



Høgskolen i Telemark

Fakultet for allmennvitenskapelige fag

EKSAMEN

**6123
Informasjonssikkerhet
16. mai 2013.**

Tid: 4 timer

Studiepoeng: 7,5

Målform: Bokmål/nynorsk

Sidetal: 2

Hjelphemiddel: Lovsamling

Merknader: Ingen

Vedlegg: Ingen

1. Risikoanalyse.

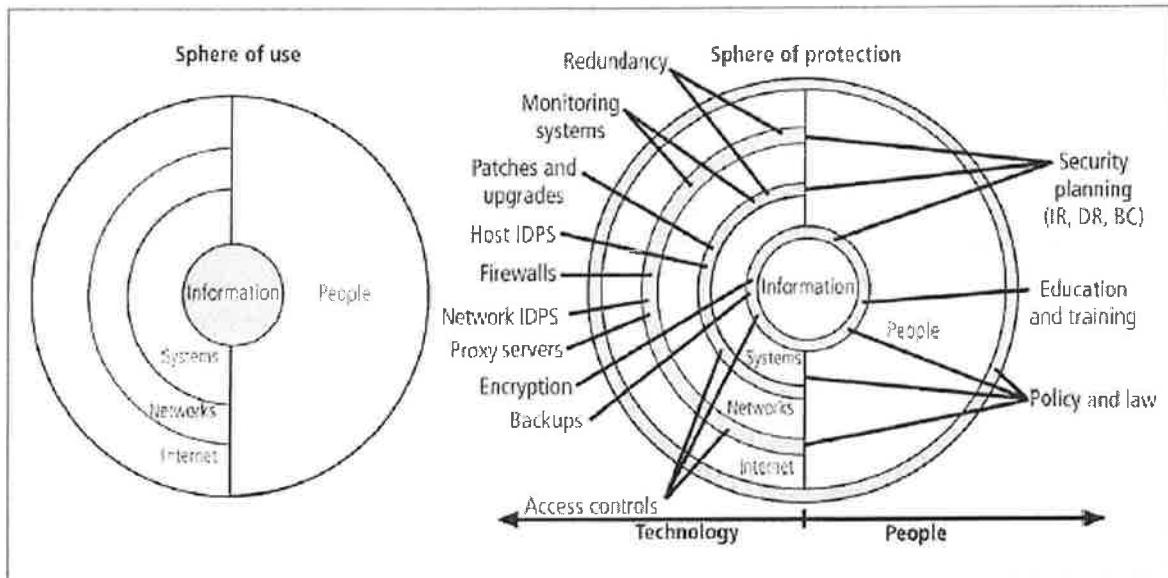
Systematisk arbeid med informasjonssikkerhet dreier seg blant annet om risikoanalyse.

- Gjør rede for begrepene *risiko* og *risikoanalyse*.
- Hva skal en risikoanalyse gi svar på?

2. Planlegging av informasjonssikkerhet.

- Forklar hensikten med Enterprise Information Security Policy (EISP).
- I forskrift til personopplysningsloven § 2-3 kan du lese om *sikkerhetsledelse*. Forklar hvordan dette henger sammen med arbeidet med å utvikle EISP.
- Forklar hva ISB (Information Security Blueprint) er og nevн relevante *dokumenter* og *standarder* for informasjonssikkerhet som har relevans for utvikling av ISB og forklar hvordan standarder kan *støtte arbeidet* med utviklingen av en ISB.
- Forklar, gjerne med eksempler fra standarden du har skrive om i førre oppgåve, hva *Plan-Do-Check-Act prinsippet* er, hvilken *innvirkning* dette prinsippet har tenkt å ha på arbeidet med ISB, og hva som er *begrunnelsen* for å trekke dette prinsippet inn i planlegging av informasjonssikkerheit.

3. Sikkerhetsarkitektur.



Figur 1 Spheres of Security (Fra Mattord og Whitman "Principles of information security" kap. 5)

- Ta utgangspunkt i Figur 1 og forklar prinsippet for «*Defense in Depth*».

- b. I Figur 1 ser du at begrepet *IDPS* er benyttet to ganger. Forklar hva som ligger i dette begrepet og hvorfor det er brukt på denne måten i modellen i Figur 1.
- c. Forklar hvilken funksjon *DMZ* har i en sikkerhetsarkitektur, og referer til Figur 1 når du forklarer hvor DMZ hører hjemme.

Slutt på eksamenstekst.

1. Risikoanalyse.

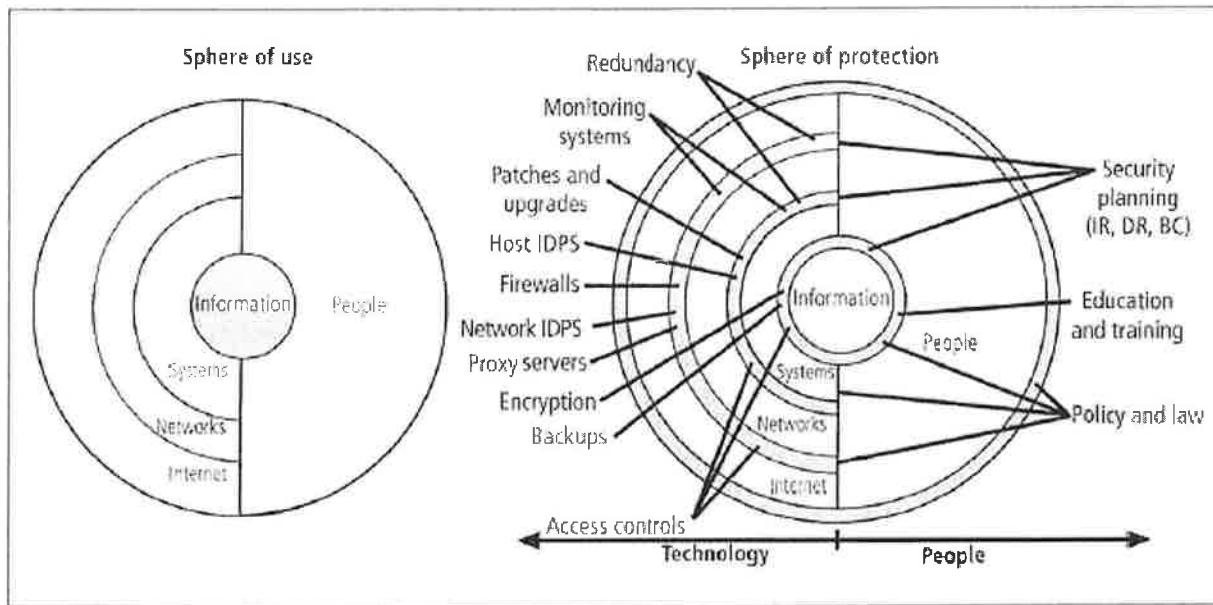
Systematisk arbeid med informasjonssikkerheit dreier seg mellom anna om risikoanalyse.

- Gjer greie omgrepa *risiko* og *risikoanalyse*.
- Kva skal ein risikoanalyse gje svar på?

2. Planleggjing av informasjonssikkerheit.

- Forklar hensikten med *Enterprise Information Security Policy* (EISP).
- I forskrift til Personopplysningsloven § 2-3 kan du lese om sikkerhetsleiing. Forklar korleis dette heng saman med arbeidet med å utvikle EISP.
- Forklar hva ISB (Information Security Blueprint) er, og nemn relevante dokument og standardar for informasjonssikkerheit som har relevans for utvikling av ISB og forklar korleis standardar kan stø opp om arbeidet med utviklinga av ein ISB.
- Forklar, gjerne med døme frå standarden du har skrive om i førre oppgåve, kva Plan-Do-Check-Act prinsippet er, kva innverknad dette prinsippet er tenk å ha på arbeidet med ISB, og kva for grunngjeving det har å trekke dette prinsippet inn i planleggjing av informasjonssikkerheit.

3. Sikkerhetsarkitektur.



Figur 1 Spheres of Security (Fra Mattord og Whitman "Principles of information security" kap. 5)

- Ta utgangspunkt i Figur 1 og forklar prinsippet for «Defense in Depth».

- b. I Figur 1 ser du at begrepet IDPS er benyttet to ganger. Forklar hva som ligger i dette begrepet og hvorfor det er brukt på denne måten i modellen i Figur 1.
- c. Forklar hvilken funksjon *DMZ* har i en sikkerhetsarkitektur, og referer til Figur 1 når du forklarer hvor DMZ hører hjemme.

Slutt på eksamenstekst.