Securitate IT

Universitatea “Transilvania” din Brasov

Agenda Securitatea in tehnologia informatiei

6 Politica de securitate IT

6.1 Analiza riscurilor

6.2 Concepte de securitate

6.3 Managementul riscurilor

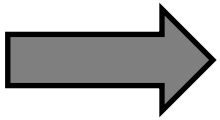
6 Evaluarea securitatii IT

6 Evaluarea securitatii IT

Evaluarea securitatii sistemelor IT

Exista diferite sisteme de criterii pentru a evalua securitatea sistemelor IT (produse si solutii)

- Exista si sunt utilizate concomitent
- Stabilesc diferite prioritati
- Se suprapun partial
- Diferite grupuri-tinta
- Exemple: BSI-Manual de protectie de baza, BS 7799, ITSEC, Common Criteria ISO/IEC 15408



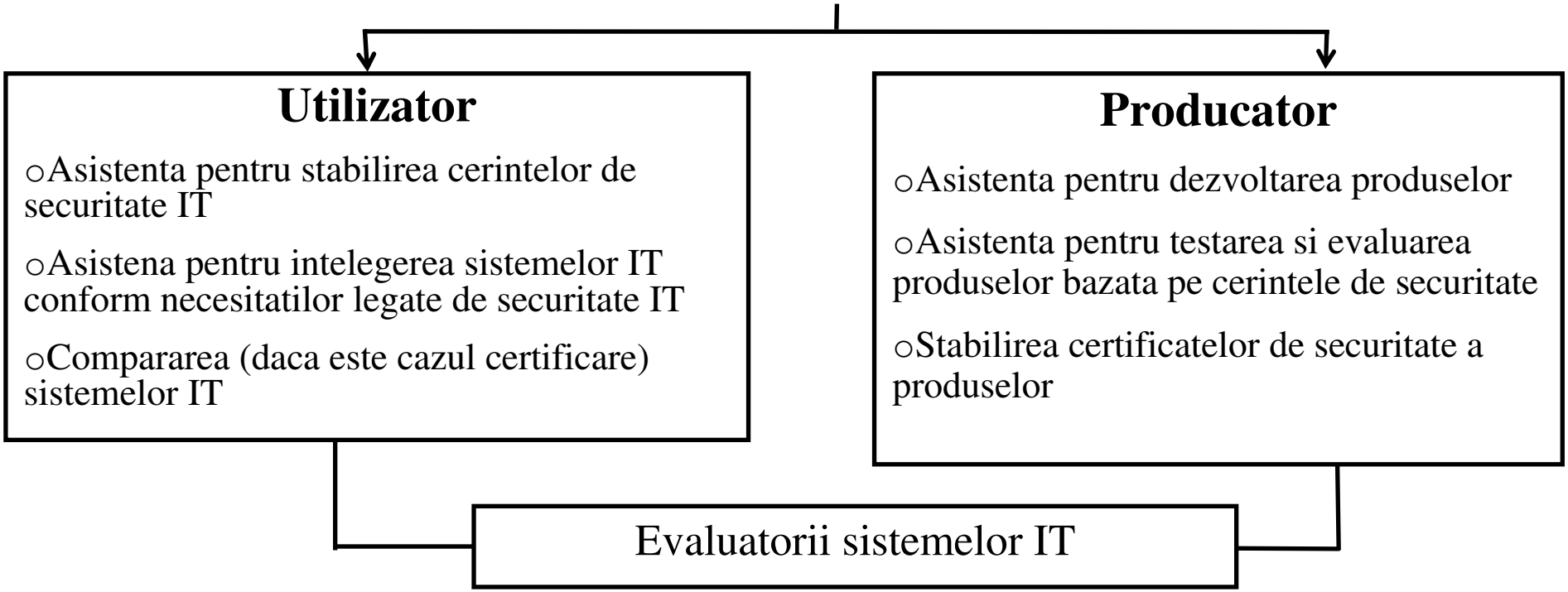
Producatorii si utilizatorii de sisteme IT necesita criterii de evaluare uniforme acceptate la nivel global pentru evaluarea securitatii sistemelor IT.

6 Politica de securitate IT

Sistem de criterii pentru securitatea IT

Ghid ca schema de testare si evaluare

A securitatii sistemelor IT



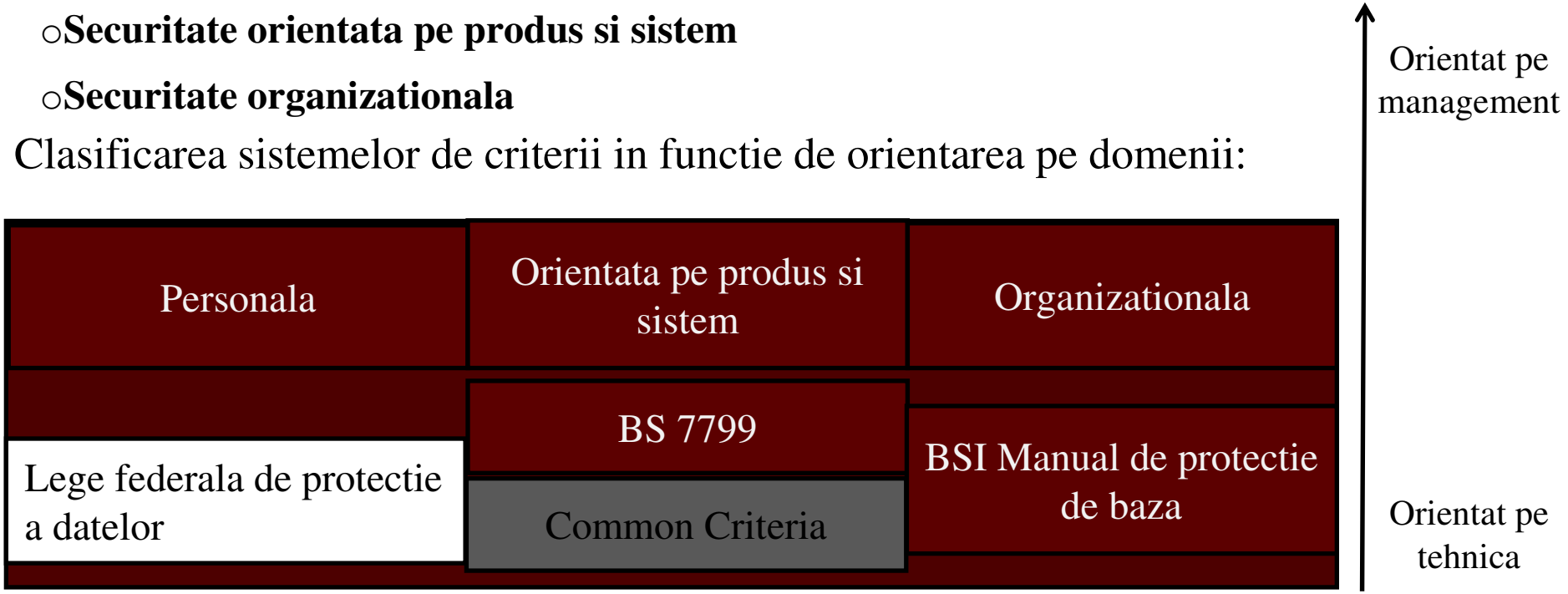
6 Evaluarea securitatii IT

Evaluarea securitatii sistemelor IT...

Securitatea It se refera la domeniile:

- **Securitate personala**
- **Securitate orientata pe produs si sistem**
- **Securitate organizationala**

Clasificarea sistemelor de criterii in functie de orientarea pe domenii:



6 Evaluarea securitatii IT

Evaluarea securitatii sistemelor IT...

(A) Sistem de criterii TCSEC (Orange Book)

- *Trusted Computer System Evaluation Criteria*
- Dezvoltat la incepul anului 1980 la US National Computer Security Center
- Clasificarea securitatii sistemelor IT pe 4 niveluri ierarhice: D, C, B, A (cel mai inalt)
- Dezavantaje si altele:
  - accent unilateral pe sisteme de operare cheie, astfel incat sistemele distribuite nu sunt inregistrate
  - neglijarea intereselor de securitate specifice utilizatorului
  - indeplinirea unei functii de evaluare nu poate fi evaluata prin eficacitatea mecanismelor de protectie impotriva amenintarilor (gradul de incredere lipseste)

6 Evaluarea securitatii IT

Evaluarea securitatii sistemelor IT...

(B) Sistemul de criterii ITSEC

- *Information Technology Security Evaluation Criteria*
- Din 1991 ca criteriu european al tarilor UK, F, NL, D
- Clasele functionale cu cerinte de securitate pentru clase de aplicatii specifice
- Clasificarea securitatii pe 7 niveluri de evaluare de la E0 (necorespunzator) la E6 (excelent)
- Componentele hard si soft pot fi evaluate pentru diferite aplicatii
- Dezavantaje si altele:
  - Ca inainte in legatura cu concentrarea pe sisteme centrale
  - Certificatele nu sunt recunoscute la nivel global

6 Evaluarea securitatii IT

Evaluarea securitatii sistemelor IT...

(C) Sistemul de criterii ISO/IEC 17799 (BS 7799-1)

- *Code of practice for Information security management*
- din decembrie 2000 luat prin ghidul ISO international (Standard 17799) pentru managementul securitatii de la Britisch Standards Institute (BS 7799-1) (Colectie de masuri optime conform Best-practice-approach)
- În plus față de măsurile tehnice de prevenire toate elementele fluxului de comunicare în cadrul organizației (procese) sunt luate în considerare, pentru a spori securitatea IT
- Masurile organizatorice, care trebuie luate de management(Security policy), sunt inregistrate in catalogul de criterii (Tehnici-Procese-Management)
- Contine multe componente generice
- Implementarea unei actiuni de siguranta depinde in totalitate de organizatie; nu prescrie tehnologii concrete

6 Evaluarea securitatii IT

Evaluarea securitatii sistemelor IT...

(D) Sistemul de criterii Common Criteria

- *Common Criteria for Information Technology Security Evaluation*
- Standardul ISO/IEC 15408 (pe scurt: CC) e format din 3 parti: Partea 1: *Introduction and general model*, Partea 2: *Security functional requirements* und Partea 3: *Security assurance requirements*
- Dezvoltat in 1996 de catre JTC (Joint Technical Cometee), ISO (International Organization for Standardization) si IEC (International Electrotechnical Commission) ca un standard international
- Versiunea 2.1 este publicata din august, 1999 si este folosita pentru evaluare de catre BSD in Germania
- Clasificarea securitatii pe 7 niveluri(Evaluation Assurance Level) de de la EAL1 (mic) la EAL7(foarte inalt)

6 Evaluarea securitatii IT

Common Criteria...

Principiu

- Ținta de evaluare (TOE – Target of Evaluation) este prezentată prima dată în profilul de protecție (PP– Protection Profile) descris independent de mediul operațional și apoi extinsă, în funcție de aplicația specifică sau clarificate
- Apoi, clasificarea de evaluare este efectuată în unul dintre nivelurile de asigurare(EAL), în conformitate cu cerințele specifice de securitate (ST – Security Target)
- Certificarea de evaluare, cu intervale de validitate pot fi specificate, în care rezultatul evaluării, în ciuda modificărilor ulterioare aduse de evaluare sau de mediul său operațional nu se schimbă (re-certificare)

6 Evaluarea securitatii IT

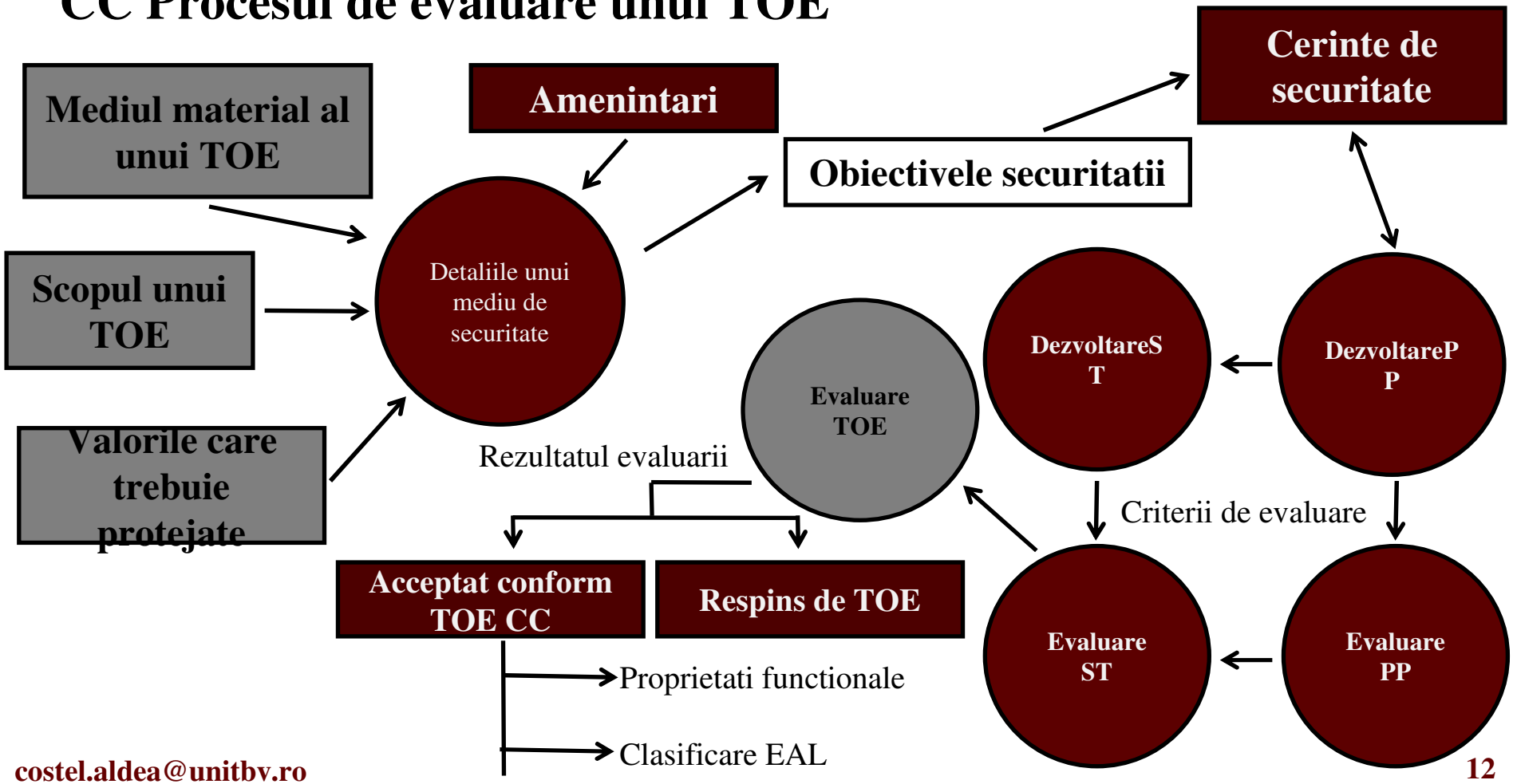
Common Criteria...

Principiu

- Criterii de evaluare a profilului de protecție (PP) și de Securitate Target (ST) sunt cuprinse în partea 3
- Cerințe de asigurare a securității sunt definite prin clase, familii și componente
- Partea 2 conține o listă de funcții predefinite cu cerințele de siguranță; cerințele lor de securitate proprii pot fi înregistrate
- TOE este evaluat în funcție de caracteristicile sale functionale si calitative:
  - Caracteristicile funcționale se referă la prezența funcțiilor tehnice cu ajutorul cărora pot fi construite sisteme sigure
  - Proprietățile calitative sunt legate de procesul de dezvoltare în sine, astfel că eficiența măsurilor de protecție prevăzute trebuie asigurată

6 Evaluarea securitatii IT

CC Procesul de evaluare unui TOE



6 Evaluarea securitatii IT

Common Criteria...

- **Evaluarea PP trebuie să îndeplinească afirmațiile "acceptat" sau "respins" (criterii din partea 3 a standardului); în cazul în care acceptarea este completă și consistentă din punct de vedere ethnic**
- **O trecere în revistă prin intermediul evaluării TOE primește o "etichetă", care indică măsura în care evaluarea poate fi de încredere pentru a îndeplini cerințele:**
  - **În conformitate cu Partea 2:** Cerințe funcționale din partea 2 se îndeplinesc
  - **Partea 2 extinsă:** și cerințele funcționale, care nu sunt din partea II, sunt îndeplinite
  - **În conformitate cu parta 3:** Cerințele pentru încredere în forma EAL se îndeplinesc
  - **Partea 3 cu adăugarea:** cerințele de asigurare sub forma unui EAL și alte metode de asigurare din partea 3 sunt îndeplinite
  - **Partea 3 extinsă:** Cerințe de asigurare sub forma unui EAL și componente de asigurare, ce nu sunt incluse în partea 3 sunt îndeplinite
- **Dacă o parte dintr-un sistem informatic TOE instalat, a fost supus la o examinare și evaluare, rezultatele de evaluare trebuie să fie luate în considerare**