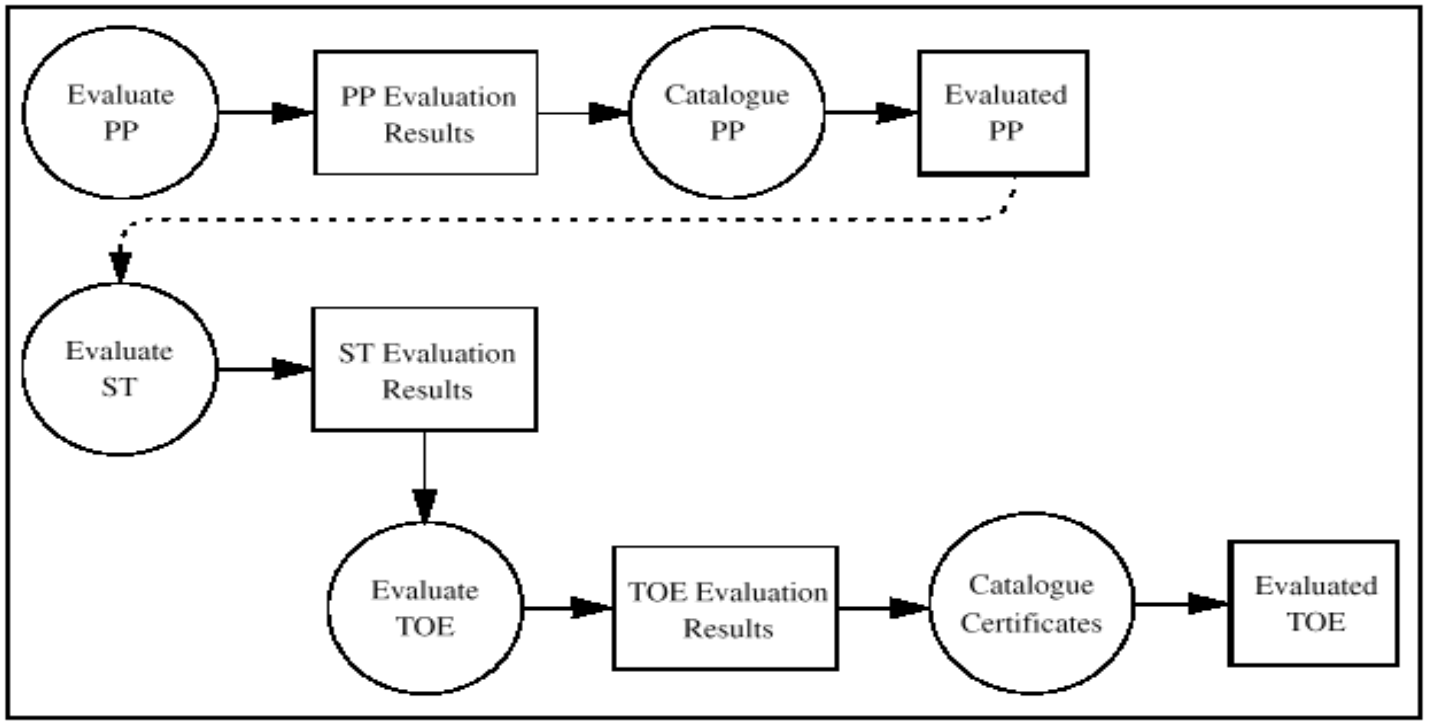
- Védelmi Profil értékelés

  teljes, konzisztens, technikailag megfelelő
- Biztonsági Specifikáció értékelés
  - teljes, konzisztens, technikailag megfelelő
  - megfelel a VP-nek
- ÉT értékelés

  megfelel a BS-nek
- Garancia-karbantartás

  ÉT módosítások után is megfelel

Értékelési eredmények



Legyen objektív és megismételhető - CC követelményei segítenek
Marad szubjektív elem - nem univerzális
Nem biztos, hogy minden alkalmazásban elfogadható, csak adott környezetben

Elvárások a VP és BR követelményeivel szemben

CC nem tartalmazhat mindent, bővíthető

A bővítés

- legyen világosan megfogalmazott, értékelhető, demonstrálható
- tegyen eleget az értékelési garanciaszintekre vonatkozó bizonyos CC osztályoknak

Az ÉT értékelési eredményeinek felhasználása