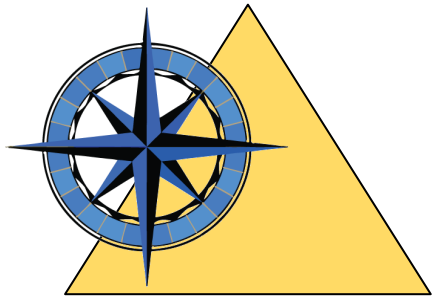
IN2120 Informasjonssikkerhet
Høst 2023

Del 12: Risikostyring

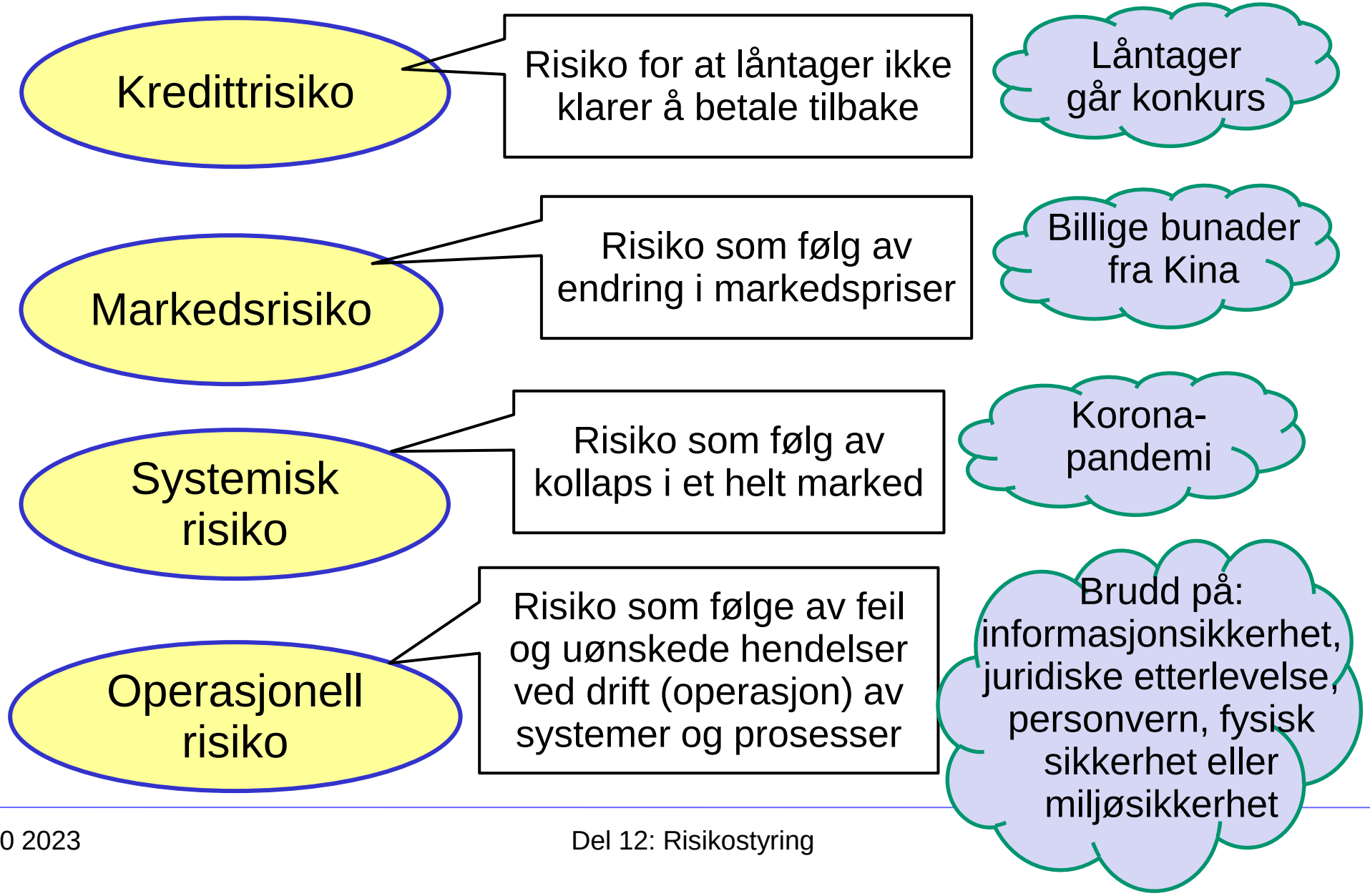
Audun Jøsang
Universitetet i Oslo

Oversikt: Risikostyring



a. Hva er risiko?
b. Risikostyring
c. Risikovurdering
d. Risikohåndtering

Typer av Risiko

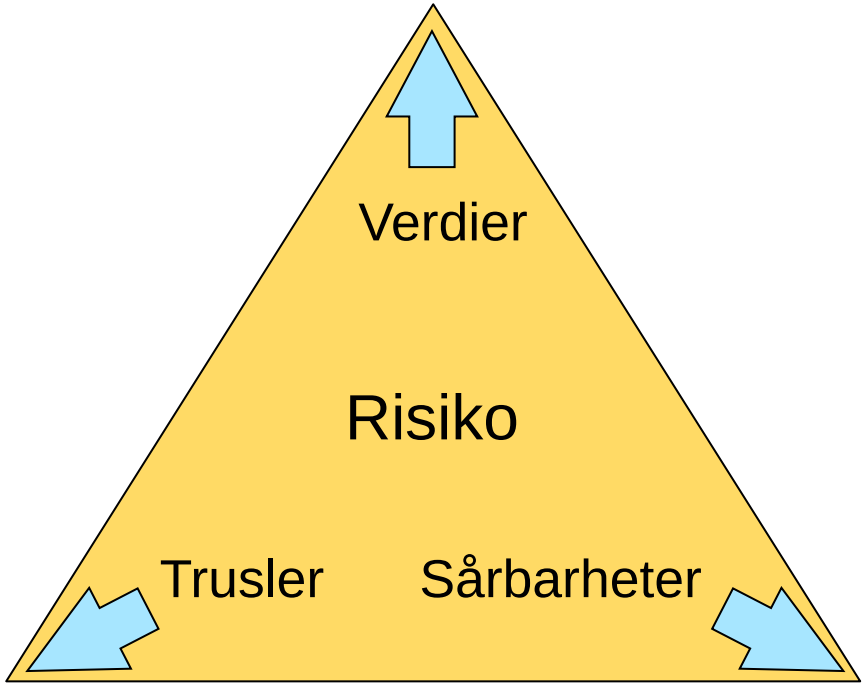


Hva er risiko, og IS-risiko?

- ISO 31000 Risikostyring og ISO 27000 Oversikt og begreper
  - **"Risiko er effekten av uvisshet rundt oppnåelse av målsettinger"**
  - Intet skille mellom positive og negative effekter av uvisshet
  - Svært generell og abstrakt definisjon, uegnet for IS-risikovurdering
  - Men ISO 31000 sier også: Risiko uttrykkes ofte som en kombinasjon av sannsynligheten for en hendelse og dens konsekvens.

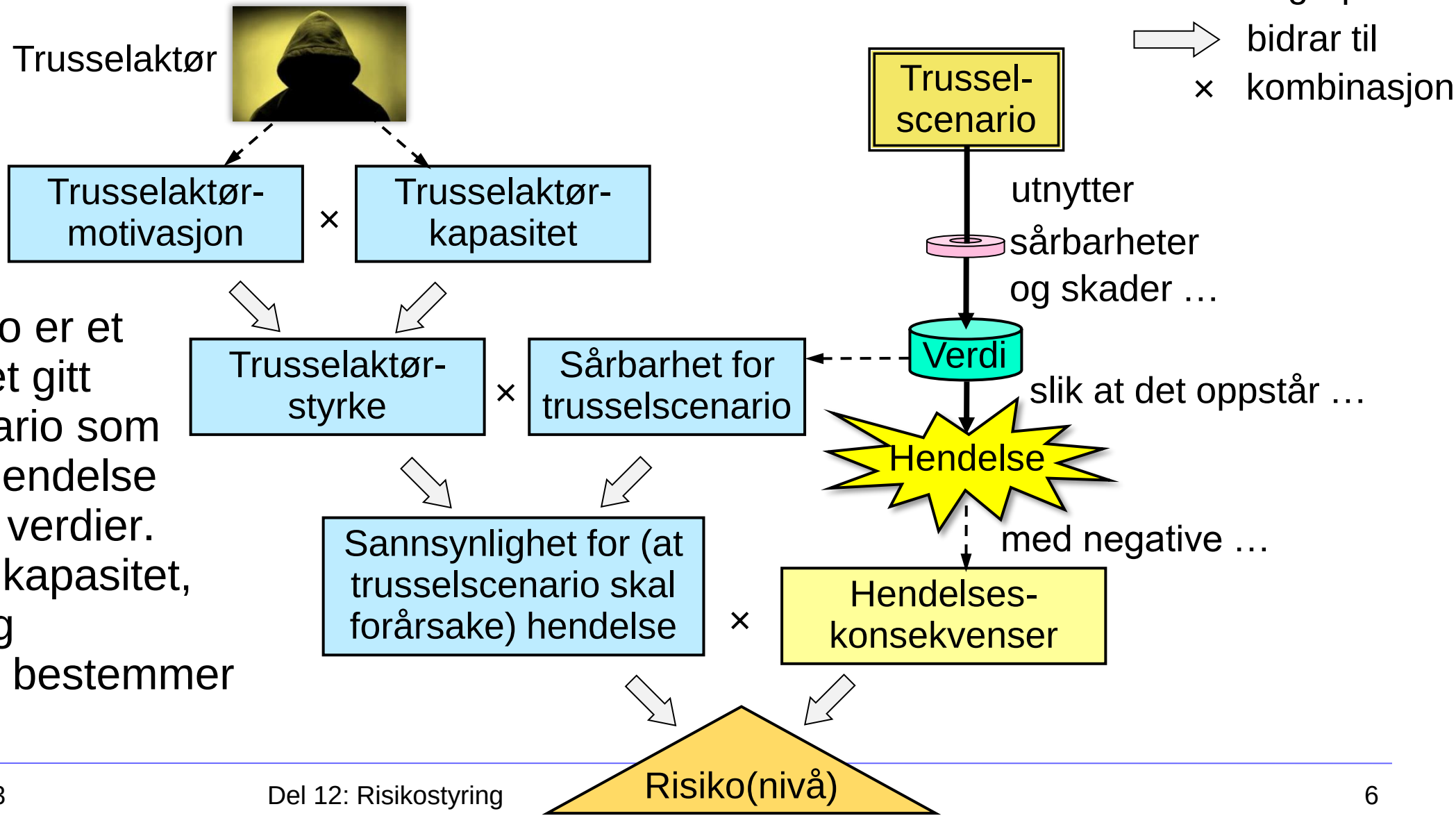
- ISO/IEC 27005 (Informasjonssikkerhetsrisiko)
  - Gjentar definisjonen fra ISO 31000, men gir også en spesifikk definisjon for informasjonssikkerhet:
  - **"Informasjonssikkerhetsrisiko er potensialet for at en gitt trussel vil utnytte sårbarheter rundt verdier og dermed skade organisasjonen."**

Generell risikomodell (NSM)



- Generell modell for risiko
  - Jo større verdier, jo større trusler, og jo mer alvorlige sårbarheter, desto større risiko er du utsatt for.

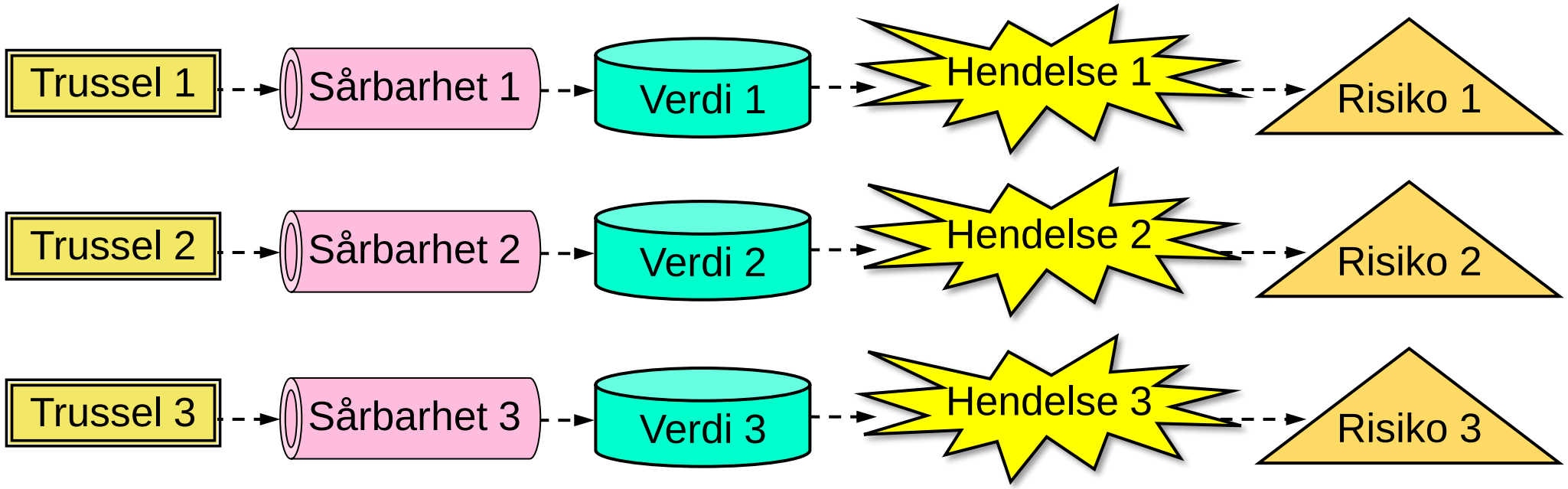
Detaljert risikomodell



- Enhver risiko er et resultat av et gitt trusselscenario som fører til en hendelse som skader verdier.
- Motivasjon, kapasitet, sårbarhet og konsekvens bestemmer risikonivået.

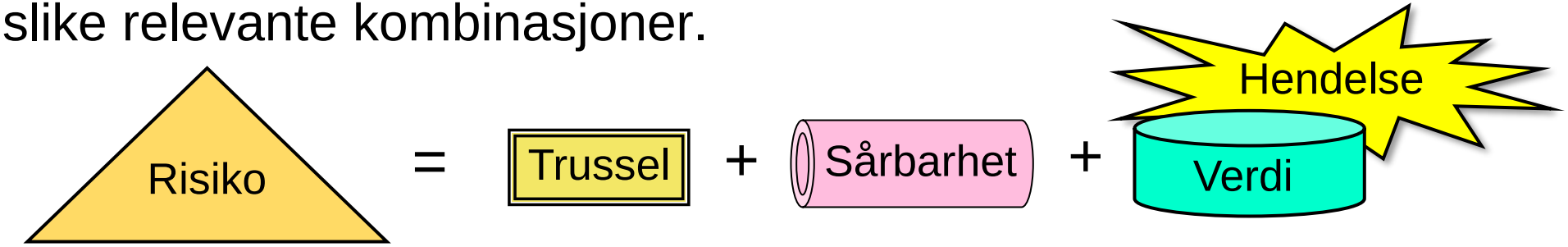
Mange risikoer

- Flere ulike trusler (scenarier) kan identifiseres
- Hver trussel kan utnytte sårbarheter og forårsake en hendelse
- Hver potensielle hendelse kan skade en verdi og ha negativ konsekvens
- Mange trusler ⇒ mange risikoer

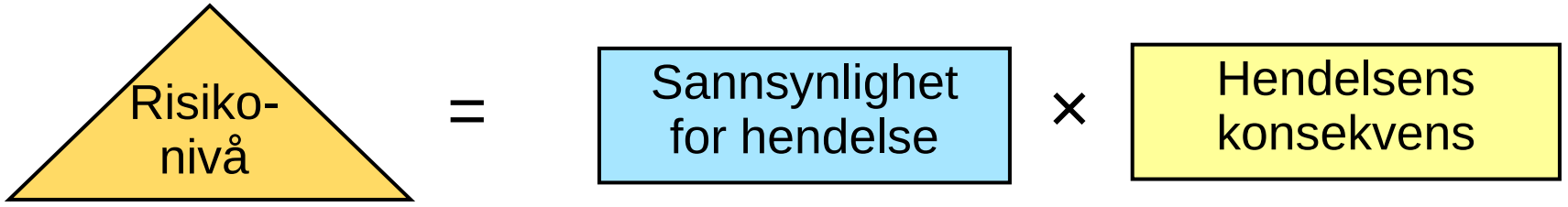


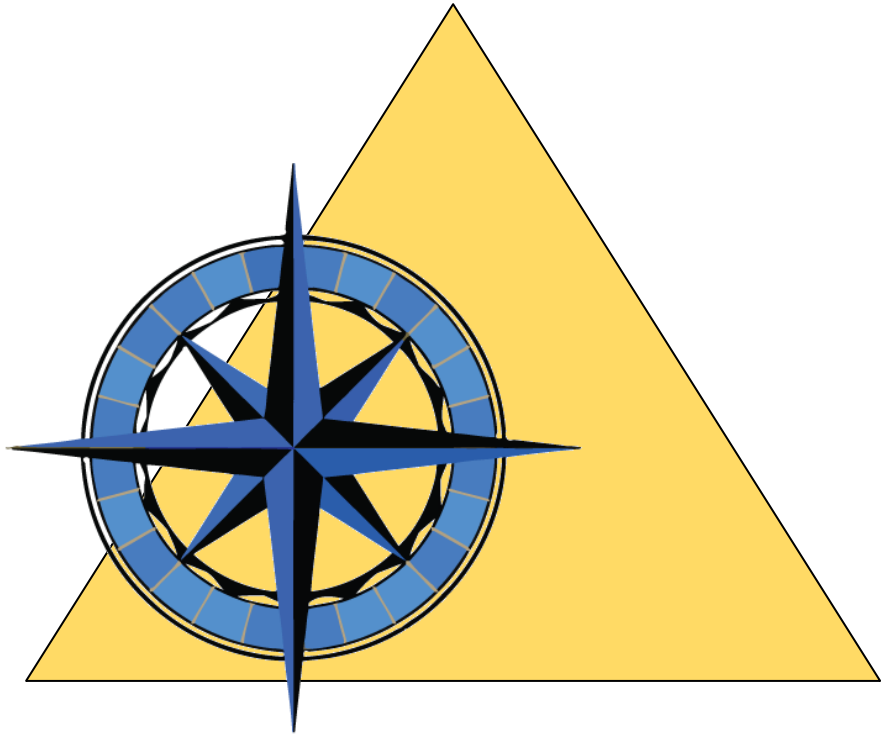
Risiko eller risikonivå?

- I dagligtale er det liten forskjell på «risiko» og «risikonivå»
  - *Hva er risikoen (risikonivået) for å bli hacket med banktrojaner?*
- På fagspråket er den en klar forskjell:
  - **Risiko** er en relevant kombinasjon av trussel / sårbarhet / hendelse som utgjør et brudd på KIT + P for en verdi. Risikoidentifisering er å kartlegge slike relevante kombinasjoner.



  - **Risikonivå** (også kalt risikoeksponering) er kombinasjonen av hendelsens sannsynlighet og konsekvens. Risikonivå beregnes med risikoanalyse.



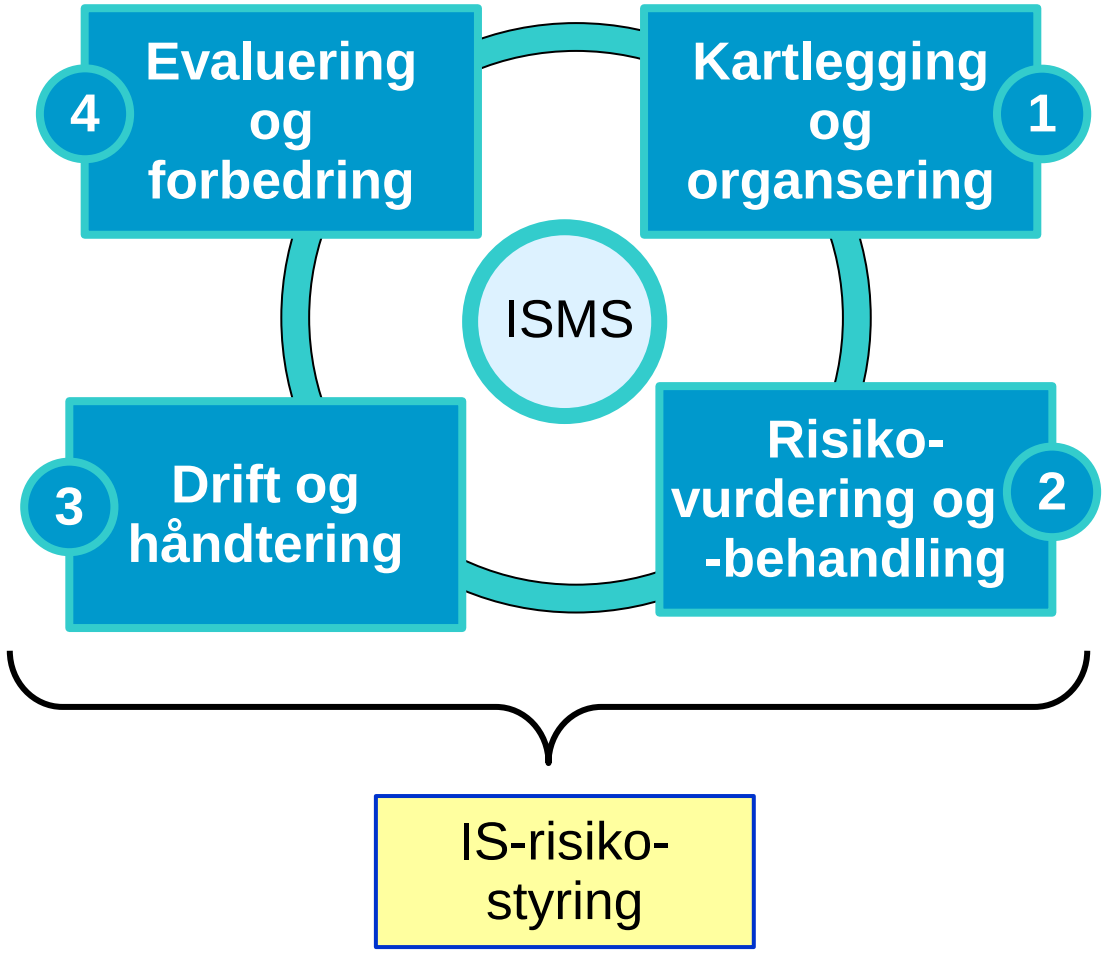


Del b: Risikostyring

Standarder for risikostyring

- ISO 31000 Risikostyring
- ISO/IEC 27005 Risikostyring for informasjonssikkerhet
- NIST SP800-39 Managing Information Security Risk
- NIST SP800-30 Guide for Conducting Risk Assessment
- NS 5814 Krav til risikovurdering
- NS 5831 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger –Risikohåndtering
- NS 5832 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

IS-risikostyring → ISMS integrering



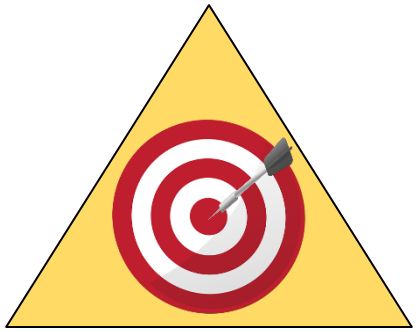
Hva er risikostyring?

- «Risikostyring består av koordinerte aktiviteter for å styre og lede en organisasjon med hensyn til risiko. » (ISO 31000)

- «Risikostyring for informasjonssikkerhet er å analysere hva som kan skje, og mulige konsekvenser, før man bestemmer hva som bør gjøres og når, for å redusere risikoen til et akseptabelt nivå. » (ISO/IEC 27005)

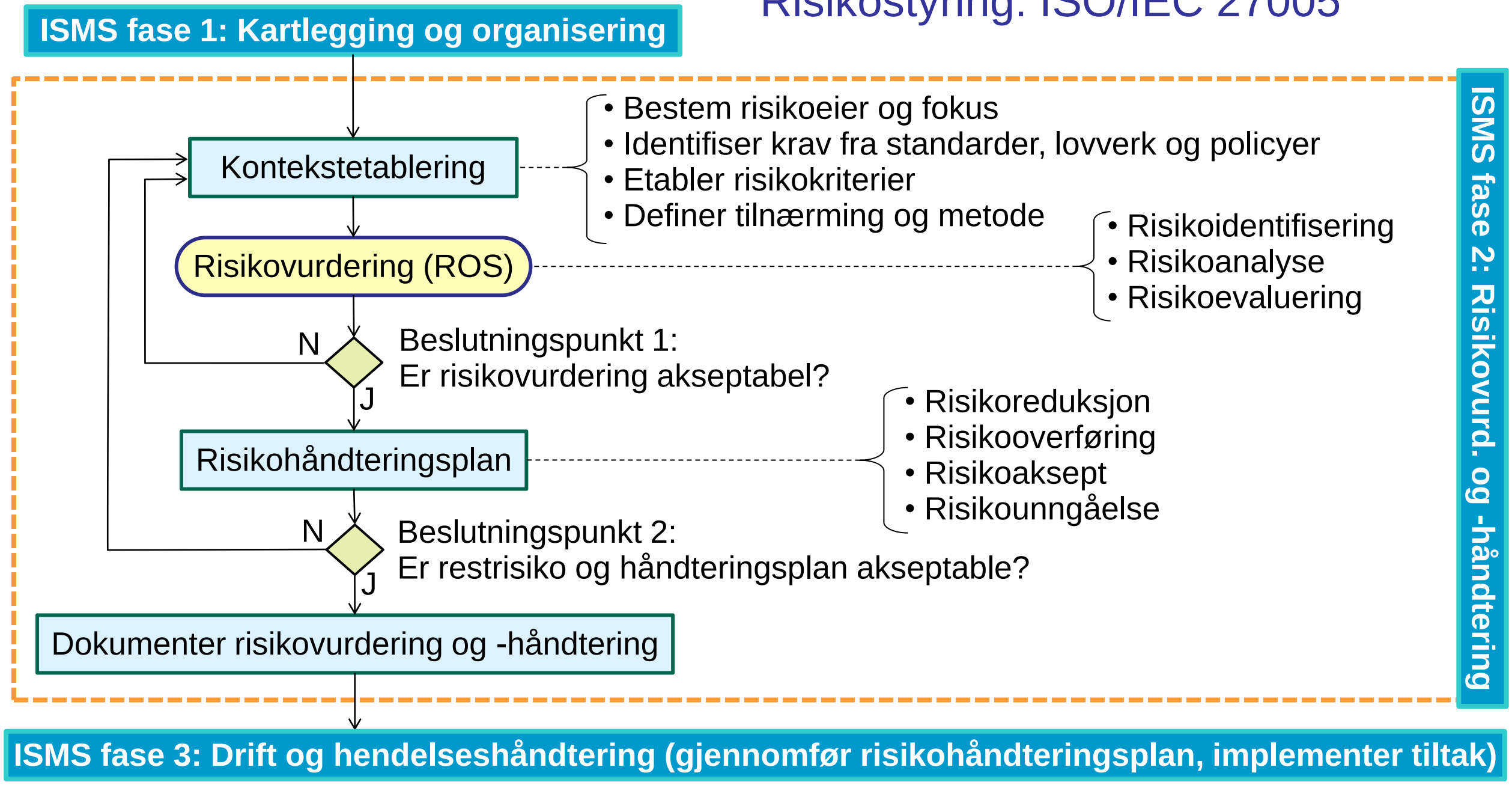
Målsettinger for risikostyring

Aktiviteter innen risikostyring kan ha ulike målsettinger.
Det kan f.eks. være en eller flere av følgende:

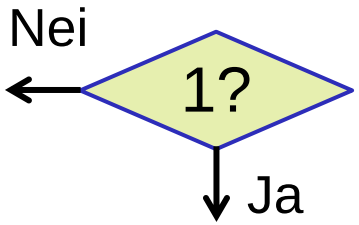


- å få oversikt over trusler
- å få oversikt over sårbarheter
- å få oversikt over eksisterende risikoer
- å foreslå nye sikkerhetstiltak
- å vurdere restrisiko etter nye foreslåtte sikkerhetstiltak
- å gi grunnlag for å kjøpe cyberforsikring
- å gi grunnlag for budsjett for håndtering av risiko

Risikostyring: ISO/IEC 27005



Beslutningspunkt 1



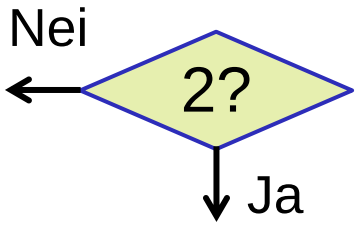
Er risikovurderingen tilfredsstillende?

Grunner for å svare "Nei", og hvordan det kan rettes.

a. Relativt dårlig spredning av risikonivåer.
   - Spredningen kan forbedres med rekalibrering av sannsynlighet eller konsekvensnivåer.

b. For stor uvisshet rundt en eller flere høye risikoer.
   - Uvissheten kan reduseres ved å gjøre en mer grundig vurdering av disse risikoene.

Beslutningspunkt 2



Er håndteringsplanen akseptabel?

Grunner for å svare "Nei", og hvordan det kan rettes.

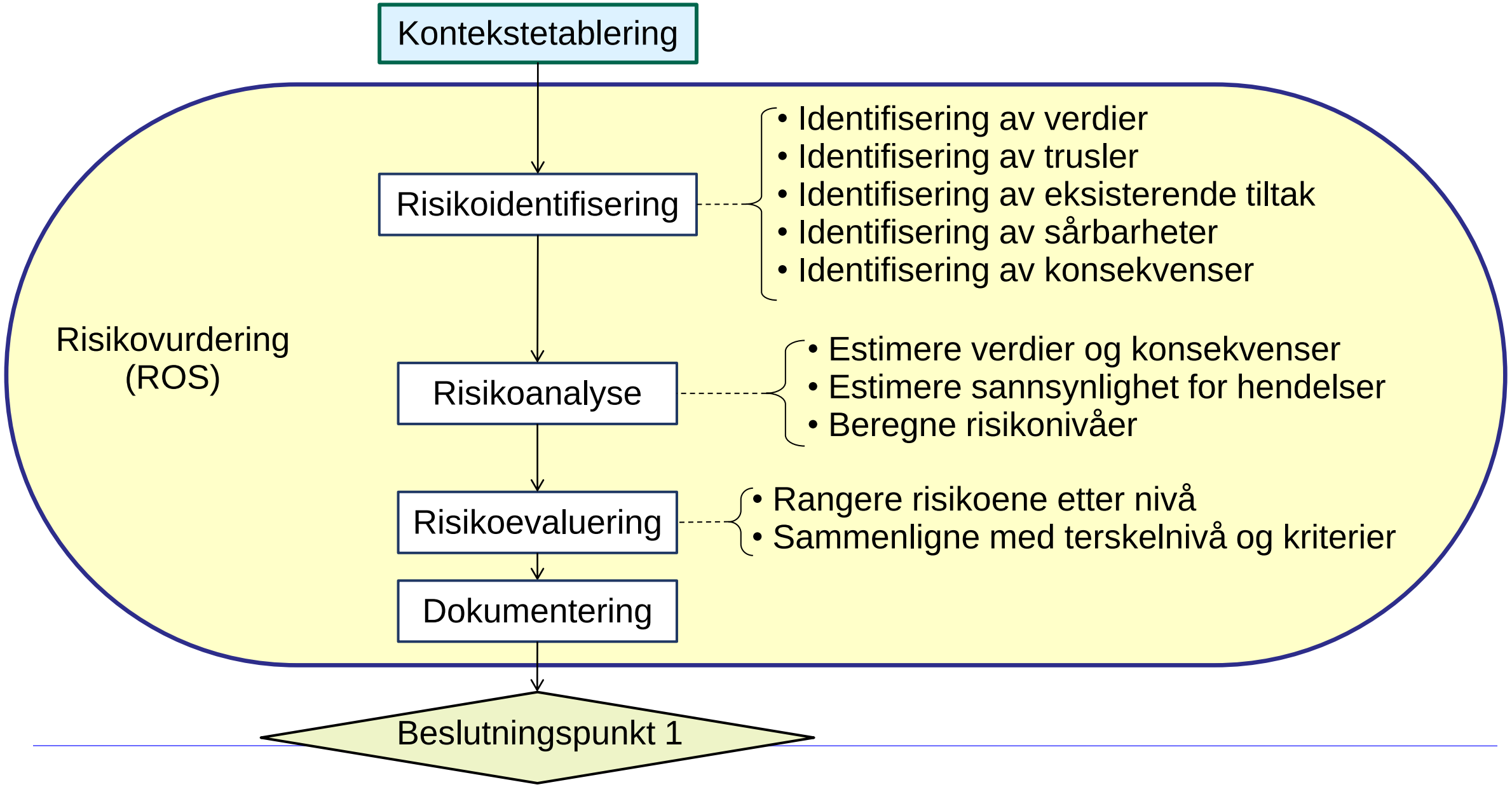
a. For høy restrisiko
   - Høy restrisiko kan senkes ved å implementere flere tiltak.
   - Høy restrisiko kan defineres som passe ved å heve risikoterskel.

b. For lav restrisiko
   - Lav restrisiko kan heves ved å implementere færre tiltak.
   - Lav restrisiko kan defineres som passe ved å senke risikoterskel.

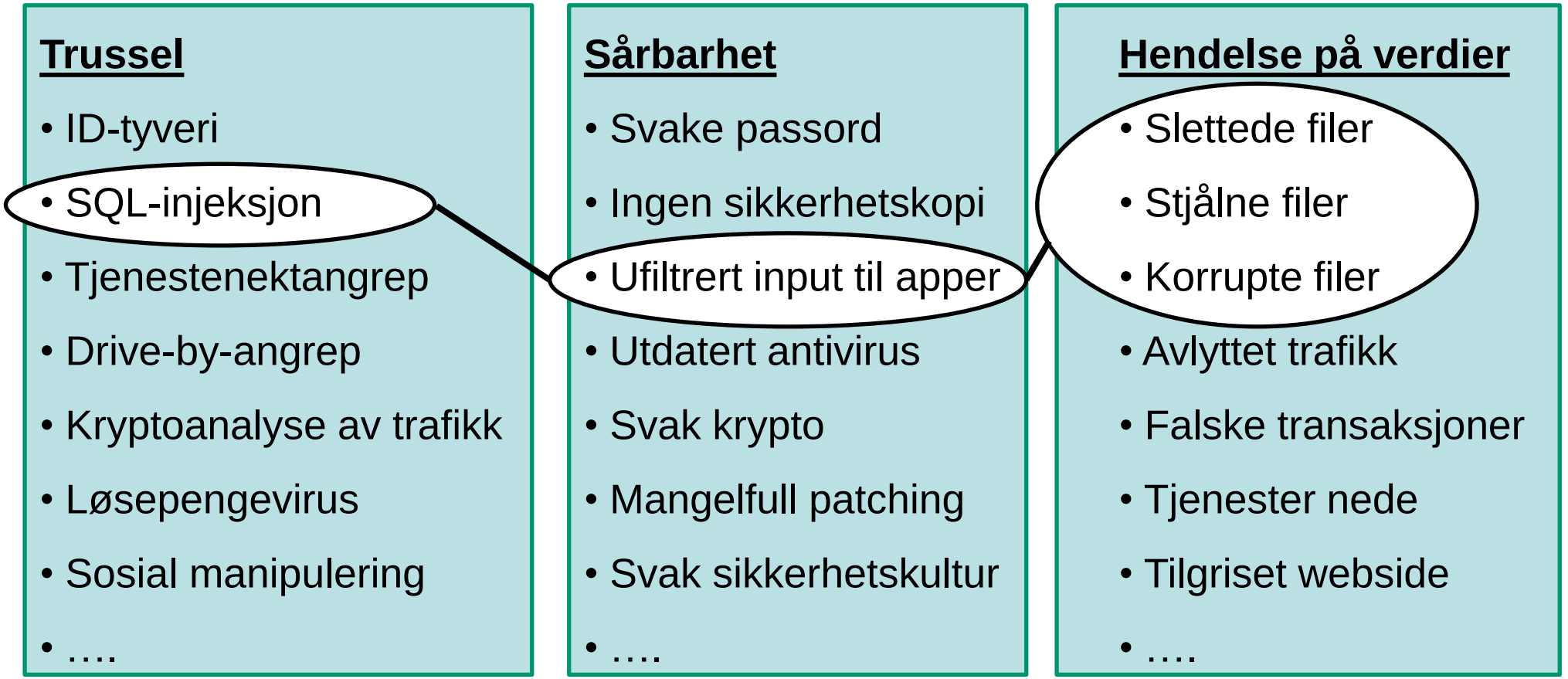
c. Passe restrisiko, men utilstrekkelig budsjett til å innføre foreslåtte risikoreduserende tiltak.
   - Tilpass budsjett ved å øke budsjettet eller kutte tiltak.

Del c: Risikovurdering (ROS-analyse)

Prosess for risikovurdering – ISO/IEC 27005

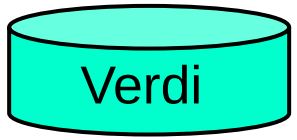


Risikoidentifisering



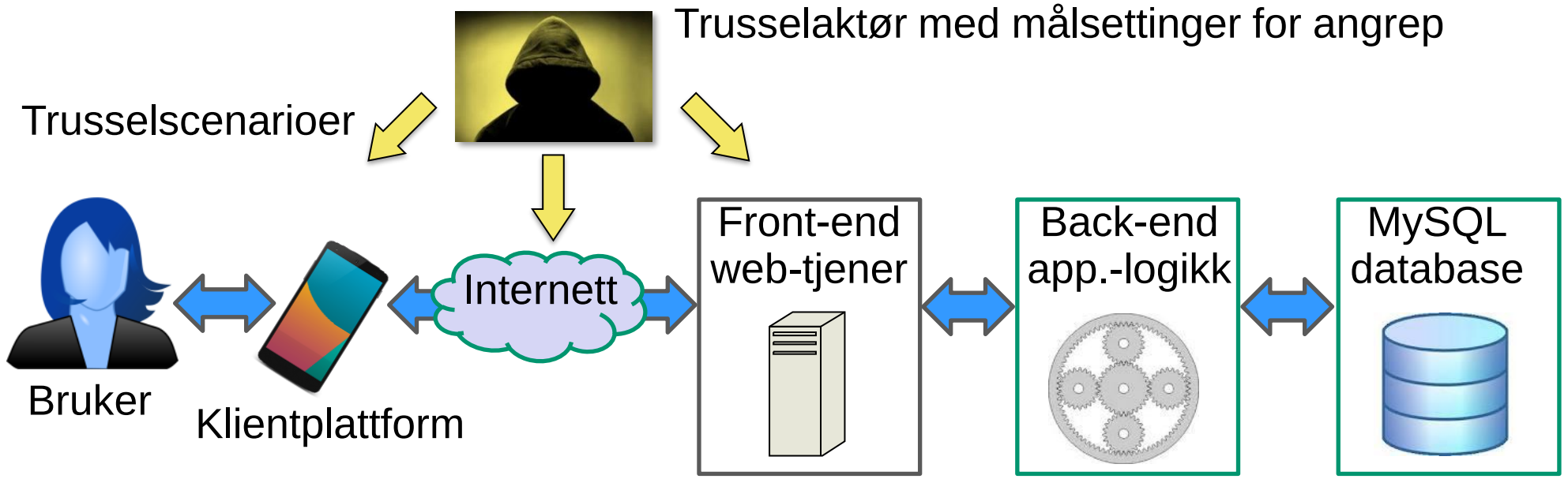
- Å identifisere en risiko betyr å finne en relevant kombinasjon av en trussel, sårbarhet(er) og hendelse(r) som kan skade verdier.

Kartlegging av verdier / ressurser



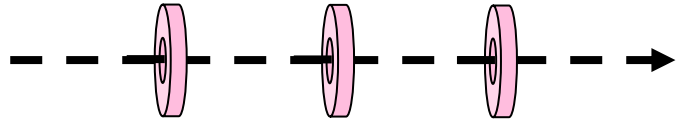
- Bredt spekter av verdier / ressurser
  - Driftsdata, persondata, system, nettverk, applikasjoner, prosesser, tjenester, etc.
- Umulig å skaffe total oversikt
  - Det er heller ikke viktig med total oversikt
  - Trusselmodelleringen vil peke ut relevante verdier
- Ansvar for å identifisere verdier ligger hos eiere
  - Derfor må eiere delta i risikovurdering
- For hver verdi bør det det spesifiseres
  - Viktighet av sikkerhetsmålsettinger (KIT + P)
  - Mulige konsekvenser for brudd på sikkerhetsmål

Trusselmodellering



- Trusselmodellering består av å identifisere, analysere og beskrive relevante angreps-scenarier.
- Utfordringen er å identifisere relevante trusler
- Tenk: Hva kan skje? Hvordan kan våre verdier skades?
  Hvem kunne være interessert i å skade oss?

Sårbarheter



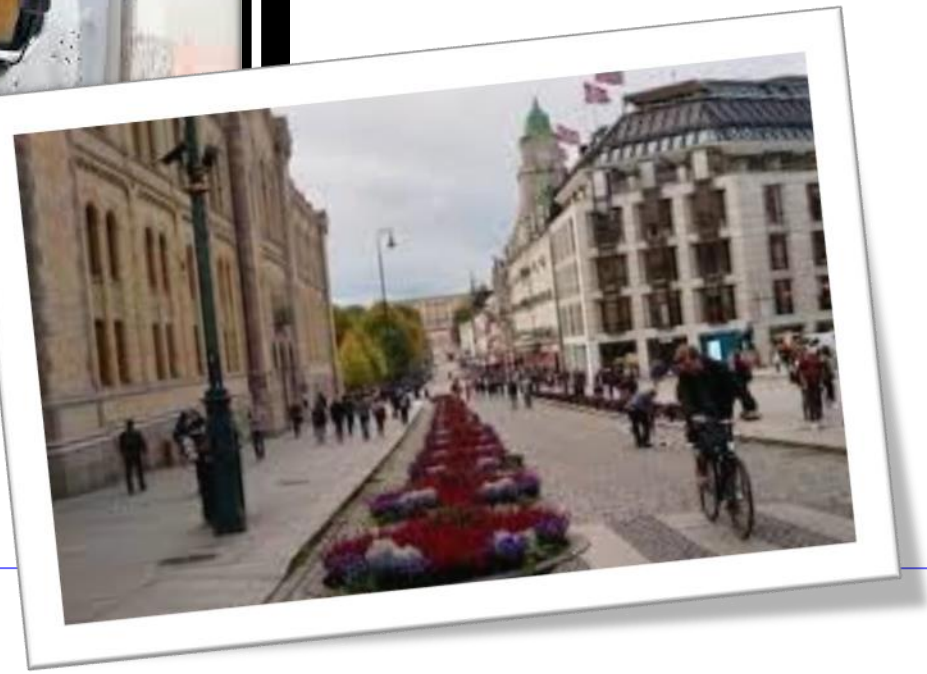
- Sårbarheter er muligheter som trusselaktører kan utnytte for å angripe systemer og informasjonsressurser.
- Generell identifisering av sårbarheter
  - Å identifisere en sikkerhetssårbarhet er det samme som å finne ut hvordan man kan stoppe et bestemt trusselscenario.
  - Fjerning av en sikkerhetssårbarhet er å blokkere en trussel.
  - En sårbarhet er **fravær av, eller svakhet i tiltak** mot en trussel.
  - Å stoppe trusler (dvs. å fjerne sårbarheter) gjøres med sikkerhetstiltak.
- Identifikasjon av sårbarheter med verktøy og sjekklister
  - Sårbarhetsskannere er automatiserte verktøy for å oppdage kjente sårbarheter i nettverk og systemer,
  - Sjekklister over sårbarheter brukes under risikovurdering og som del av arbeid med å fjerne sårbarheter, for eksempel med «OWASP Top 10».

Ingen sårbarhet uten en trussel

Karl Johans gate
Oslo

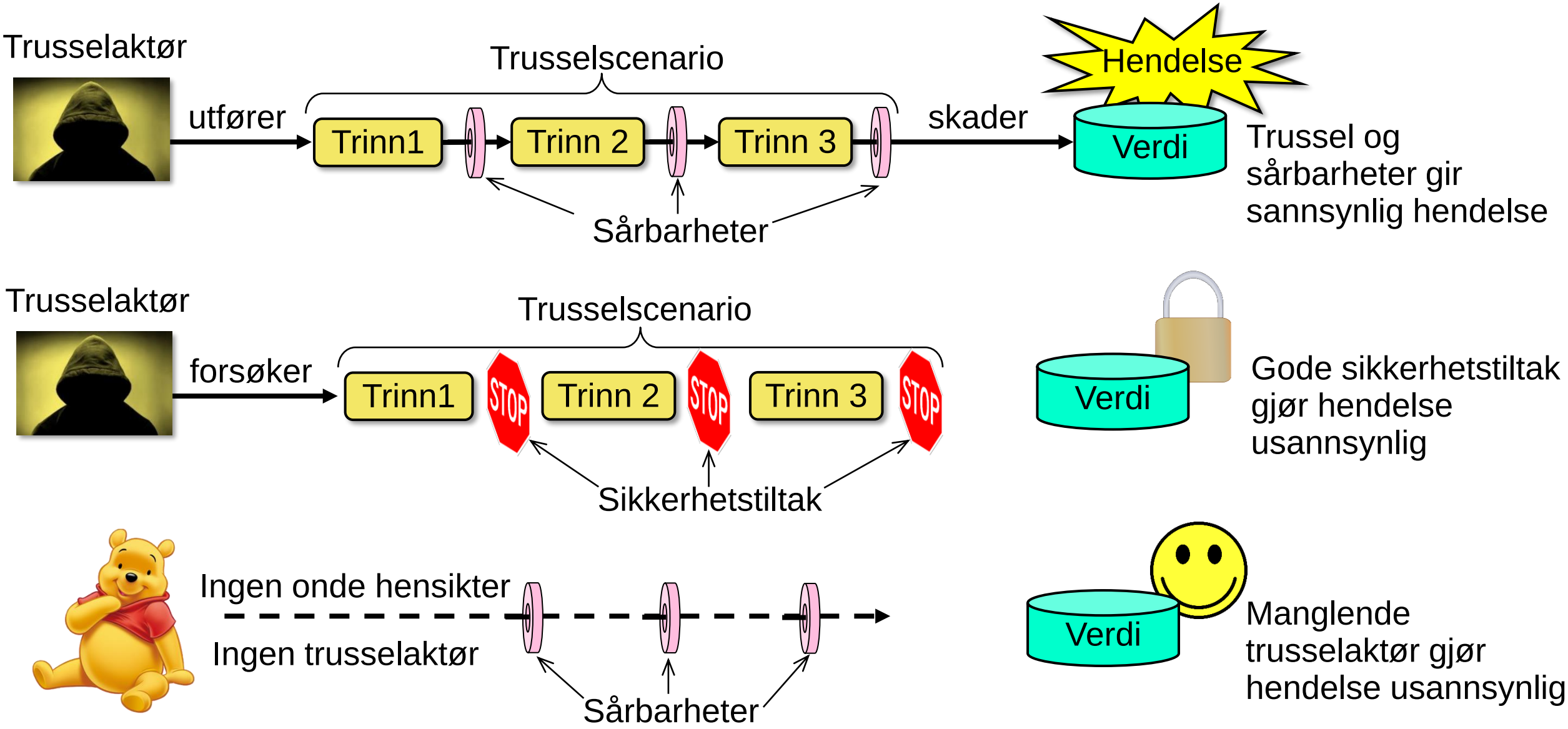
Nice
Berlin
London
Barcelona

Ny trussel oppstod i 2016

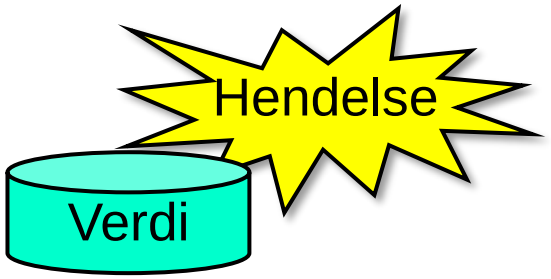


Trussel blokkert
(dvs. sårbarhet fjernet)

Sannsynlighet for at en hendelse inntreffer



Vurdering av konsekvenser



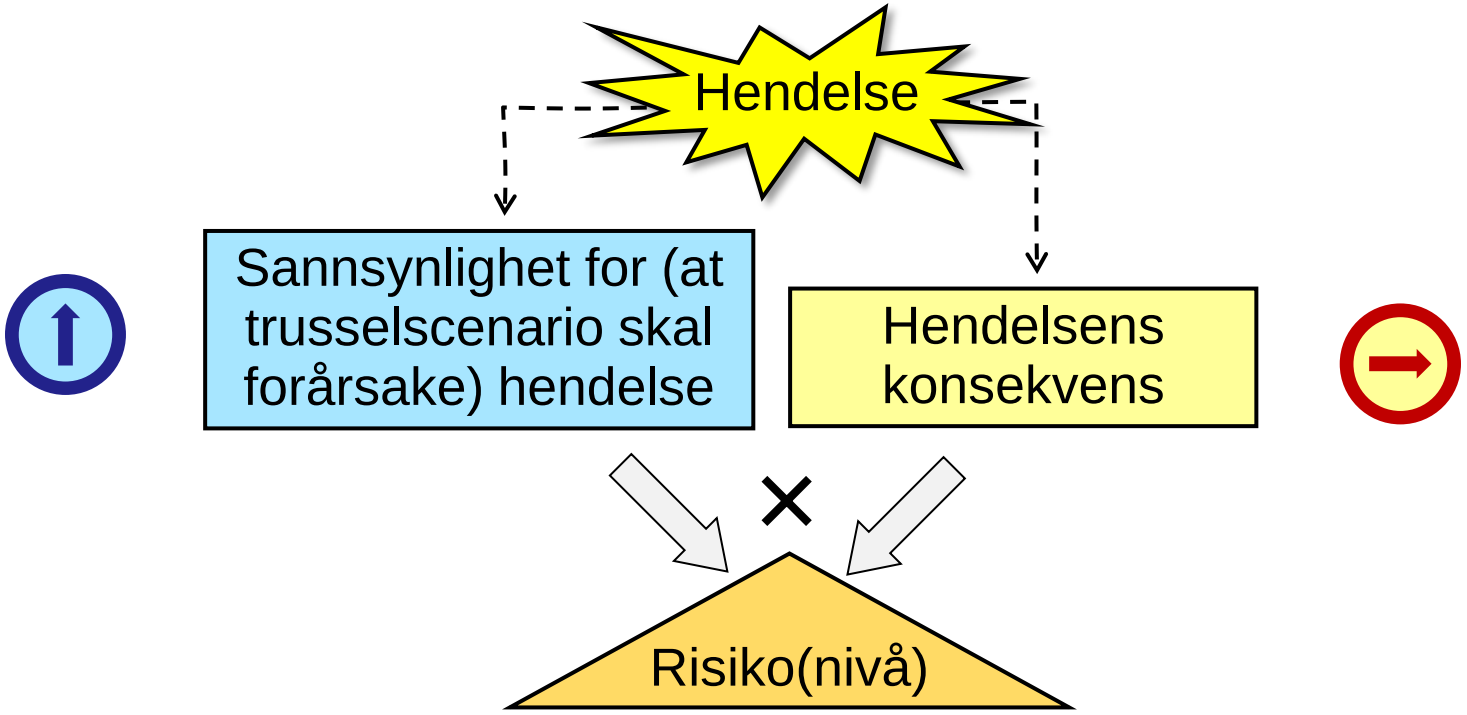
- En hendelse fører til brudd på sikkerhetsmål for verdier
  - **Brudd på sikkerhetsmål:** KIT + P for verdier
    (konfidensialitet, integritet, tilgjengelighet, personvern)
- Konsekvensnivået estimeres for hver type hendelse
- Konsekvenser kan bestå av ulike aspekter:
  - Redusert omsetning/profitt, tap
  - Svekket ytelse av tjeneste
  - Brudd på juridisk etterlevelse, advokatutgifter, erstatning, bøter §
  - Skadet omdømme
  - Kostnader ved håndtering og gjenoppretting
  - Belastning på ansatte og brukere

Konsekvensaspektene vurderes som helhet. Den høyeste (mest alvorlige) konsekvens er tilnærmet lik helhetlig konsekvens.

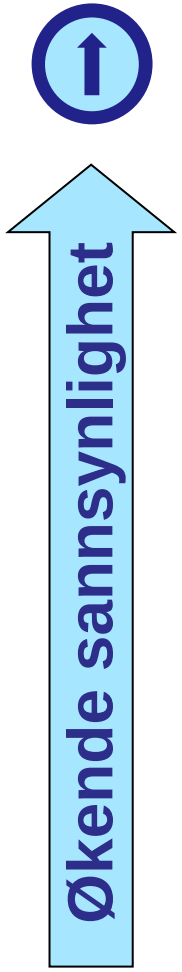
Risikoanalyse

Praktisk risikoanalyse vurderer vanligvis to faktorer for å bestemme nivået på hver risiko

- Sannsynlighet (frekvens/tenkelighet) for hver type hendelse
- Konsekvens for verdier som følge av hver type hendelse



Kvalitativ sannsynlighetsskala



Sannsynlighet	Beskrivelse
(5) Svært høy	Det fins motiverte trusselaktører som med letthet kan nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet for denne risikoen. En hendelse er antagelig allerede i ferd med å skje, eller vil skje om kort tid.
(4) Høy	Motiverte trusselaktører vil med høy sannsynlighet nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet. En hendelse kan inntreffe noen ganger per måned.
(3) Betydelig	Trusselaktører har en betydelig mulighet til å nå sitt mål ved å bruke det vurderte trusselscenarioet. En hendelse kan inntreffe noen ganger per år.
(2) Lav	Trusselaktører har relativt liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. Det vil antagelig gå flere år mellom hver hendelse.
(1) Usannsynlig	Trusselaktører har svært liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. Det vil kanskje aldri skje en hendelse.

- Skalaen over er et eksempel. Antall nivåer og fortolkning defineres etter behov.

Kvalitativ konsekvensskala

Konsekvensnivå	Beskrivelse
(5) Svært alvorlig	Svært alvorlig skade på verdier, paralyserende tjenestavbrudd , svært stort økonomisk tap og mulig konkurs. Gjenoppretting krever langvarig arbeid med store ressurser. Eksterne funksjoner som avhenger av virksomheten kan falle bort i lang periode.
(4) Alvorlig	Alvorlig skade på verdier som kan medføre alvorlig tjenesteavbrudd og stort økonomisk tap. Det kreves store ressurser for å håndtere hendelsen. Funksjoner utenfor den berørte virksomheten kan bli negativt påvirket, men uten langvarige konsekvenser.
(3) Betydelig	Betydelig skade på verdier som kan medføre betydelig tjenesteavbrudd og betydelig økonomisk tap. Gjenoppretting og tjenestekontinuitet krever betydelig arbeid. Funksjoner utenfor virksomheten blir sannsynligvis lite påvirket.
(2) Liten	Relativt liten skade på verdier som kan true kvalitet av drift, og antagelig lite eller intet tjenesteavbrudd. Bare lite økonomisk tap. Håndteres greit med moderate ressurser.
(1) Ubetydelig	Ubetydelig skade på verdier, uten tjenesteavbrudd. Hendelsen håndteres relativt lett som del av rutinemessig drift. Lite eller intet økonomisk tap.

- Skalaen over er et eksempel, der nivåer og fortolkning kan defineres etter behov.

Risikomatrise for kvalitativ risikoberegning

Risikomatrisen er en oppslagstabell med forhåndsdefinerte risikonivåer i hver celle

Kvalitative konsekvensnivåer

Kvalitativ sannsynlighet

Kvalitative risikonivåer	(1) Ubetydelig	(2) Liten	(3) Betydelig	(4) Alvorlig	(5) Sv. alvorlig
(5) Svært høy	**(3) M**	**(4) S**	**(4) S**	**(5) SS**	**(5) SS**
(4) Høy	**(2) L**	**(3) M**	**(4) S**	**(4) S**	**(5) SS**
(3) Betydelig	**(2) L**	**(2) L**	**(3) M**	**(4) S**	**(4) S**
(2) Lav	**(1) SL**	**(2) L**	**(2) L**	**(3) M**	**(3) M**
(1) Usannsynlig	**(1) SL**	**(1) SL**	**(2) L**	**(2) L**	**(2) L**

Tolkning av risikonivåer:

- **(5) SS:** Svært stor risiko, må behandles med høy prioritet
- **(4) S**: Stor risiko, skal vanligvis behandles
- **(3) M:** Moderat risiko, behandling og tiltak bør vurderes
- **(2) L:** Liten risiko, kan vanligvis aksepteres
- **(1) SL:** Svært liten risiko, kan ignoreres

Regneark for risikovurdering

- Mange ulike veiledere, maler og verktøy for risikovurdering
  - ➢ Ofte relativt komplisert, krever opplæring for å bruke
- Kvalitative risikomatriser er tilnærmet additive
  - – Risiko ≈ (Sannsynlighet + Konsekvens) / 2
  - ➢ UiO digital sikkerhet har enkelt regneark med kvalitativ risikoberegning:

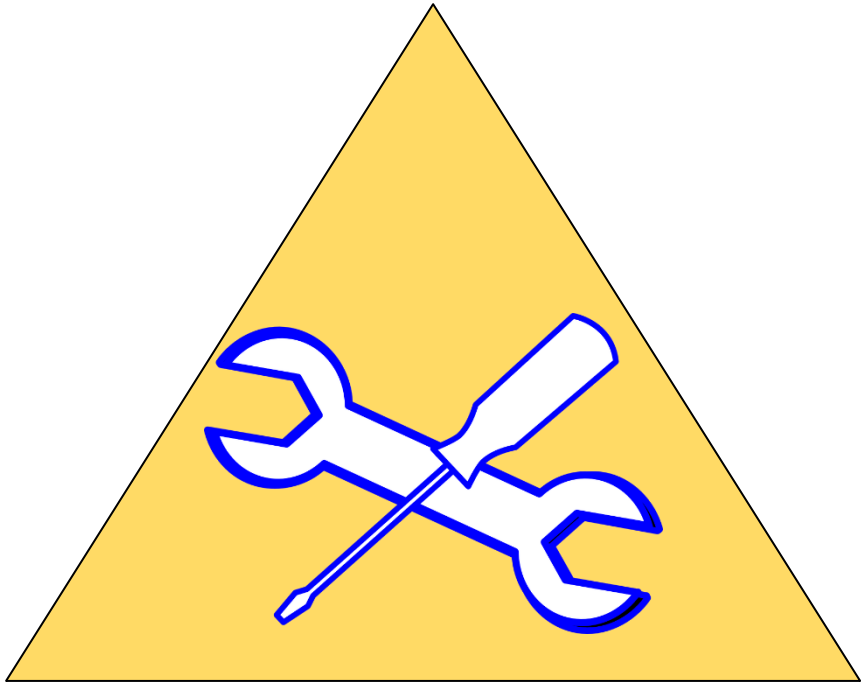
https://www.mn.uio.no/ifi/forskning/grupper/sec/laeringsressurser/uio-risikovurdering-kvalitativ.xlsx

Forklaring av regneark

- Trussel
  - Trusselscenario og eventuelt trusselaktør
- Sårbarhet
  - Hvilke svakheter og feil som gjør at trusselscenarioet kan gjennomføres
- Berørte verdier
  - Beskriver hendelse (brudd på sikkerhetsmål)
- Konsekvenser
  - Beskriv forventede konsekvenser av hendelsen
- Eksisterende sannsynlighetsreduserende eller konsekvensreduserende tiltak
  - Tiltak som allerede er ment å forhindre trusselscenarioet eller mitigere konsekvenser
- Deteksjon og etterforskning
  - Hvordan kan en slik hendelse (eller trinn i trusselscenariet) oppdages og etterforskes?
- Beregning av risikonivå med regneark
  - a) kvalitativ risiko = (kvalitativ sannsynlighet + kvalitativ konsekvens)/2
  - b) relativ risiko = relativ sannsynlighet × relativ konsekvens
- Anbefalte nye tiltak
  - Forslag til nye sikkerhetstiltak for å forhindre hendelsen eller mitigere konsekvenser

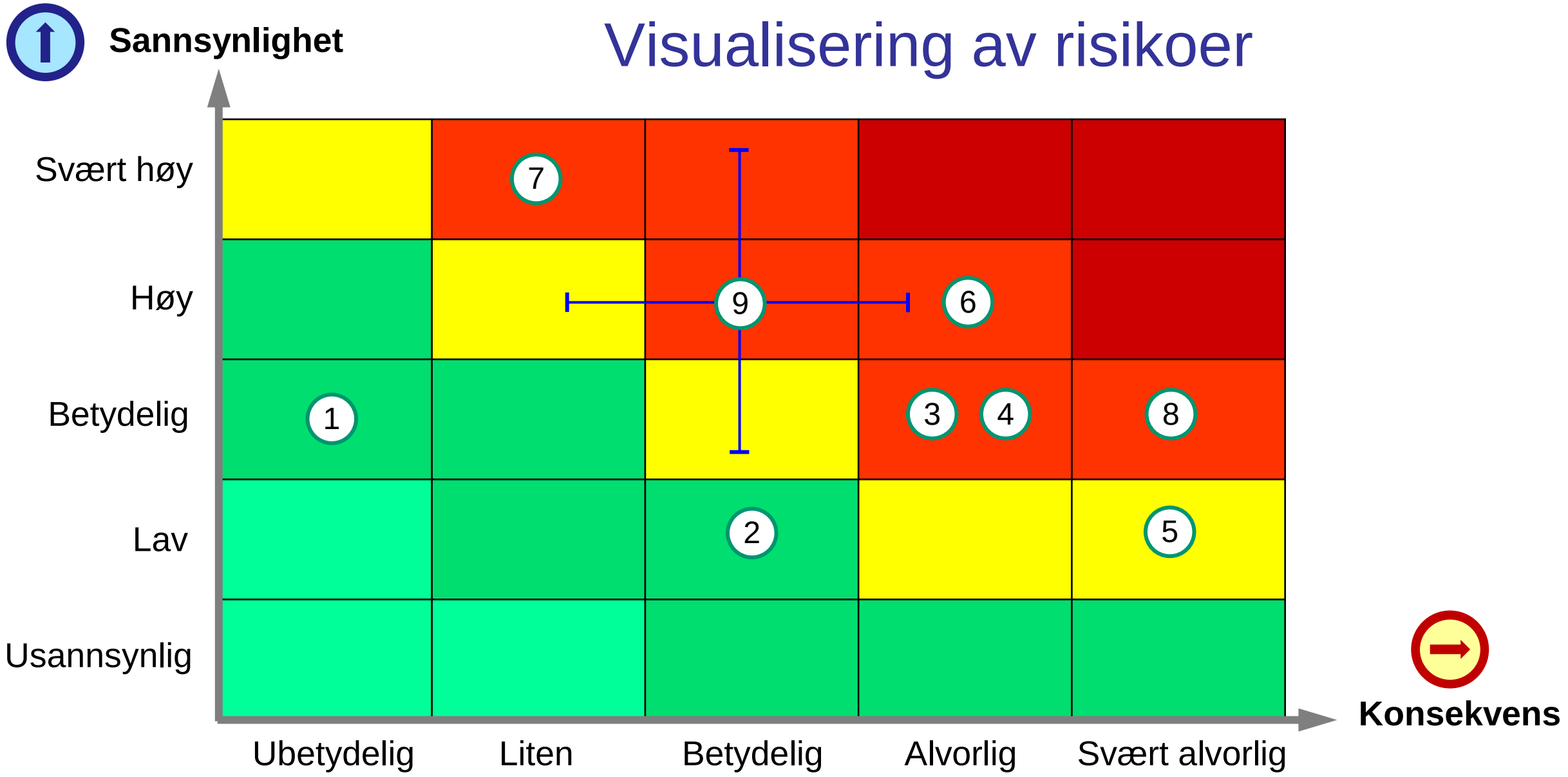
Bruk av regneark

- Antagelser:
  - identifisering av verdier, trusler og sårbarheter gjøres separat
  - estimering av sannsynligheter og konsekvensnivåer gjøres separat
- Risikoberegning kan gjøres både før og etter nye tiltak
  - Risikonivå beregnes i utgangspunktet før nye tiltak
  - Risikonivå kan også beregnes med antagelse om nye tiltak
- Kostnad for nye tiltak er ikke inkludert i regneark
  - Estimering av kostnad for nye tiltak kan beskrives separat
  - Nytte-kost (ROI: Return On Investment) kan beskrives separat, men vil kreve kvantitativ estimering/beregning av (kostnad ved) risikonivå.

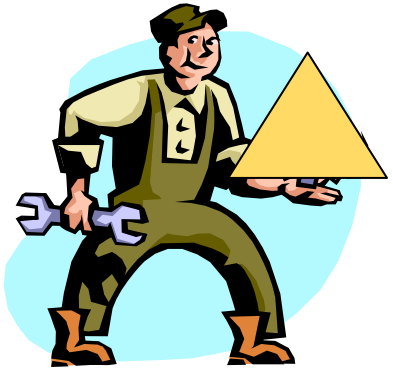


Del d: Risikohåndtering

Visualisering av risikoer



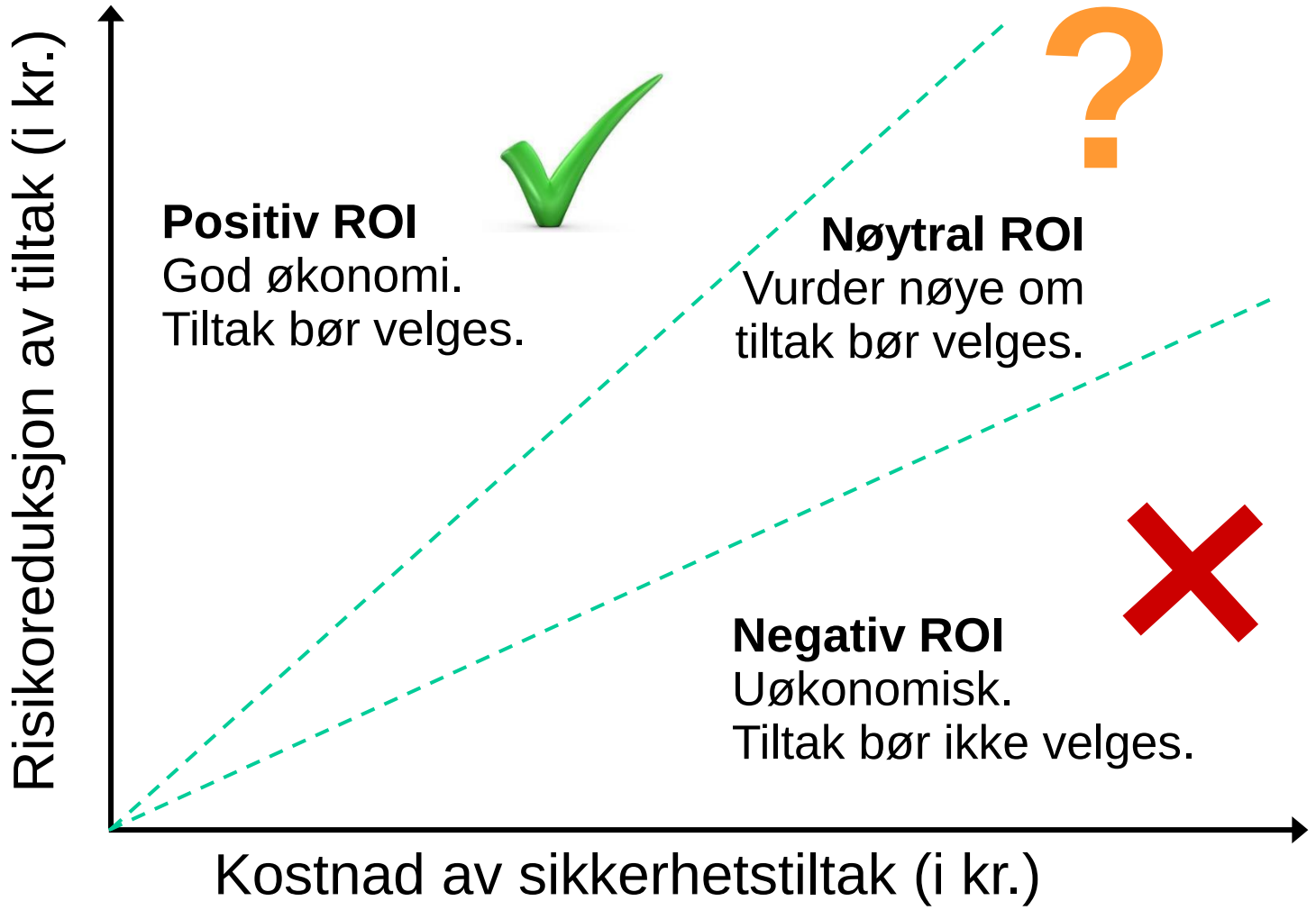
Håndtering av risiko



- Sortere risikoene etter nivå/alvorlighet
- Velg måte å håndtere de mest alvorlige risikoene

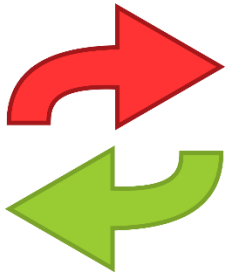
1. Reduser risikoen ved å implementere sikkerhetstiltak. Kan velges fra tiltaksbanker som ISO/IEC 27002, NIST CSF eller NSM Grunnprinsipper.
2. Del / overfør risikoen (outsource aktivitet som forårsaker risikoen). Alternativt, kjøp cyberforsikring.
3. Behold risikoen (forstå og tolerere potensielle konsekvenser)
4. Unngå risikoen (stopp aktivitet som forårsaker risikoen)

ROI av sikkerhetstiltak (Return on Investment)



$$\text{ROI} = \frac{\text{Risikoreduksjon} - \text{Kostnad}}{\text{Kostnad}}$$

Deling / overføring av risiko



- Alternativ for risikohåndtering som har til hensikt å dele eller flytte risiko over til andre enheter, prosesser eller organisasjoner
- Organisasjonen kan f.eks. overføre risiko knyttet til drift av komplekse systemer til en annen organisasjon med større kompetanse på å håndtere disse risikoene
- Alternativt kan organisasjonen kjøpe forsikring mot potensielle tap forårsaket av sikkerhetshendelser, som kalles cyberforsikring.

Beholde risiko

- Alternativ som består i å ikke gjøre noe for å håndtere en risiko videre, som dermed betyr å akseptere risikoen slik den er.
- Forsvarlig bare når risikonivået er relativt lavt i forhold til kostnadene med behandling / innføring av tiltak.
- Risikoappetitt beskriver i hvilken grad organisasjonen er villig til å akseptere risiko som en avveining i forhold til kostnadene med behandling.

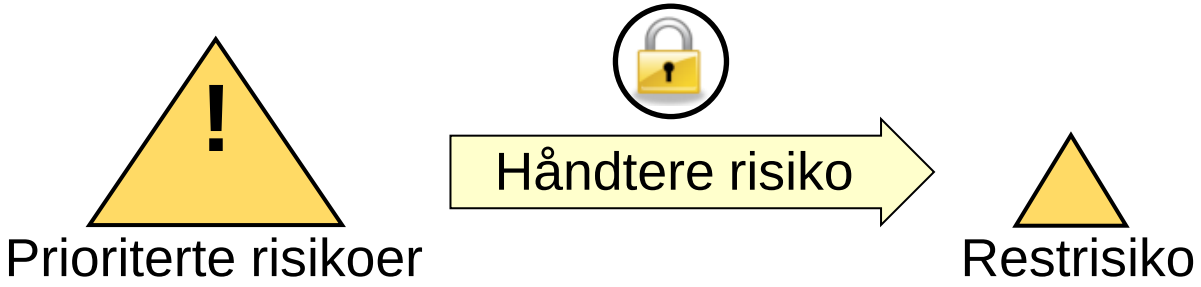
Risikounngåelse

- Enhver forretningsaktivitet medfører en viss risiko, men nytten og fortjeneste oppveier normalt risikoen.
- I tilfelle risikoen er for høy sammenlignet med nytten og fortjenesten, og det ikke er mulig å redusere, mitigere, overføre eller beholde risikoen, er siste utvei å stoppe forretningsaktiviteten som medfører risiko.

- Vær oppmerksom på risikoen for tapt nytte og fortjeneste ved å ikke drive en forretningsaktivitet.

Risikohåndtering og restrisiko

- For hver prioriterte risiko, identifiser potensielle tiltak eller annen håndtering som vil redusere risikoen.



- Restrisiko er den risiko som gjenstår etter håndtering.

- Det er en ledelsesbeslutning å akseptere restrisiko. Den aksepterte restrisiko skal være forsvarlig i henhold til virksomhetens risikostrategi.

Slutt på presentasjon