Etik och säkerhetsfilosofi i praktiken

Margaretha Eriksson

Civ.Ing. och doktorand i informationssäkerhet KTH

irbiskonsult@tele2.se

Föreläsning 3

- Etiska frågor
- Säkerhetsfilosofi

Etiska frågor

- Etiska regler för ingenjörer
- Speciell etik för IS-folk?

Några definitioner

- **Moral**
  är det vi till vardags våra vanor
- **Moralsatser** är vägledande
  Etik = Moral i vardagsspråk
- **Ideal moral** är den moral som
  bör praktiseras
- **Gällande moral** är hur vi faktiskt gör,
  dvs den moral som praktiseras

ISACAs etiska regler (1)

ISACA® Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

Members and ISACA certification holders shall:

- Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
- Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
- Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.

ISACAs etiska regler (2)

- Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
- Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
- Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
- Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Ansvar

- **Uppgiftsansvar**
  att svara för att någonting blir utfört eller omhändertaget
- **Skuldansvar**
  att kunna ställas till svars om någonting blir fel

Ansvar

- Diskutera:
- Har informationssäkerhetsingenjörer ett särskilt moraliskt ansvar genom sin yrkesroll?
- Vilket i så fall? Motivera!

Whistle-blowing

En whistle-blower är en person som sätter stopp för något

- **Extern whistle-blowing**
  när man går utanför sin arbetsplats och informerar allmänheten (t.ex press eller myndigheter) om oegentligheter.
- **Intern whistle-blowing**
  när man går förbi den vanliga företagshierarkin
- **Öppen whistle-blowing**
  när man avslöjar sin identitet
- **Anonym whistle-blowing**
  när man inte avslöjar sin identitet

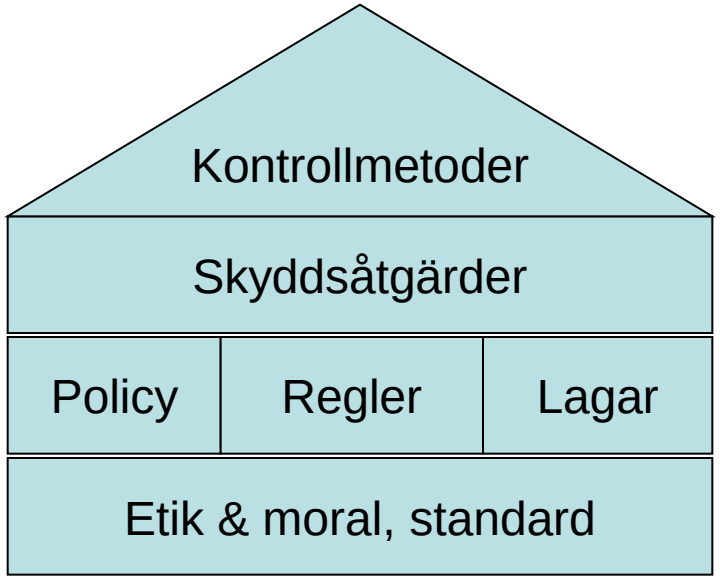
Säkerhetsfilosofi

- gäller hela organisationen och dess informationstillgångar
- under hela livscykeln
- levande och kräver underhåll

Baserat på ”Effektiv säkerhetsorganisation”, SIS HB 68

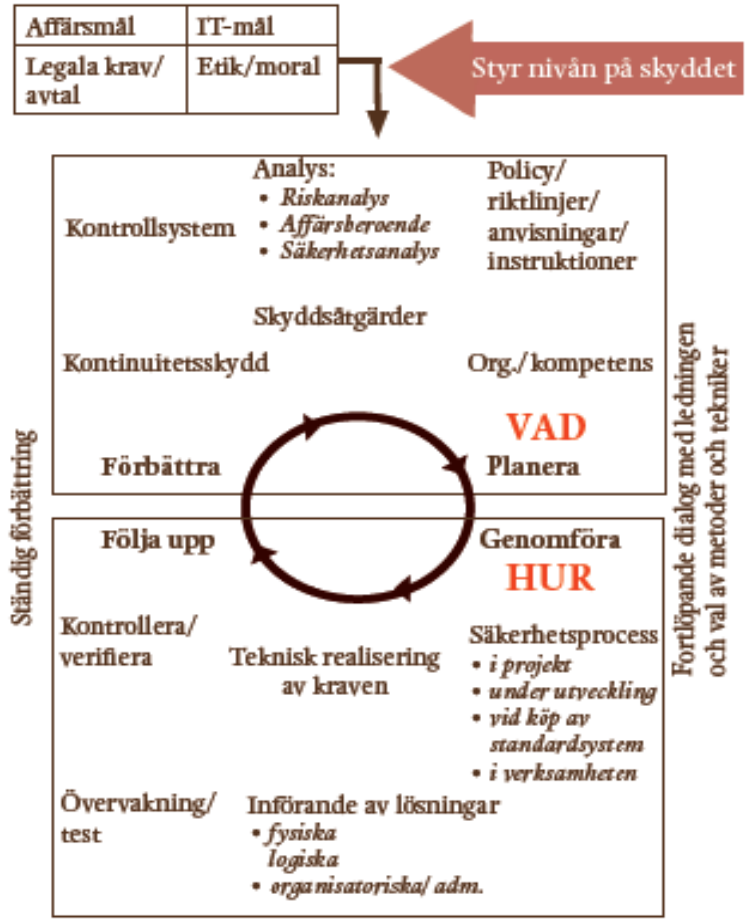
”Säkerhetshuset”

En stabil grund…



PDCA

- **P**lan (planera)
- **D**o (genomför)
- **C**heck (verifiera)
- **A**ct (utvärdera)



Säkerhet på djupet (1)

1. Säkerhetsledning
2. Personalen
3. Tillgänglighet och tillförlitlighet
4. Kringmiljön
5. Tillträde
6. Försörjning – el, luft, etc.

Säkerhet på djupet (2)

7. Brandskydd
8. Skydd mot vattenskador
9. Systemsäkerhet
10. Nätverk och telekommunikation
11. Systemutveckling och systemändringar
12. Persondatorer och arbetsstationer
13. Säkerhetskopiering och arkivering
14. Kontinuitetsplanläggning

Öka informationssäkerheten!

- Diskutera konkreta åtgärder i grupp

  Grupp 1 – punkt 1,

  Grupp 2 – punkt 2,

  Grupp 3 – punkt 3,

  Grupp 4 – punkt 4, osv

Redovisa

- Kort redovisning av konkreta åtgärder
- Gruppvis (max 3 minuter/grupp)