# Retningslinjer for scenariobasert trusseldokumentasjon, erfaringer fra praksis

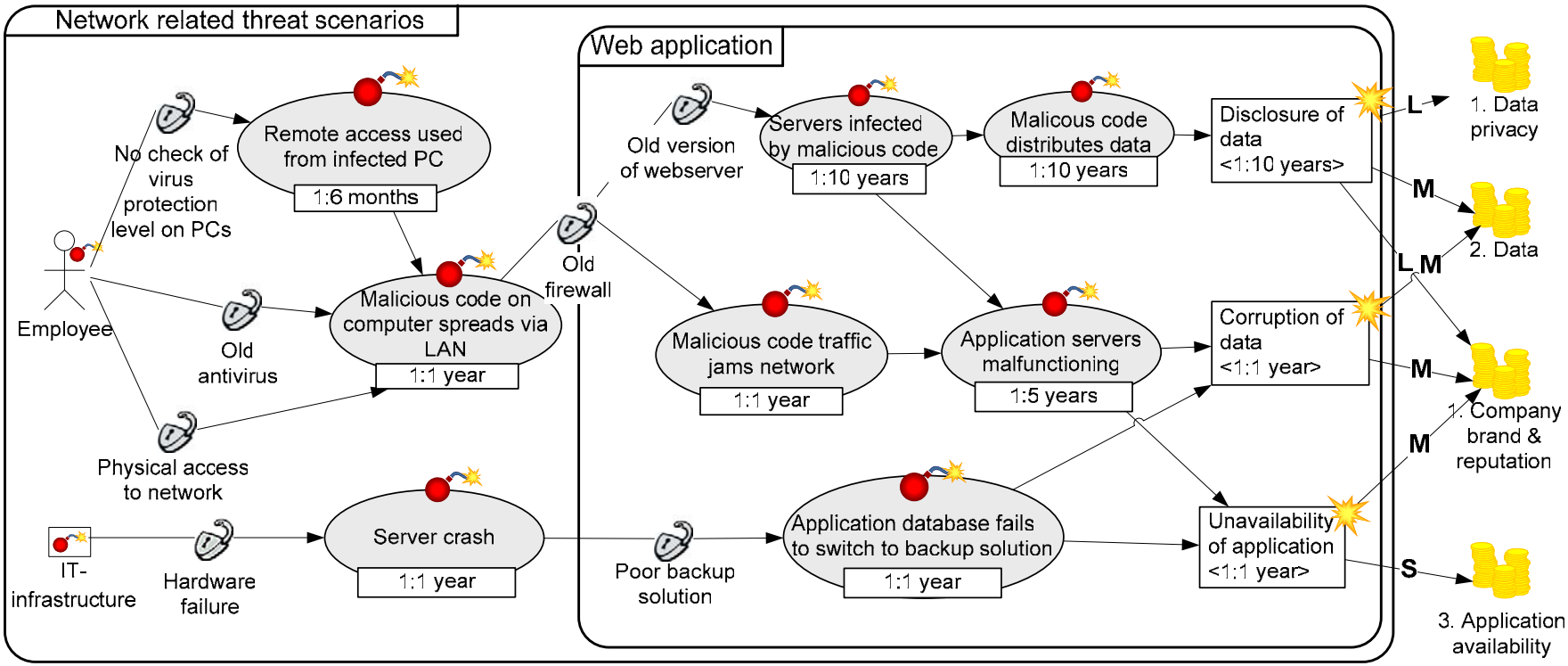
Ida Hogganvik, PhD student
SINTEF/UiO

# Innhold

- Hva er scenariobasert risikodokumentasjon?
- I hvilke sammenhenger brukes det?
- Hvordan lager man slik dokumentasjon?
- Erfaringer fra bruk

# Hva er scenariobasert trusseldokumentasjon?

- Viser hvilke uønskede situasjoner som kan oppstå
- Både dokumenterer og spesifiserer risikobildet



# Når brukes det?

- Strukturert idémyldring (structured brainstorming)
  - Stegvis gjennomgang av analyseobjektet for å finne mulige trusler, sårbarheter, uønskede hendelser etc.
- Deltakerne har inngående kjennskap til analyseobjektet
  - Eks: utviklere, brukere, beslutningstakere
- Hensikt:
  - spesifiserer et felles risikobilde
  - understøtte frekvens og konsekvens estimering av risikoer (hvor ofte kan risikoen forekomme og hvor alvorlig er den)

# I hvilken sammenheng har vi brukt det?

- SECURIS forskningsprosjekt (2003-2007)
- Tester ut risikoanalysemetoder for IT systemer
- Partnere:
  - Hydro CSI
  - FLO/IKT
  - NetCom
  - Statnett
  - WesternGeco
  - Det Norske Veritas (DNV)*
  - Microsoft Research*
  - Norsk senter for informasjonssikring (NorSIS)*

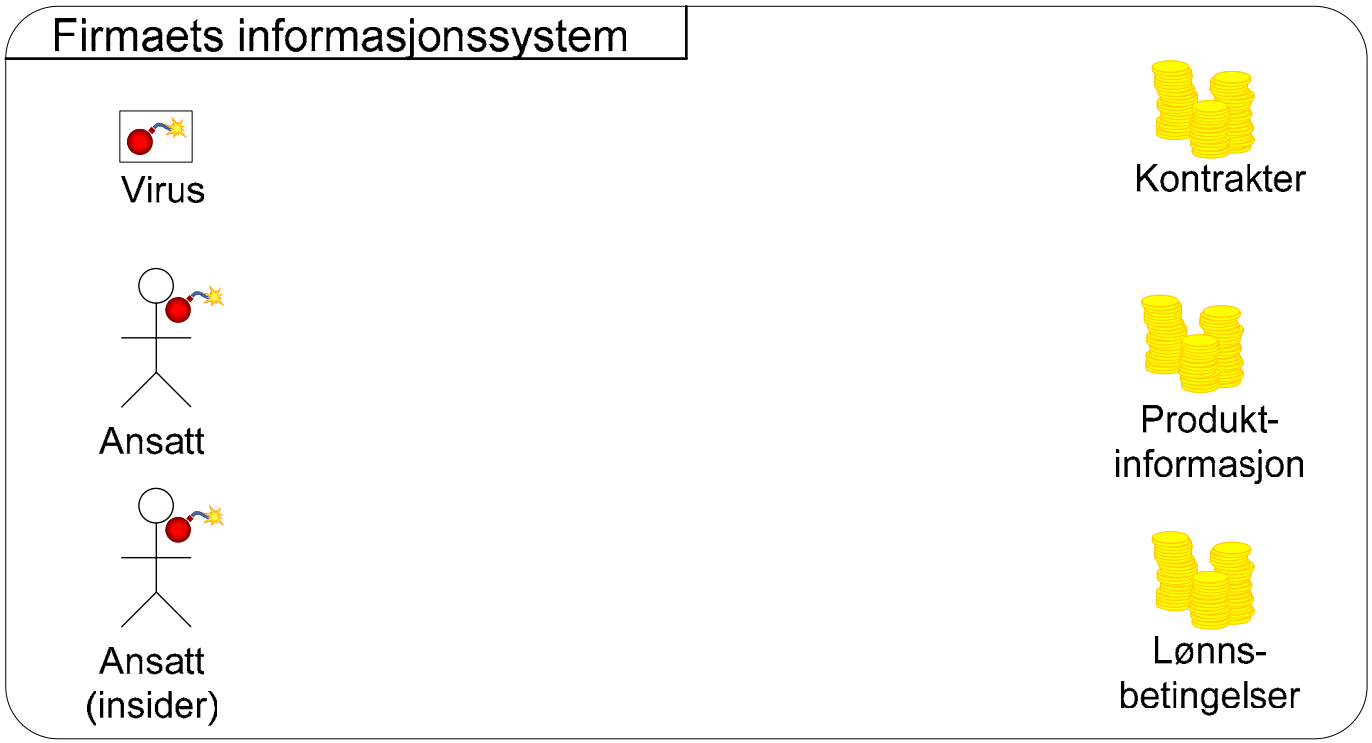
  * tidligere partnere

# Scenariobasert risikodokumentasjon (1)

- Grunnleggende begreper i risikoanalyse:
  - Aktiva: noe med verdi som må beskyttes
  - Sårbarhet: en feil/svakhet som kan utnyttes
  - Trussel: en som med vilje eller ved et uhell kan forårsake skade mot aktiva
  - Trusselscenario: en beskrivelse av hvordan trusselen går frem
  - Uønsket hendelse: en hendelse som skader ett eller flere aktiva
  - Risiko: en uønsket hendelse som et tildelt konsekvens og sannsynlighet

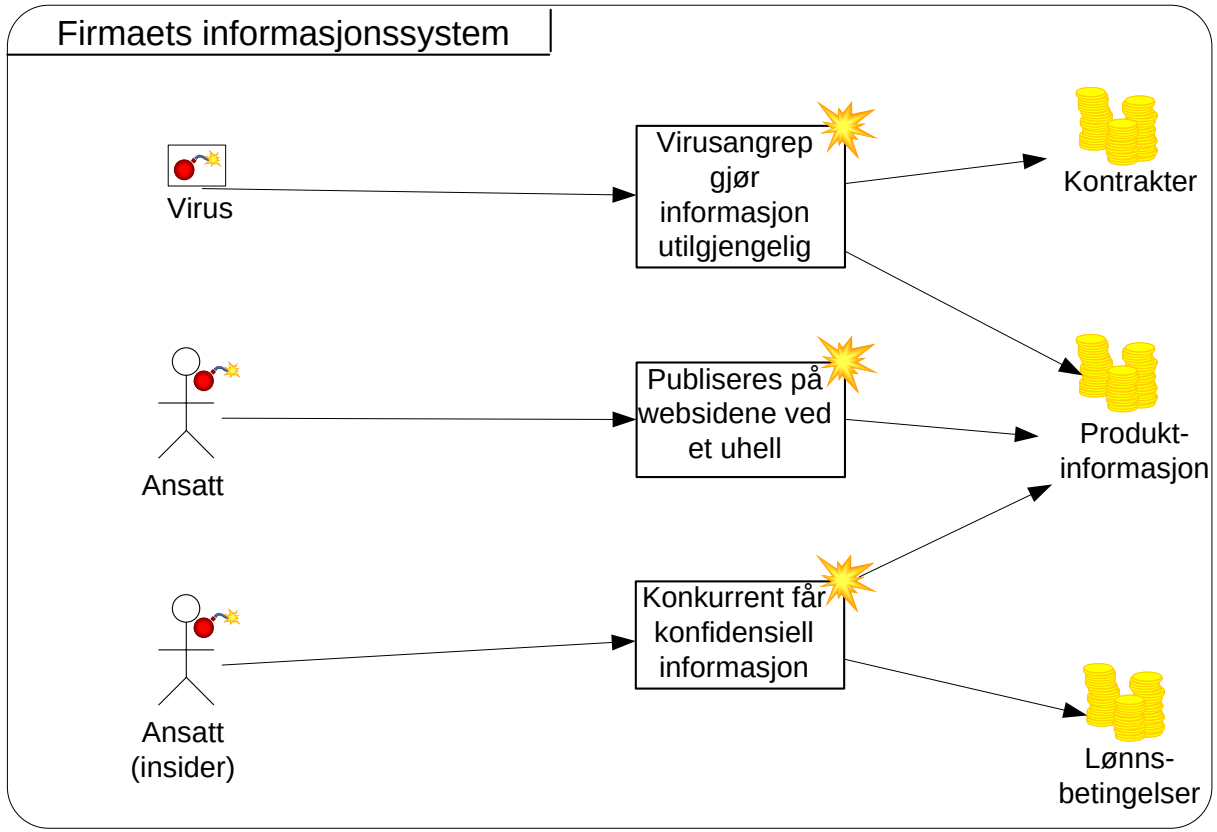
# Scenariobasert risikodokumentasjon (2)

- bygger opp trusseldiagram (trusler, aktiva):



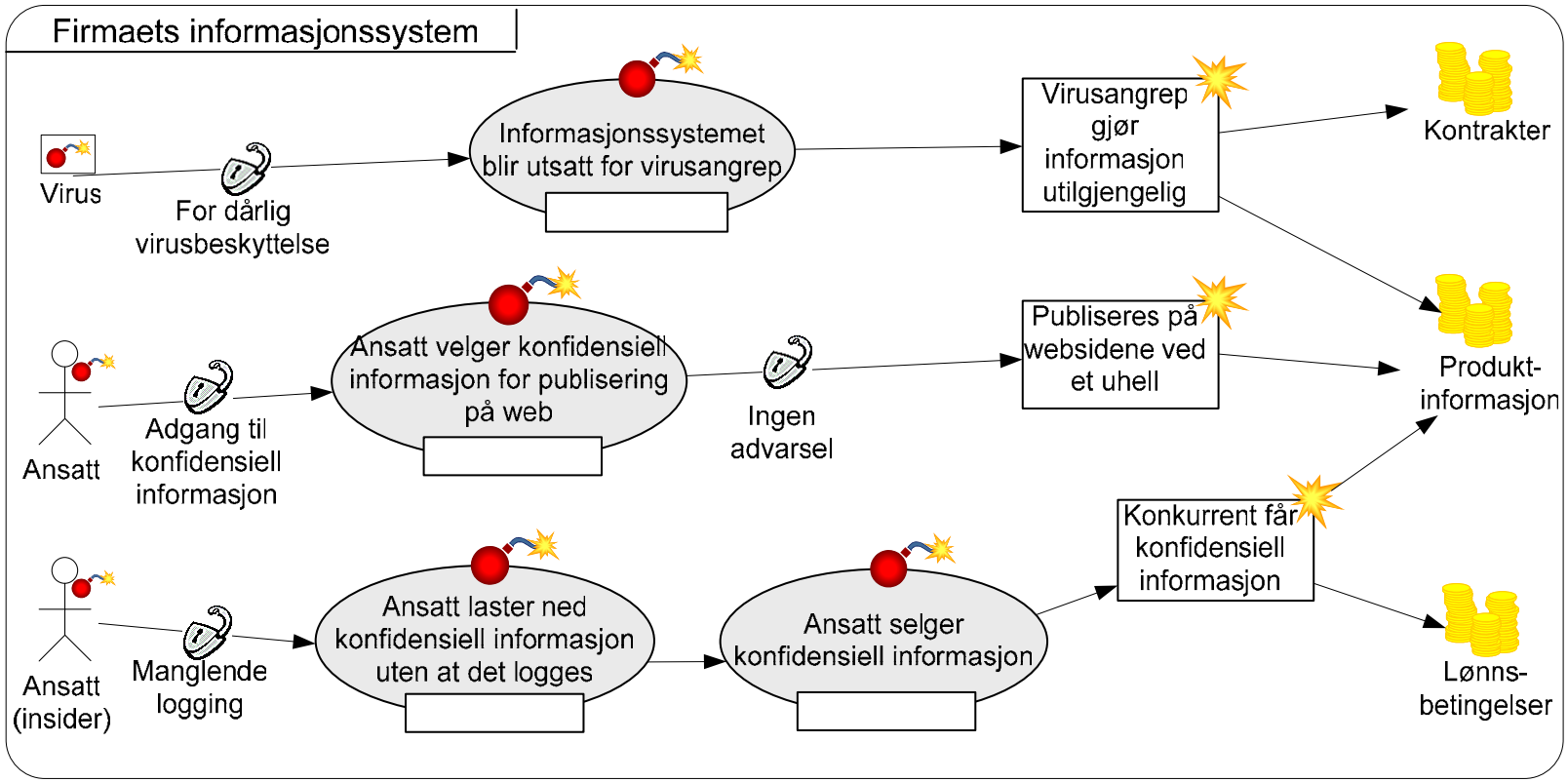
# Scenariobasert risikodokumentasjon (3)

- bygger opp trusseldiagram (legger til uønskede hendelser):



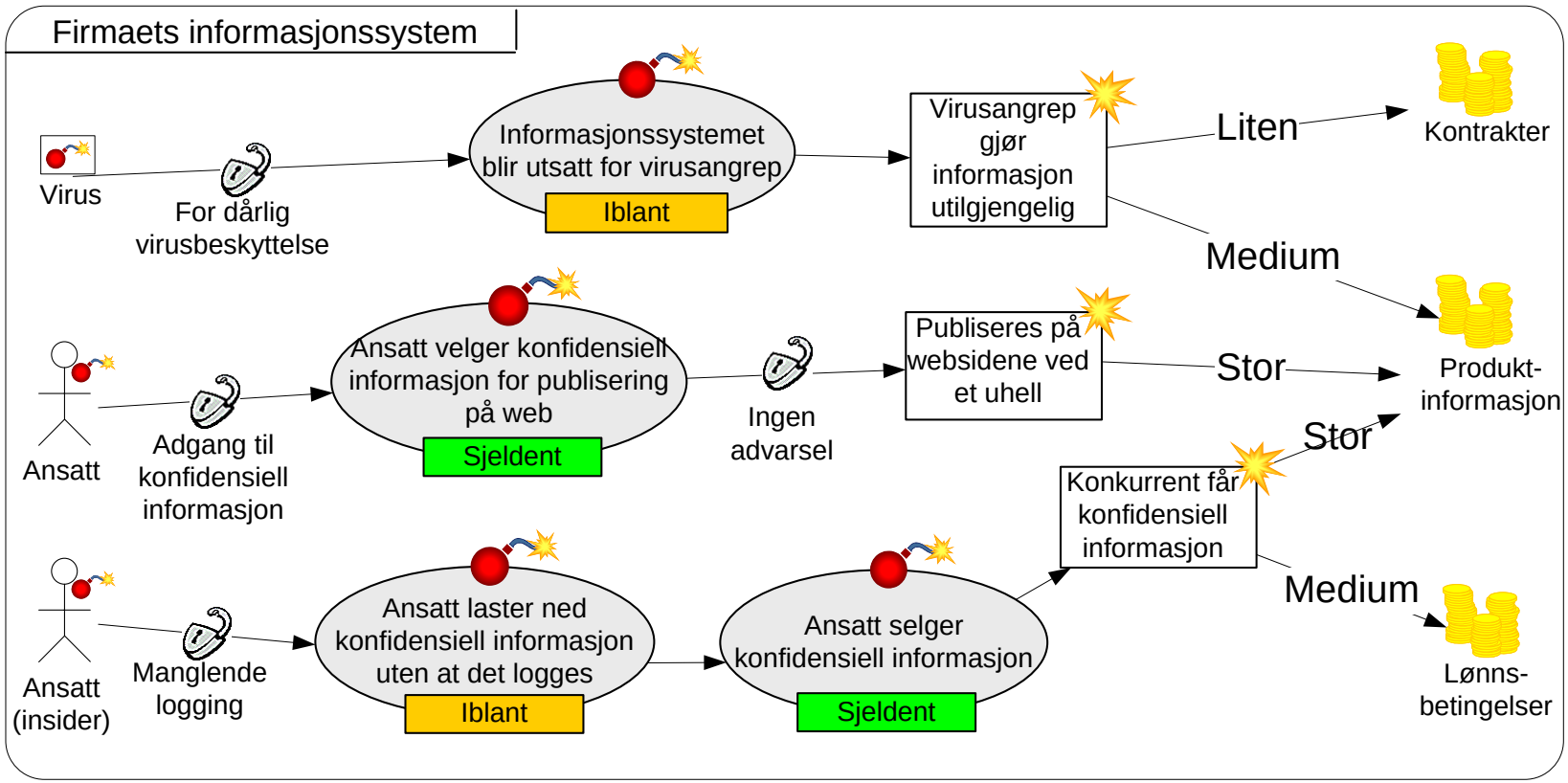
# Scenariobasert risikodokumentasjon (4)

- bygger opp trusseldiagram (legger sårbarheter og trusselscenarier):



# Scenariobasert risikodokumentasjon (5)

- estimerer frekvens og konsekvens vha trusseldiagrammet:



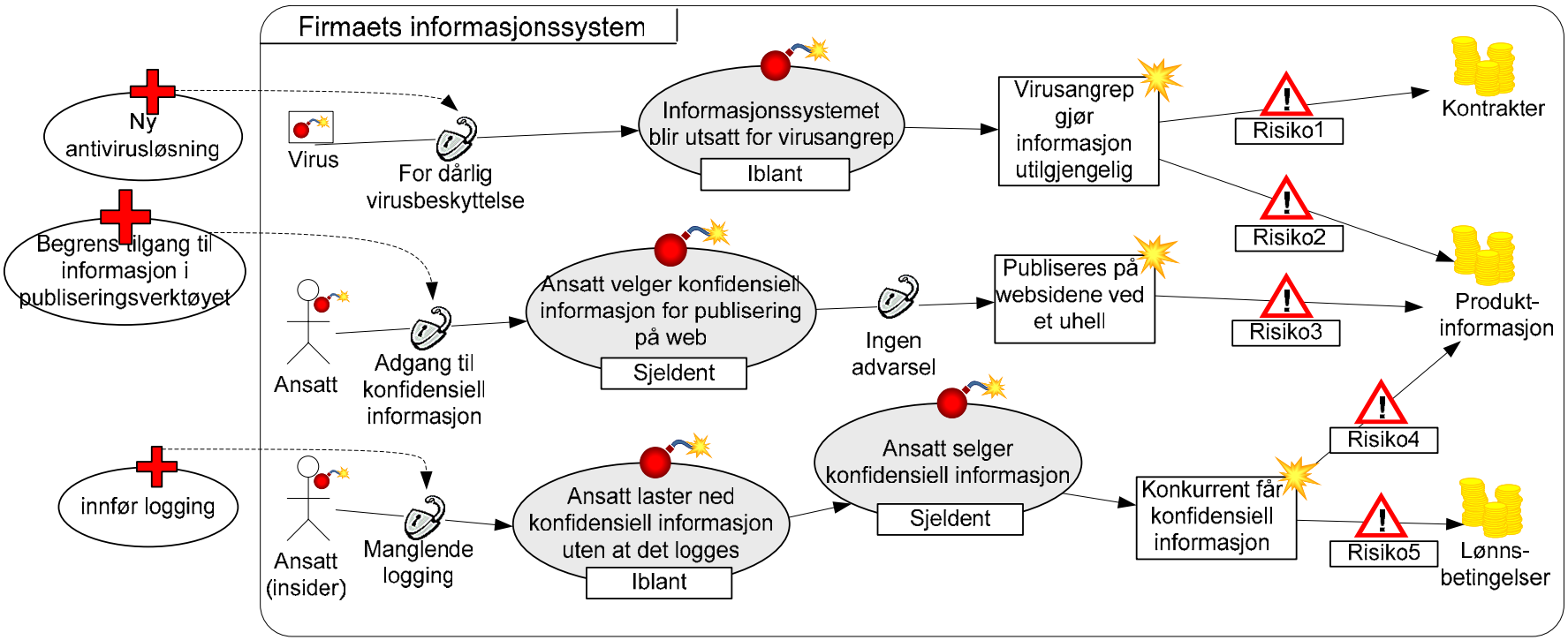
# Scenariobasert risikodokumentasjon (6)

- Risikomatrise, bestemmer hvilke risikoer som aksepteres og hvilke som må evalueres videre.

| | **Sjeldent** | **Iblant** | **Ofte** |
|---|---|---|---|
| **Liten konsekvens** | | Risiko1 | |
| **Middels konsekvens** | Risiko5 | Risiko2 | |
| **Stor konsekvens** | Risiko3<br>Risiko4 | | |

# Scenariobasert risikodokumentasjon (7)

- Risikoer som er utenfor akseptabelt nivå evalueres for å se om det er nødvendig å sette inn tiltak



# Erfaringer fra bruk (1)

- Scenariobasert risikodokumentasjon i feltstudier har:
  - økt engasjementet fra deltakerne
  - effektivisert kommunikasjonen mellom de ulike deltakerne
  - vært en nyttig visualiseringsteknikk: velegnet for presentasjoner, forsterker budskapet i analysen
  - gitt en presis spesifisering av risikoer: spesielt kjeden av hendelser mellom en trussel og en uønsket hendelse
  - bidratt til et detaljert dokumentasjon av risikobildet

# Erfaringer fra bruk (2)

- Ved bruk av scenariobasert risikodokumentasjon bør man:
  - ha en god introduksjon til diagrammene.
  - begrense mengden informasjon presentert i ett diagram.
  - involvere nødvendige deltakere så tidlig som mulig for å få diagrammene så korrekte som mulig.
  - bruke sjekklister i tillegg til deltakernes kunnskap for å forsikre seg om at alle områder er dekket.
  - justere diagrammene underveis ved evt. feil eller ny informasjon.
    - endringer av diagrammer representerer viktig informasjon og må dokumenteres.

# For mer informasjon

- Webside: http://coras.sourceforge.net/ Open source verktøy, metodebeskrivelse mm.
- Artikkel: "*A Graphical Approach to Risk Identification, Motivated by Empirical Investigations*", av Ida Hogganvik og Ketil Stølen. Kontakt Ida pr email (iho@sintef.no) for å få tilsendt denne.
- Visiostensil: inneholder ikonene brukt i diagrammene. Kontakt Ida for å få denne også.