Značaj i pojam sigurnosti u informacijskim sustavima

doc.dr.sc. Sandro Gerić
Fakultet organizacije i informatike
lipanj, 2013.

Značaj i pojam sigurnosti u informacijskim sustavima

- “…informacijska sigurnost nikad nije bila važnija nego danas…te predstavlja fenomen na svjetskoj razini koji potiče drugačiji način upotrebe informacijske tehnologije u poslovanju…” (DTI Director's Guide)

Značaj i pojam sigurnosti u informacijskim sustavima

- Gotovo 90% britanskih tvrtki koristi Internet za svakodnevnu poslovnu komunikaciju
- Više od 50% britanskih tvrtki pruža mogućnost udaljenog pristupa informacijskim sustavima
- Gotovo trećina malih i srednjih tvrtki, odnosno gotovo polovica velikih, koristi PDA uređaje za pristup svojim informacijskim sustavima
- Velik porast upotrebe bežičnih računalnih mreža (2002. godine koristilo ih je 2% britanskih tvrtki, a 2004. oko 30%)
- 2004. godine 87% posto britanskih tvrtki je bilo iznimno ovisno o ICT-u (DTI Director's Guide)

Značaj i pojam sigurnosti u informacijskim sustavima

- Tvrtka srednje veličine zabilježi oko 20 zaraza računalnim virusima na godinu, velika tvrtka identificira zarazu virusom svaki tjedan.
- Broj sigurnosnih incidenata je u porastu.
- Prosječna britanska tvrtka identificira jedan sigurnosni incident mjesečno, dok je u velikim tvrtkama ta stopa nešto viša – jedan sigurnosni incident na tjedan.
- Sigurnosne prijetnje informacijskoj sigurnosti još uvijek ne spadaju u 5 najznačajnijih poslovnih rizika. (DTI Director's Guide)

Značaj i pojam sigurnosti u informacijskim sustavima

- Informacije i resursi informacijskog sustava su organizacijski resursi.
- Informacijska sigurnost je u funkciji:
  - Osiguravanja poslovnog kontinuiteta,
  - Minimiziranja štete nastale realizacijom sigurnosnih prijetnji nad informacijama,
  - Maksimiziranja povrata ulaganja i poslovnih prilika,

  - Osiguranja tajnosti informacija,
  - Osiguranja integriteta informacija,
  - Osiguranja raspoloživosti informacija.

Značaj i pojam sigurnosti u informacijskim sustavima

- **Informacijska sigurnost** – očuvanje povjerljivosti, integriteta i raspoloživosti informacija (a također može uključivati i druge elemente kao što su autentičnost, mogućnost praćenja, neporecivost i pouzdanost).
- **Povjerljivost informacija** – informacija treba biti dostupna samo onim osobama koje posjeduju odgovarajuća korisnička prava.
- **Integritet informacija** – očuvanje točnosti i cjelovitosti informacija i metoda obrade.

(ISO/IEC 17799:2000/05)

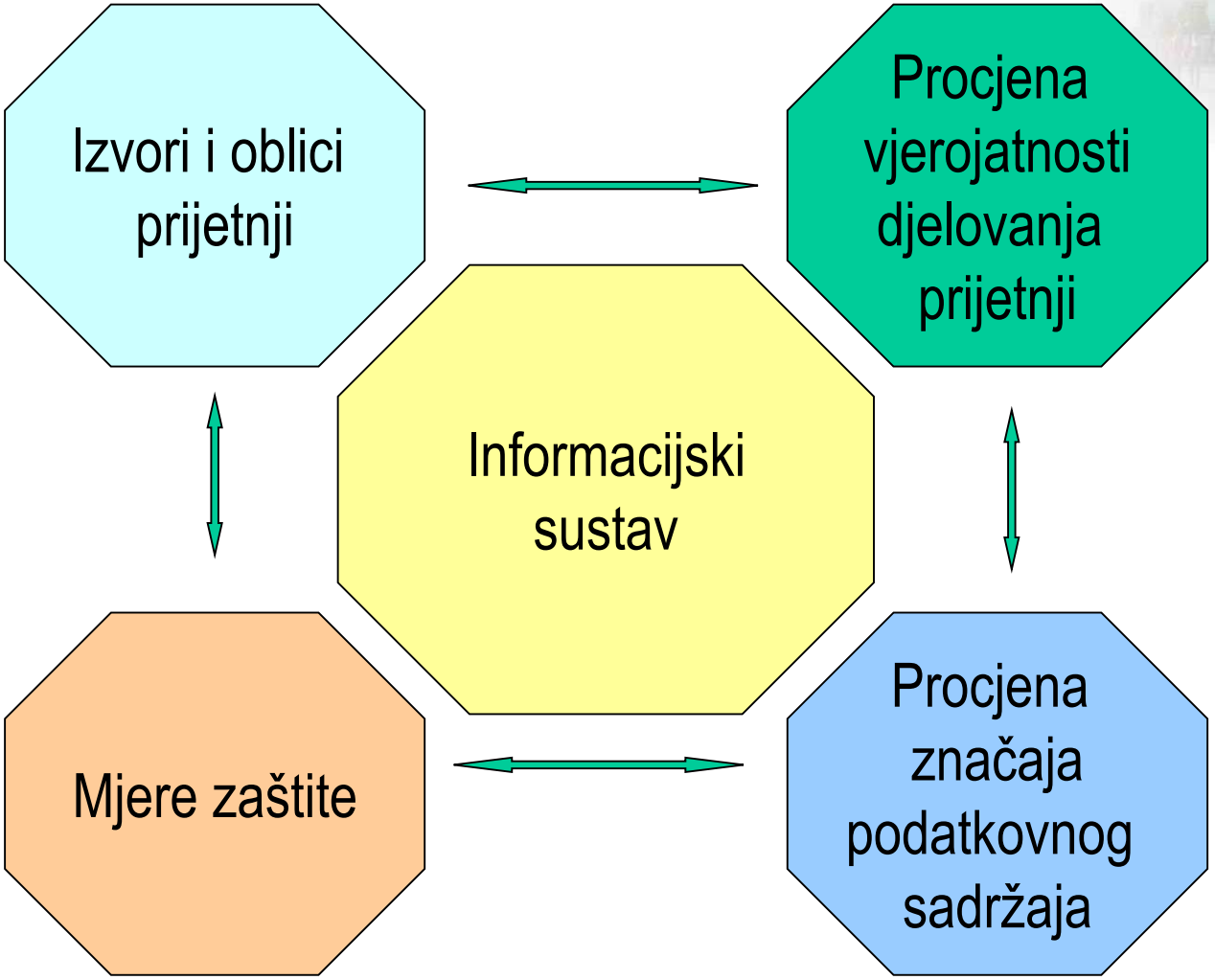
Značaj i pojam sigurnosti u informacijskim sustavima

- **Raspoloživost informacija** – osiguravanje da ovlašteni korisnici imaju mogućnost pristupa potrebnim informacijama i pripadajućim resursima kada im je to potrebno.
- **Procjena rizika** – procjena sigurnosnih prijetnji, učinaka prijetnji i ranjivosti informacijskog sustava, informacija i resursa za obradu informacija te procjena vjerojatnosti pojave sigurnosnih prijetnji.
- **Upravljanje rizikom** – proces identificiranja, kontroliranja, minimiziranja i eliminiranja sigurnosnog rizika koji može djelovati na informacijski sustav uz prihvatljive troškove. (ISO/IEC 17799:2000/05)

Struktura sustava informacijske sigurnosti

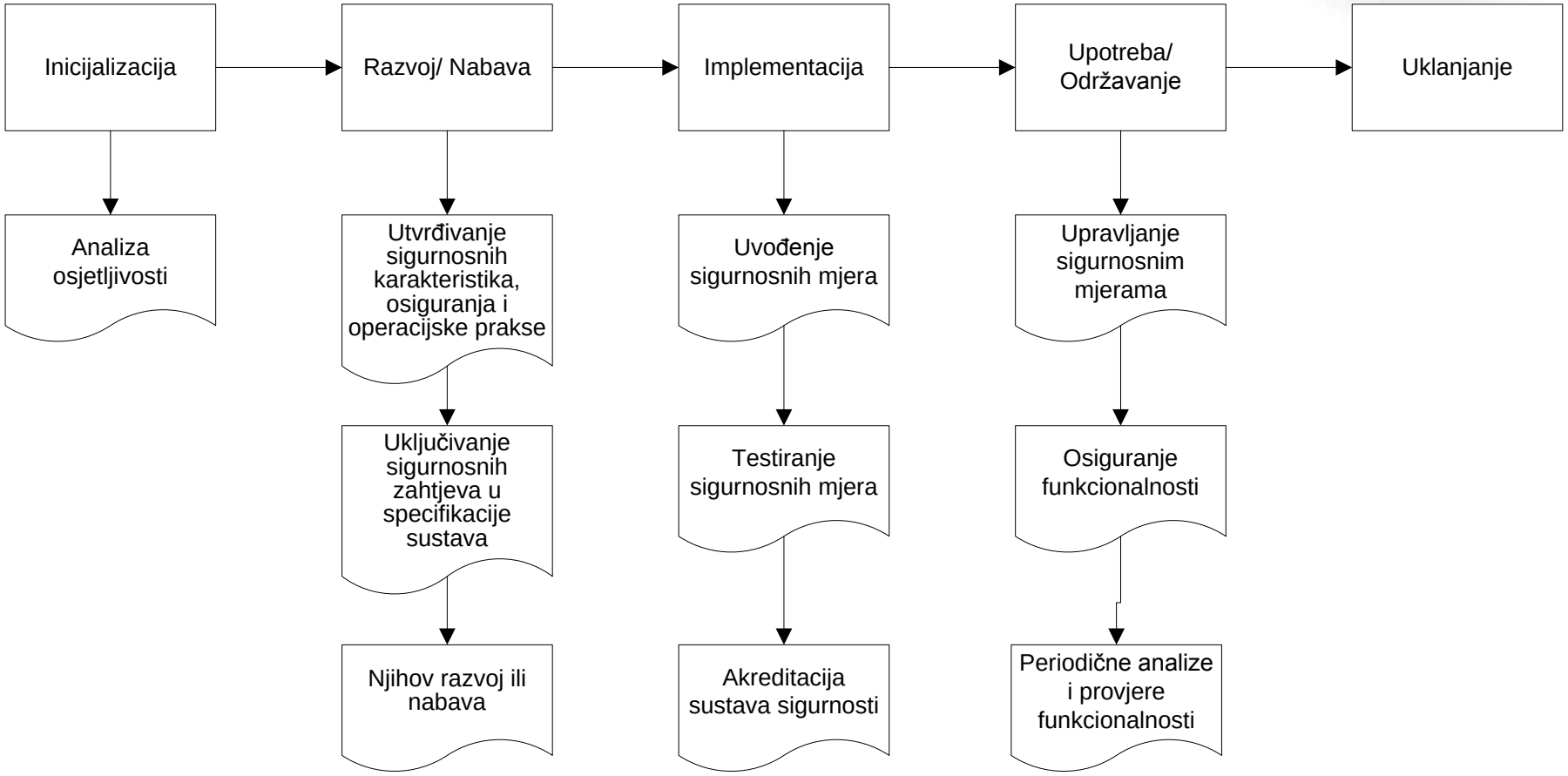
- **Sigurnost informacijskog sustava** je niz mjera poduzetih prilikom njegova projektiranja s ciljem ostvarenja funkcionalnosti sustava u uobičajenim uvjetima djelovanja.
- **Zaštita informacijskog sustava** je niz poduzetih mjera kojima se osigurava željena razina funkcionalnosti sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji.

Struktura sustava informacijske sigurnosti



Struktura sustava informacijske sigurnosti

Razvoj sustava sigurnosti informacijskog sustava

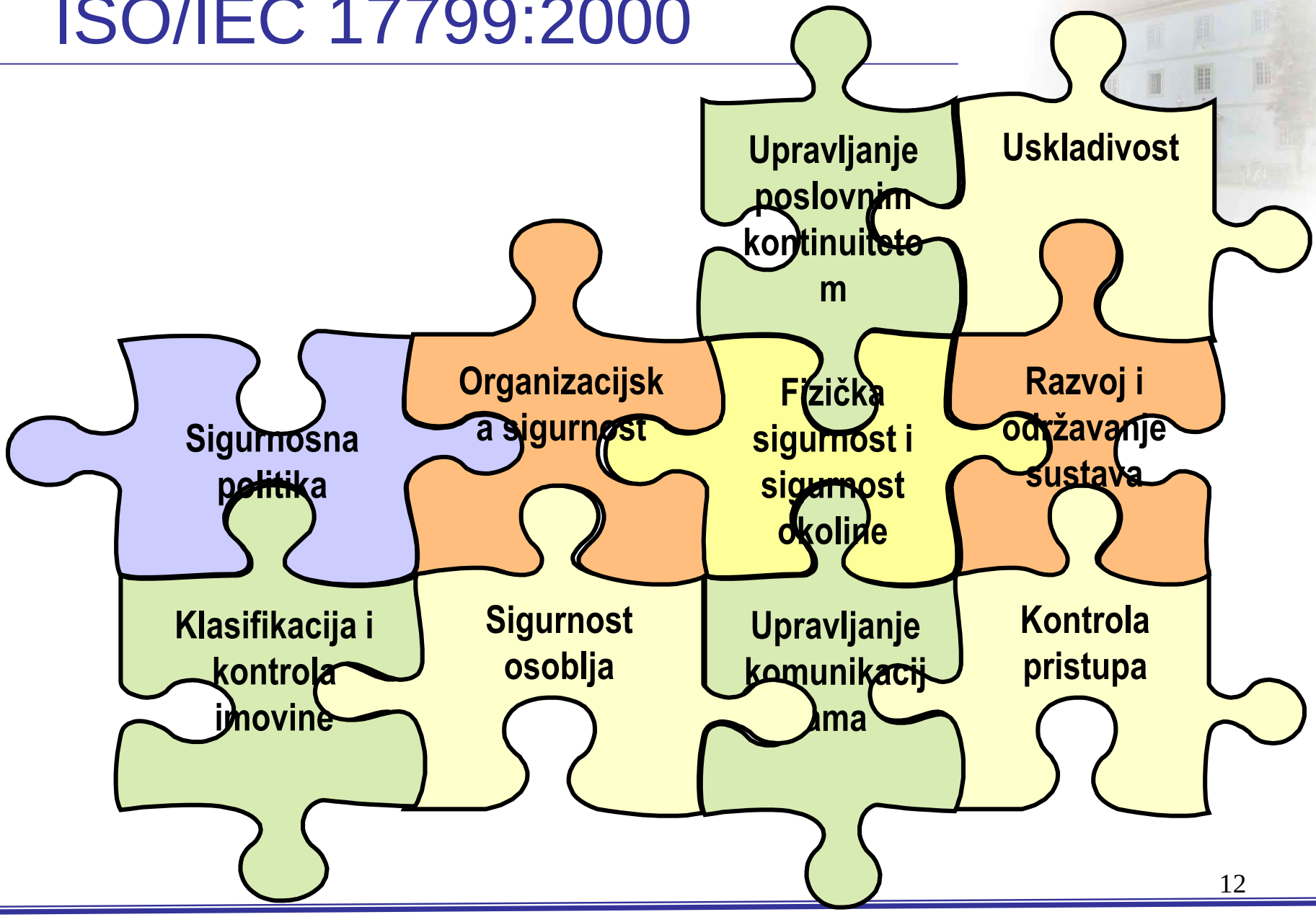


Izgradnja sustava sigurnosti prema standardima i normama

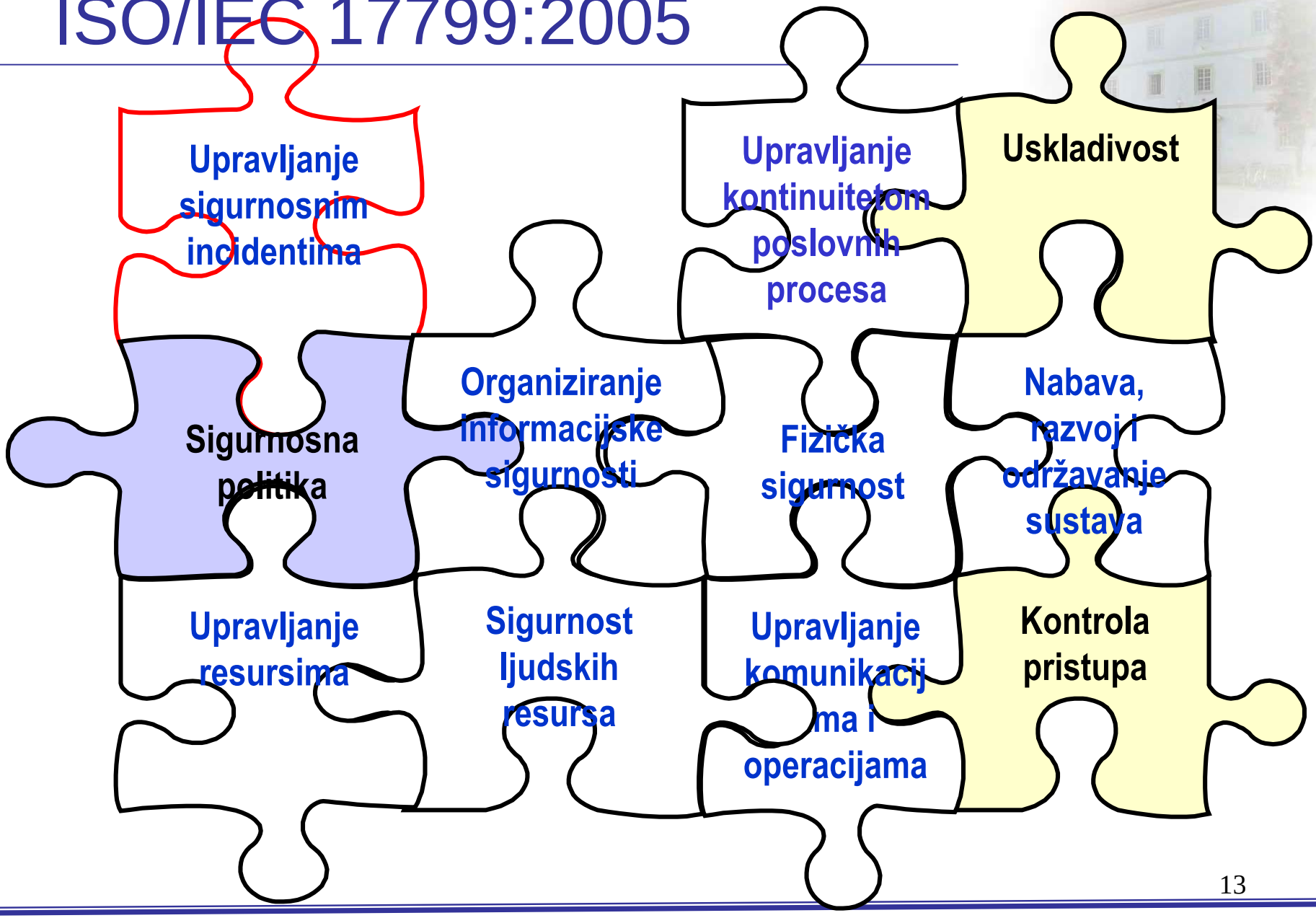
- Standardi međunarodne organizacije za standardizaciju i Britanski standardi:
  - ISO/IEC 17799:2000 (2005)
  - BS 7799: Part 2
  - ISO/IEC 27000 (usvajanje standarda u tijeku)
  - BS 7799: Part 3 (usvajanje standarda u tijeku)

- Ostali standardi: ISO 21827 *Systems Security Engineering Capability Maturity Model*, ISO 15408 *Common Criteria*, ITIL/BS 15000 *IT Service Management*, ISO 13335 *IT Security Management*, NIST, COBIT, VISA ISP, GAISP.

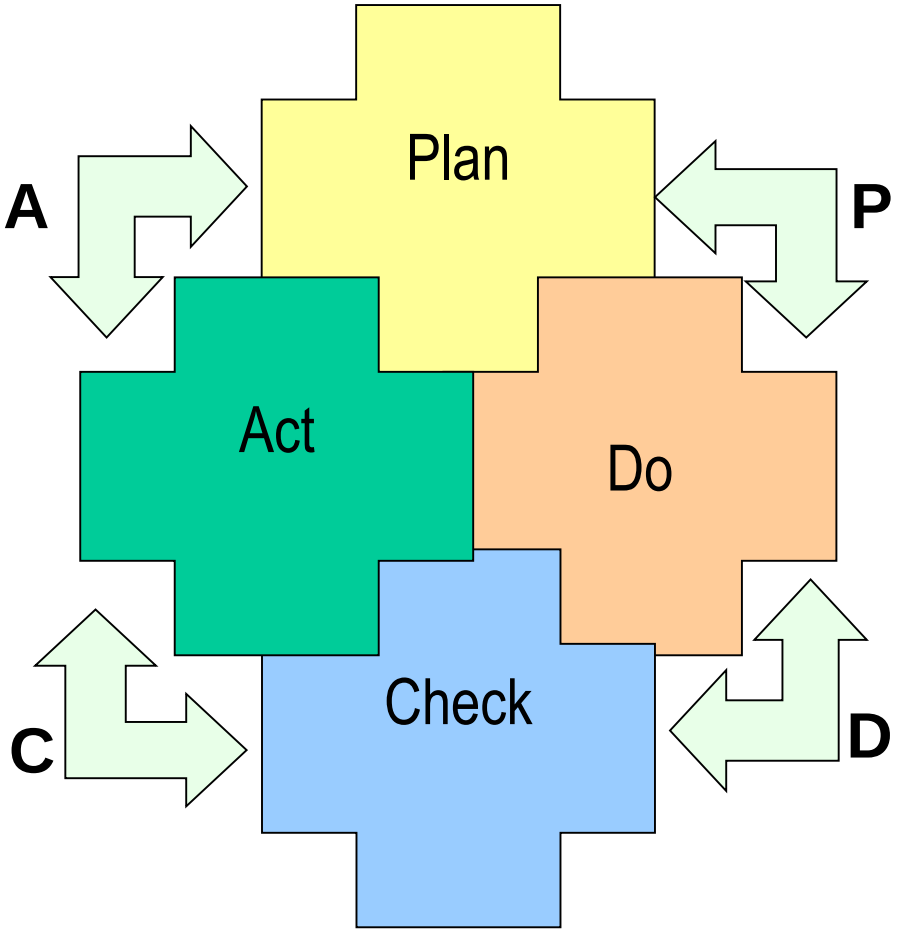
ISO/IEC 17799:2000



ISO/IEC 17799:2005



BS 7799: Part2



ciklus

Mjere zaštite od sigurnosnih prijetnji

- Mjere zaštite predstavljaju skup aktivnosti, postupaka, implementacije zaštitnih mehanizama i naprava, s ciljem ostvarenja zaštite informacijskog sustava od različitih sigurnosnih rizika i prijetnji.
- Više skupina zaštitnih mjera:
  - Programske mjere zaštite
  - Fizičke i tehničke mjere zaštite,
  - Organizacijske mjere zaštite,
  - Mjere zaštite iz područja prava.

Upravljanje sigurnošću IS-a

- Upravljanje sigurnošću informacijskog sustava započinje i treba se odvijati paralelno sa uvođenjem i djelovanjem informacijskog sustava.
- Sastavni elementi upravljanja sigurnošću IS-a:
  - Definiranje sigurnosne politike,
  - Odnos prema sigurnosnim rizicima,
  - Procjena rizika i sigurnosnih prijetnji,
  - Strategije postupanja sa rizikom,
  - Definiranje sigurnosnih mjera,
  - Implementacija sustava sigurnosti,
  - Ispitivanje i analiza sustava sigurnosti.