IN2120 – Informasjonssikkerhet

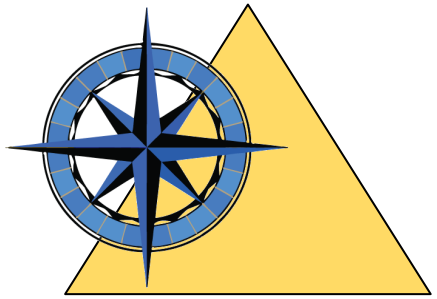
Risikostyring for cybersikkerhet

Janne Hagen



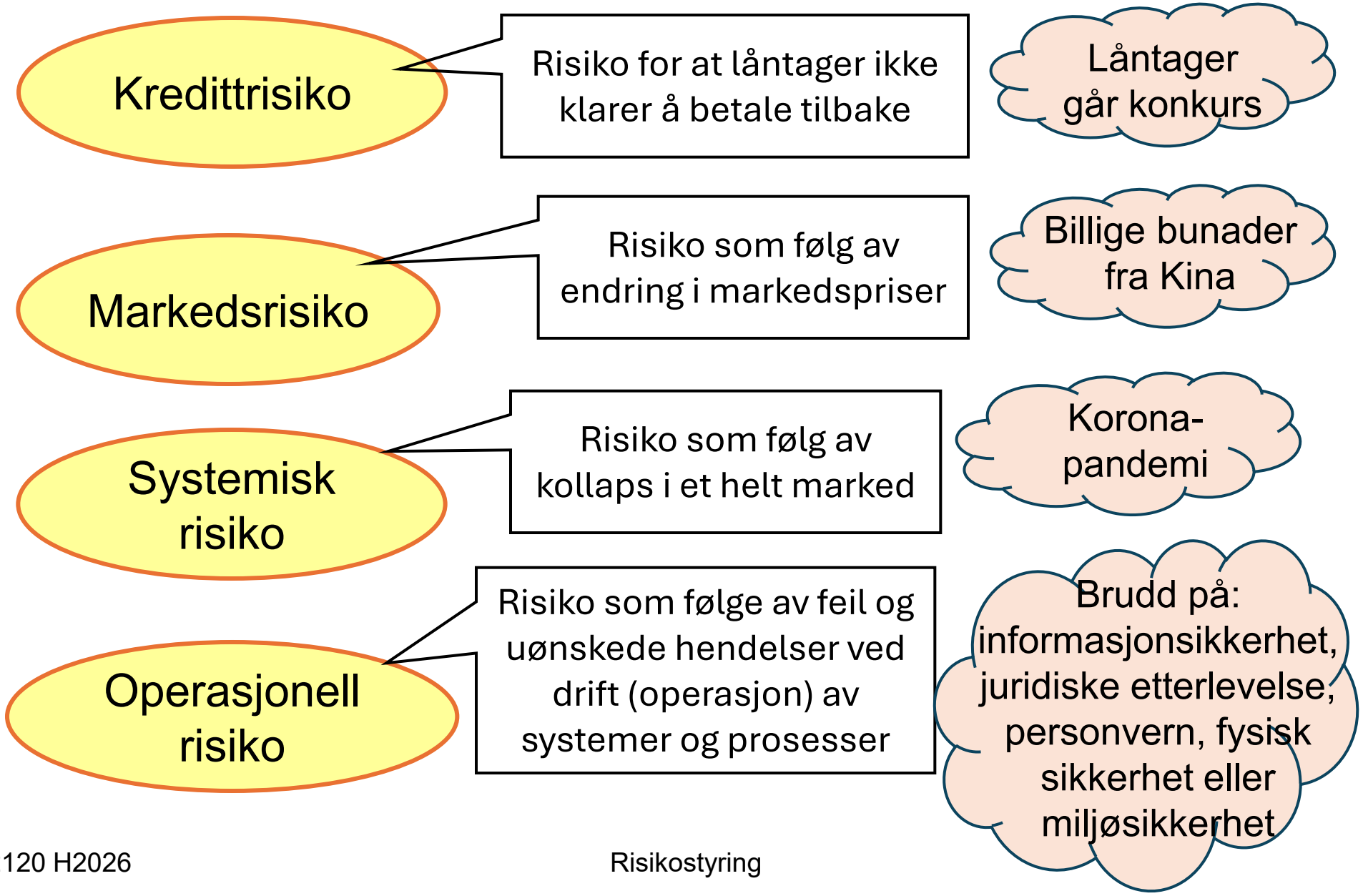
Universitetet i Oslo, høst 2026

Oversikt: Risikostyring



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

Typer av Risiko



Hva er risiko, og IS-risiko?

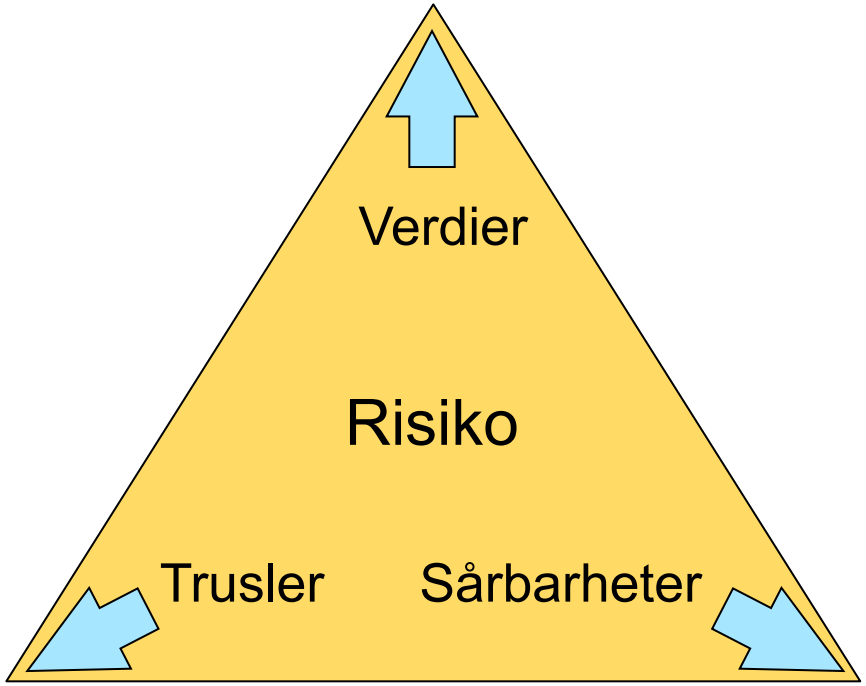
- ISO 31000 Risikostyring og ISO 27000 Oversikt og begreper
  - **“Risiko er effekten av uvisshet rundt oppnåelse av målsettinger”**
  - Intet skille mellom positive og negative effekter av uvisshet
  - Svært generell og abstrakt definisjon, uegnet for IS-risikovurdering
  - Men ISO 31000 sier også: 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.”**



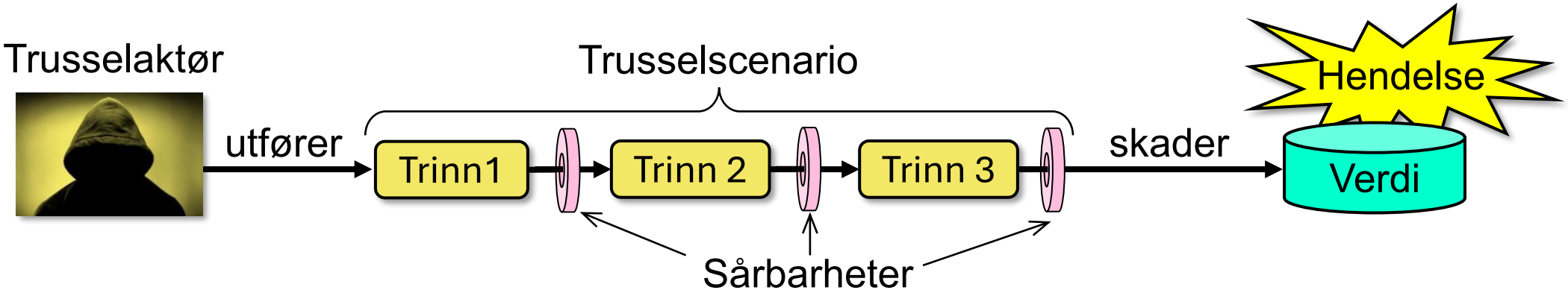
Generell risikomodell (NSM)



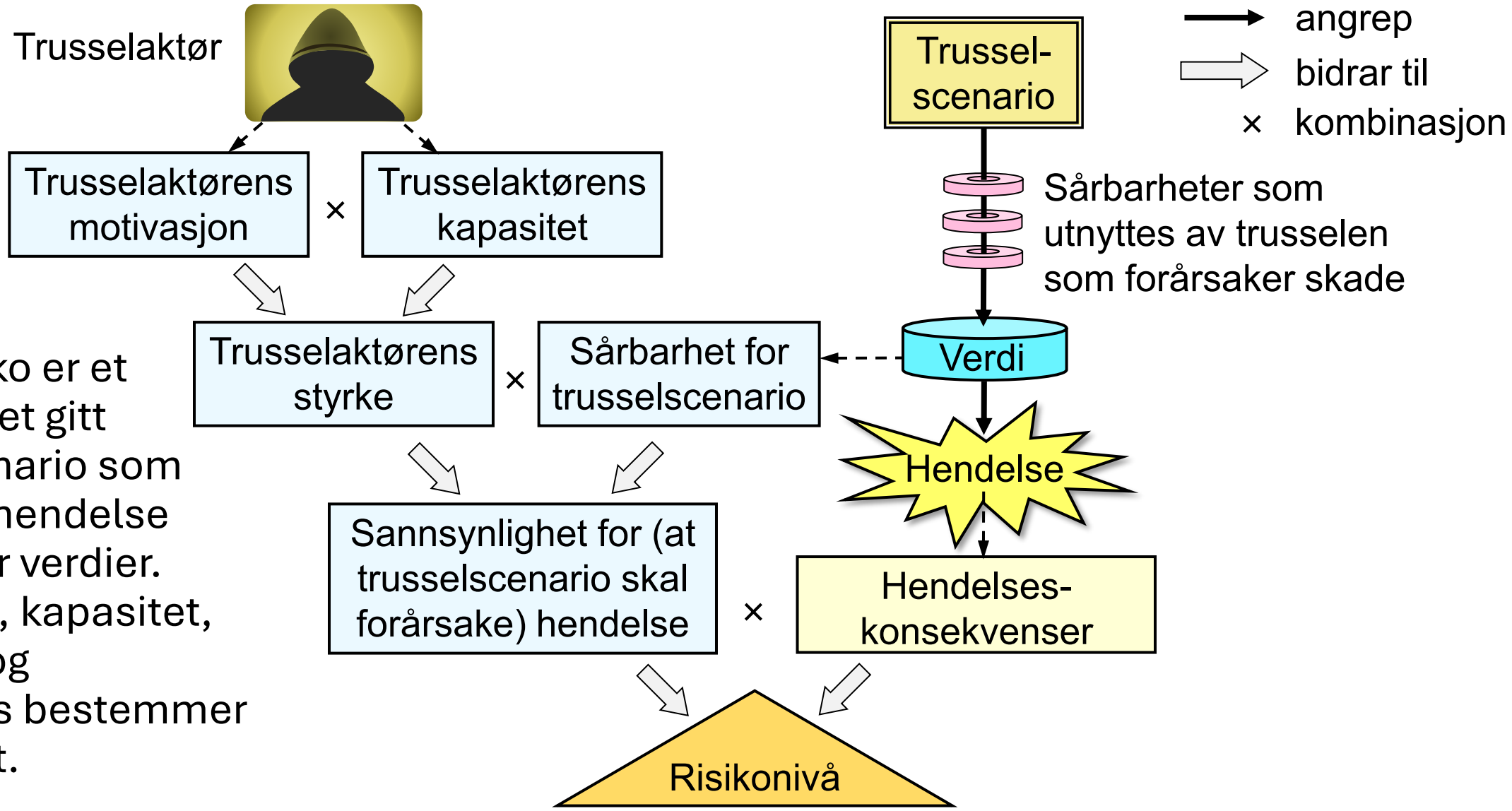
- Generell modell for risiko
  - Jo større verdier, jo større trusler, og jo mer alvorlige sårbarheter, desto større risiko er du utsatt for.

Trusler

- **Trusselscenario:** En sekvens av trinn eller hendelser som kan styres eller utløses av en trusselaktør, og som kan skade verdier/ressurser. Et trusselscenario er mulig å gjennomføre når det fins sårbarheter (svakheter) som kan utnyttes.
- **Trusselaktør:** En aktiv entitet som kan styre eller utløse trusselscenarier. Trusselaktører kan være intelligente entiteter med bevisst skadehensikt, eller naturkrefter som er for sterk eller uforutsigbare for effektivt forebygging.
- Begrepet «trussel» tolkes ofte i betydning «trusselscenario».



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.

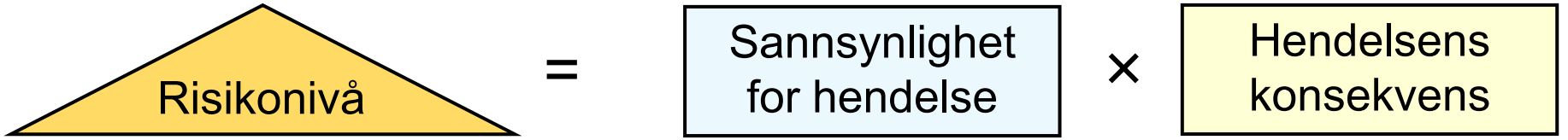
Risiko eller risikonivå?

- 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 / potensiell hendelse som utgjør et brudd på KIT + P for en verdi. Risikoidentifisering er å kartlegge slike relevante kombinasjoner.

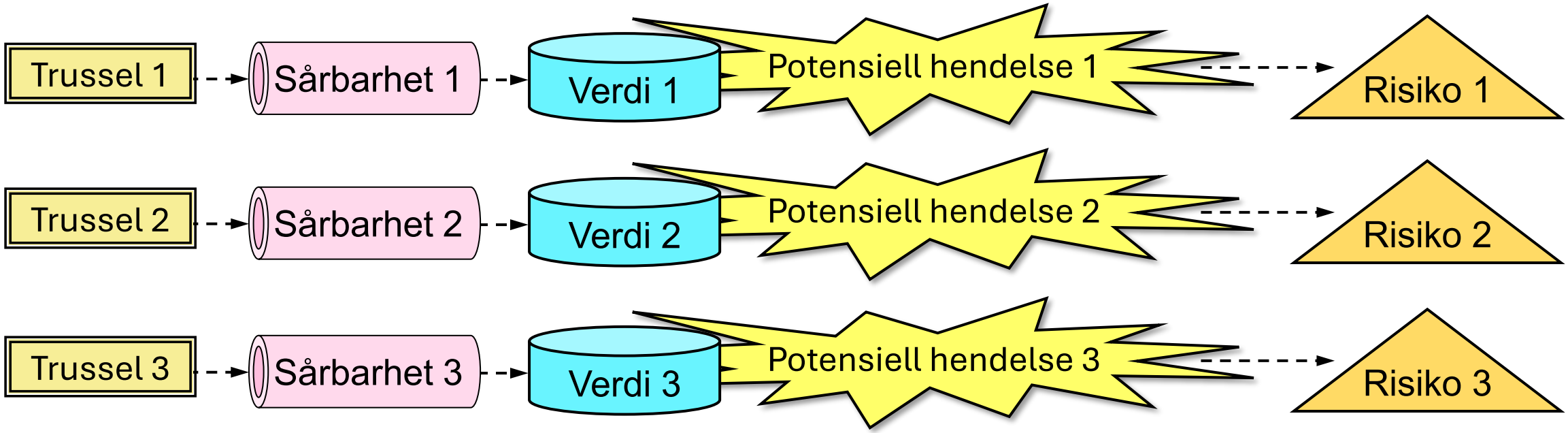


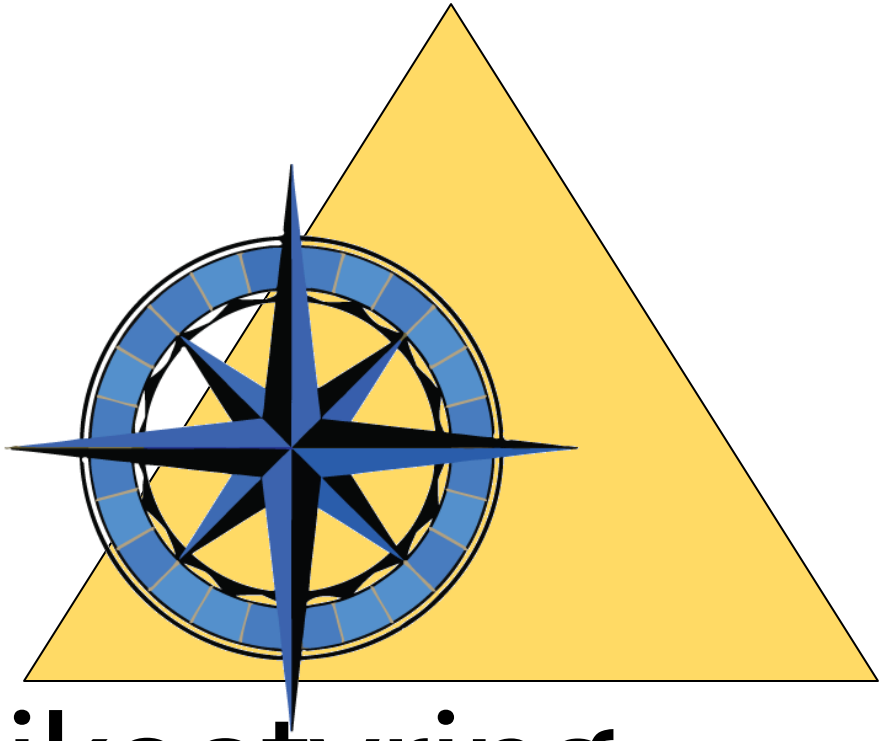
  - **Risikonivå** (også kalt risikoeksponering) er kombinasjonen av hendelsens sannsynlighet og konsekvens. Risikonivå beregnes med risikoanalyse.



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





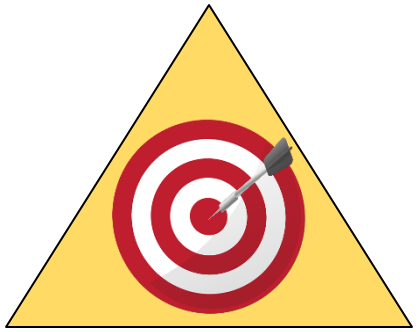
Del b: Risikostyring

Hva er risikostyring?

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

International Organization for Standardization

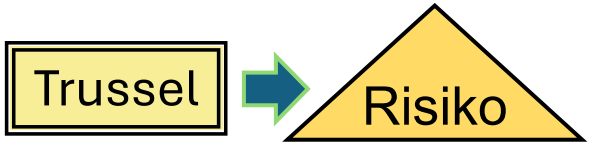
- Aktiviteter innen risikostyring kan ha ulike målsettinger. Det kan f.eks. være en eller flere av følgende:
  - å få oversikt over verdier
  - å få oversikt over trusler
  - å få oversikt over sårbarheter
  - å få oversikt over eksisterende risikoer
  - å vurdere risikoene
  - å foreslå nye sikkerhetstiltak
  - å vurdere restrisiko etter nye foreslåtte sikkerhetstiltak
  - å gi grunnlag for å kjøpe cyberforsikring
  - å gi grunnlag for budsjett for håndtering av risiko



Fokus, kontekst, kriterier for risikoaksept



- Risikostyring skal skape balanse mellom identifisert risiko som kan forårsake tap, og investering i sikkerhetstiltak som beskytter mot sikkerhetshendelser og forhindrer tap.
- Bygger på en serie risikovurderinger, som hver tar utgangspunkt i et trusselscenario:
  - som kan forårsake en sikkerhetshendelse som gir brudd på informasjonssikkerhet for verdier, og som dermed skaper negative konsekvenser for virksomheten.



- Metode og modell for risikoanalyse må bestemmes
  - F.eks. kvalitativ, kvantitativ, relativ
- Kriterier for risikoaksept bør fastsettes før risikovurderingen



Sannsynlighet



Konsekvens

Utgangspunkt for vurdering av IS-risiko

- Oversikt over digitale verdier: identifiser og forstå deres forretningsverdi.
- Oversikt over truslene: identifiser relevante trusselscenarier som kan skade informasjonsressurser og -systemer.
- Oversikt over sårbarhetene som kan utnyttes av trusler, og som dermed kan føre til hendelser.
- Forståelse av potensielle konsekvenser av hendelser.
- Klarhet i eierskap av verdier og ansvar for å håndtere de identifiserte risikoene.

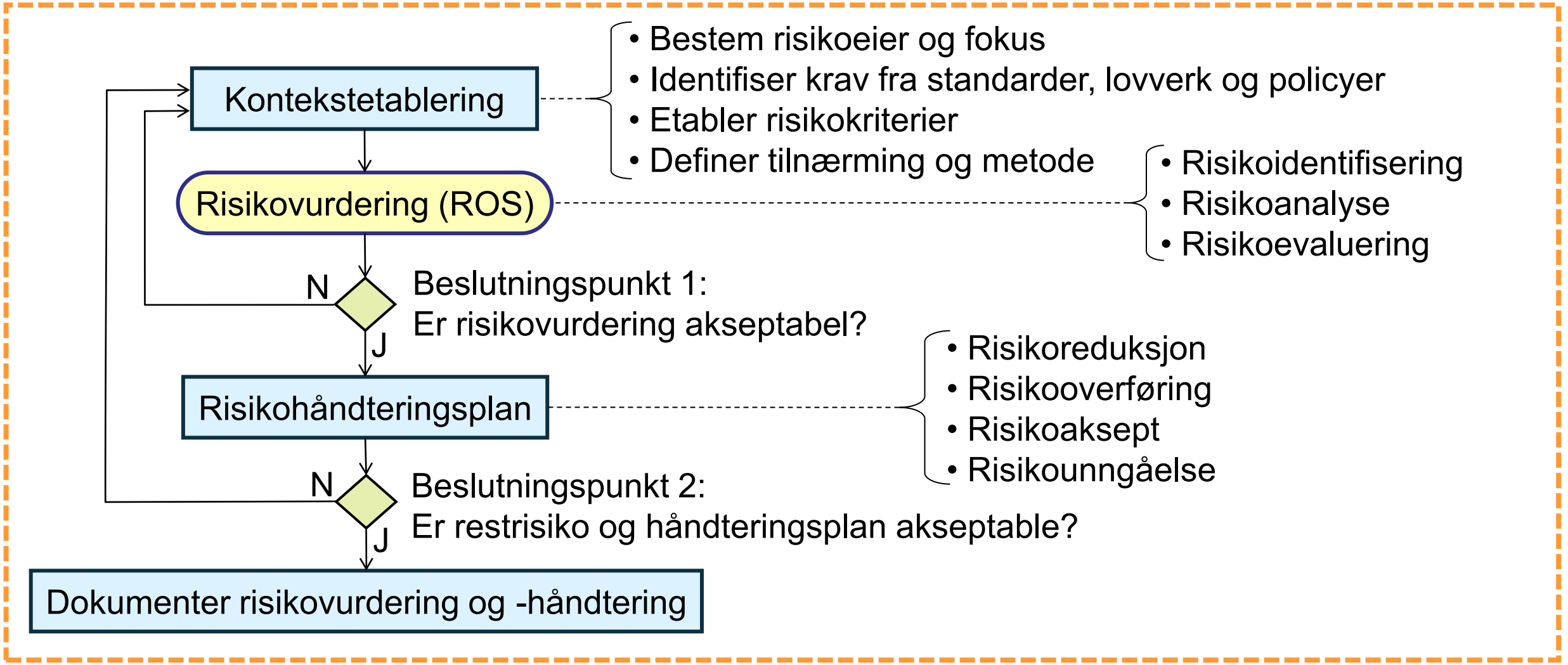
Roller involvert i risikovurdering og risikohåndtering



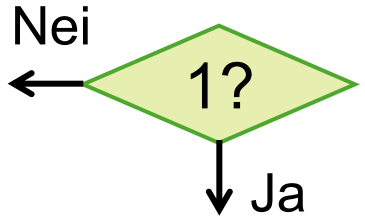
Ledelse, eiere, brukere og fageksperter må samarbeide.

- Eiere av verdier må hjelpe til med å
  - lage oversikt over verdier, og spesifisere sikkerhetsmålsettinger (KIT+P)
  - vurdere konsekvens av brudd på sikkerhetsmål
- Brukere og sikkerhetseksperter må hjelpe til med å
  - identifisere trusler og sårbarheter,
  - vurdere sannsynligheter
- Risikoeksperter må veilede risikoanalyseprosessen
- Sikkerhetseksperter må gi råd om sikkerhetstiltak
- Ledelsen må gjennomgå risikostyringsprosessen og godkjenne budsjett for foreslåtte sikkerhetstiltak

Risikostyring: ISO/IEC 27005



Beslutningspunkt 1



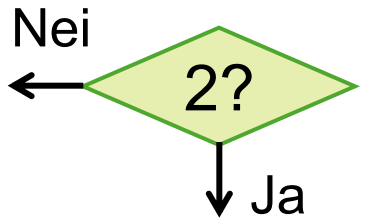
Er risikovurderingen tilfredsstillende?

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?

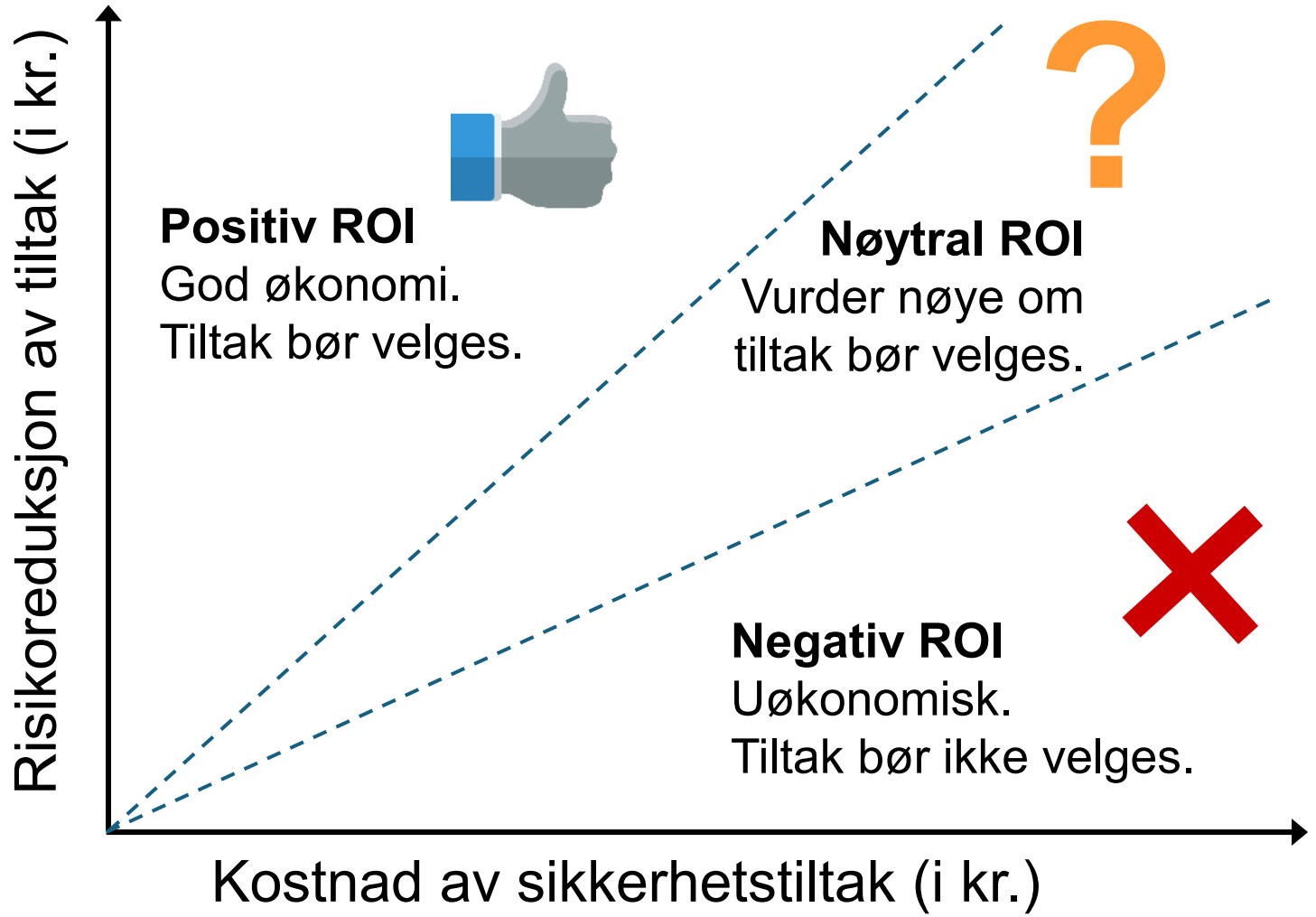
Grunner for å svare "Nei", og hvordan det kan rettes.

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.

ROI av sikkerhetstiltak (Return on Investment)

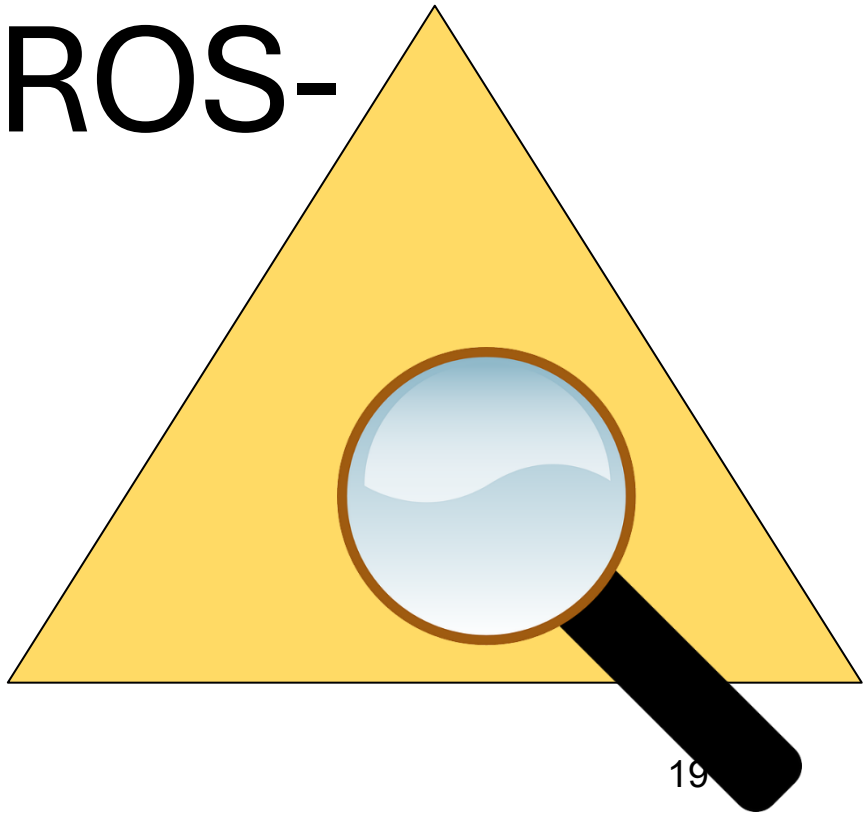


$$\text{ROI} = \frac{\text{Gevinst} - \text{Investering}}{\text{Investering}}$$

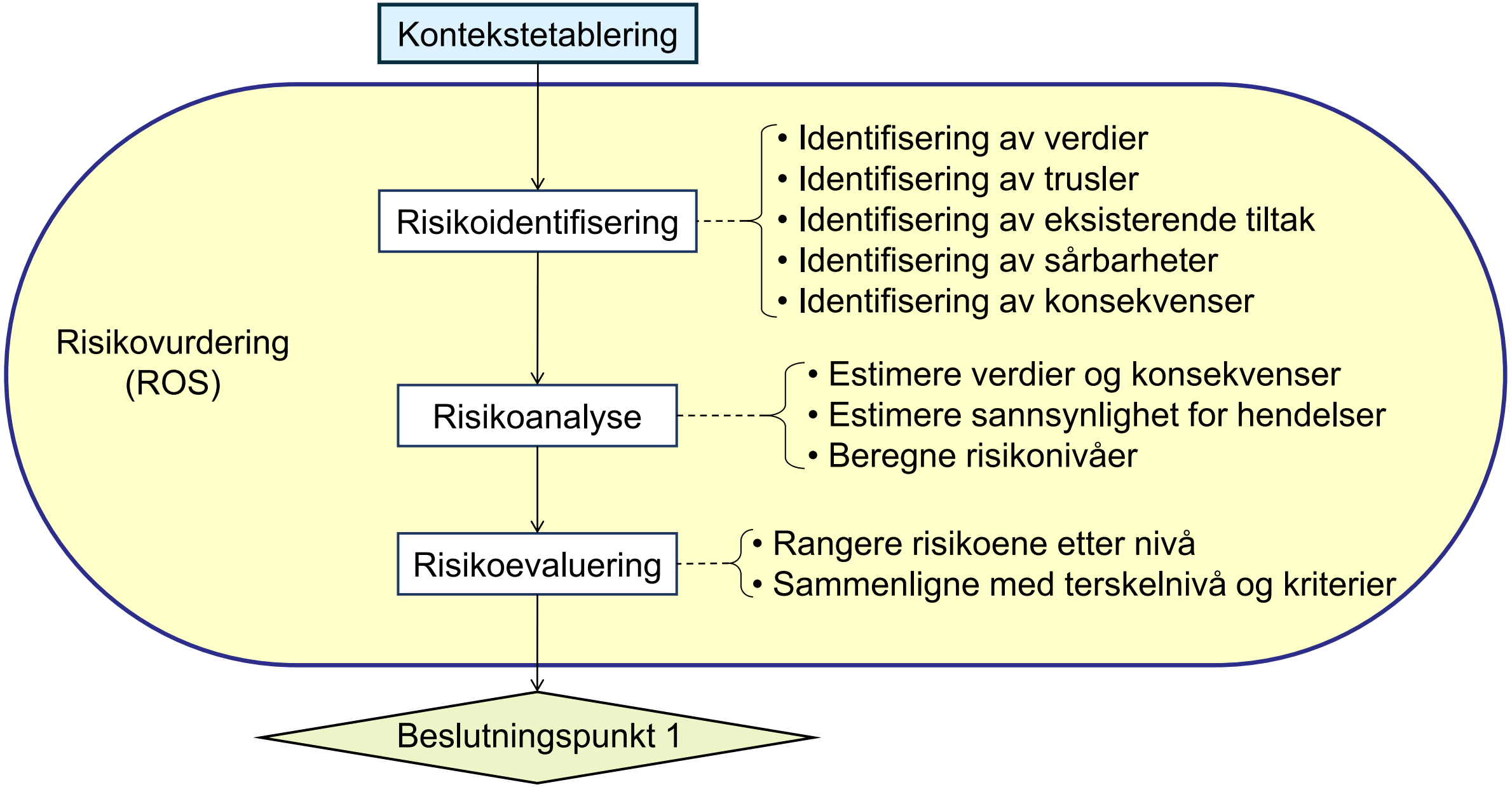
$$\text{ROI} = \frac{\text{Risikoreduksjon} - \text{Kostnad}}{\text{Kostnad}}$$

1. Risikoidentifisering
2. Risikoanalyse
3. Risikoevaluering
4. Regneark for risikovurdering

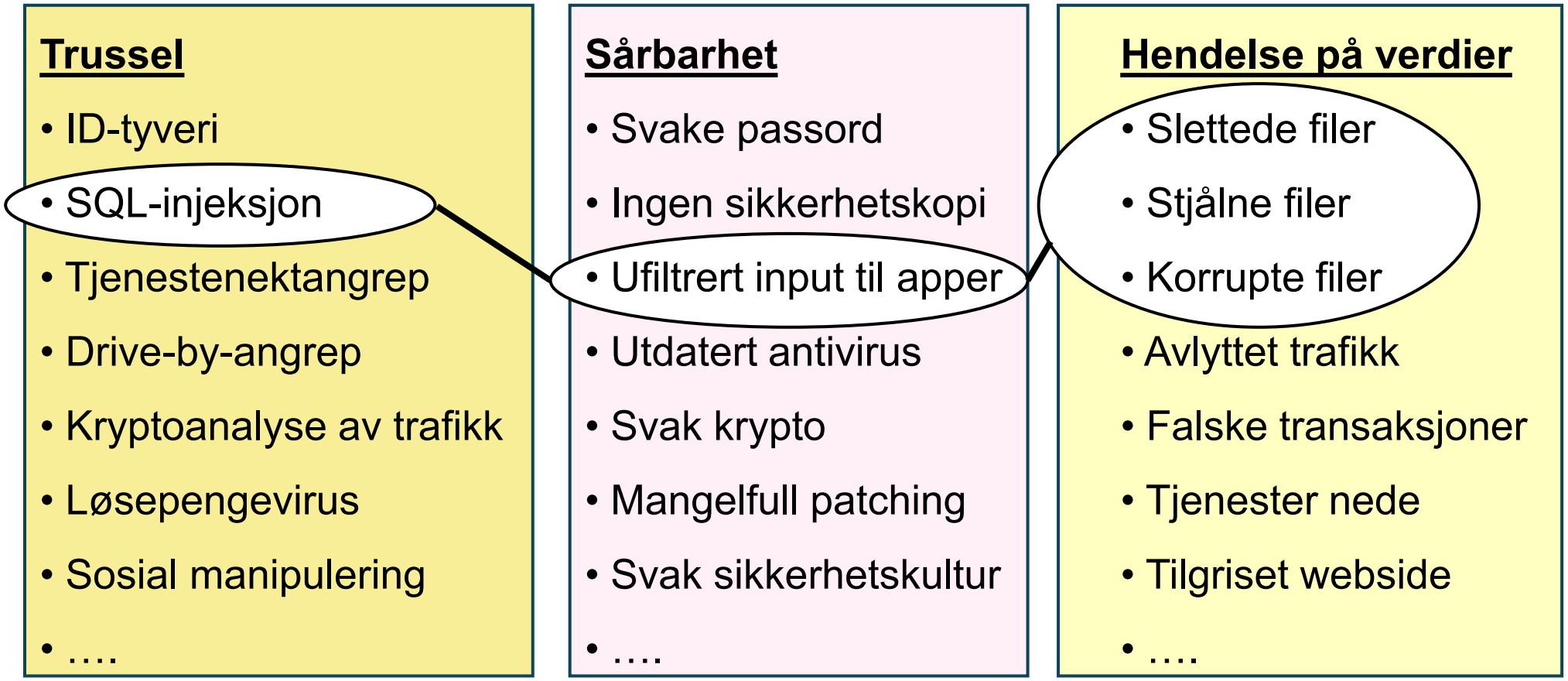
Del c: Risikovurdering (ROS-analyse)



Prosess for risikovurdering – ISO/IEC 27005

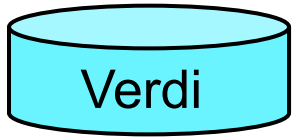


Risikoidentifisering



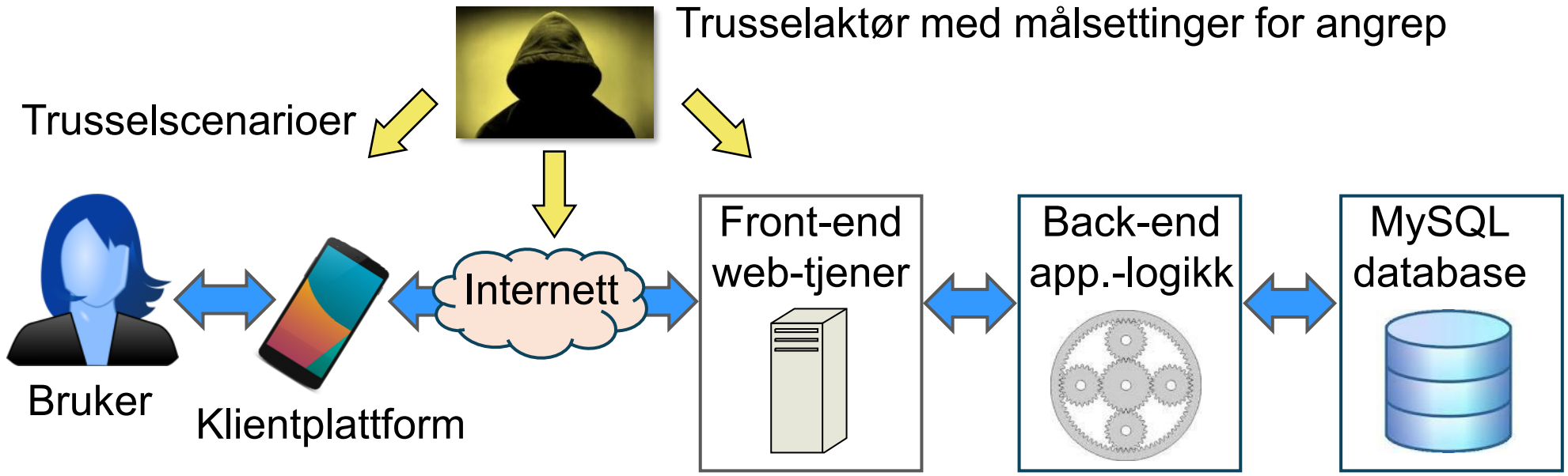
- Å identifisere en risiko betyr å finne en relevant kombinasjon av en trussel, sårbarhet(er) og hendelse(r) som kan skade verdier.

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

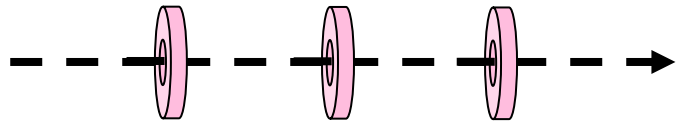
Trusselmodellering



- 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?

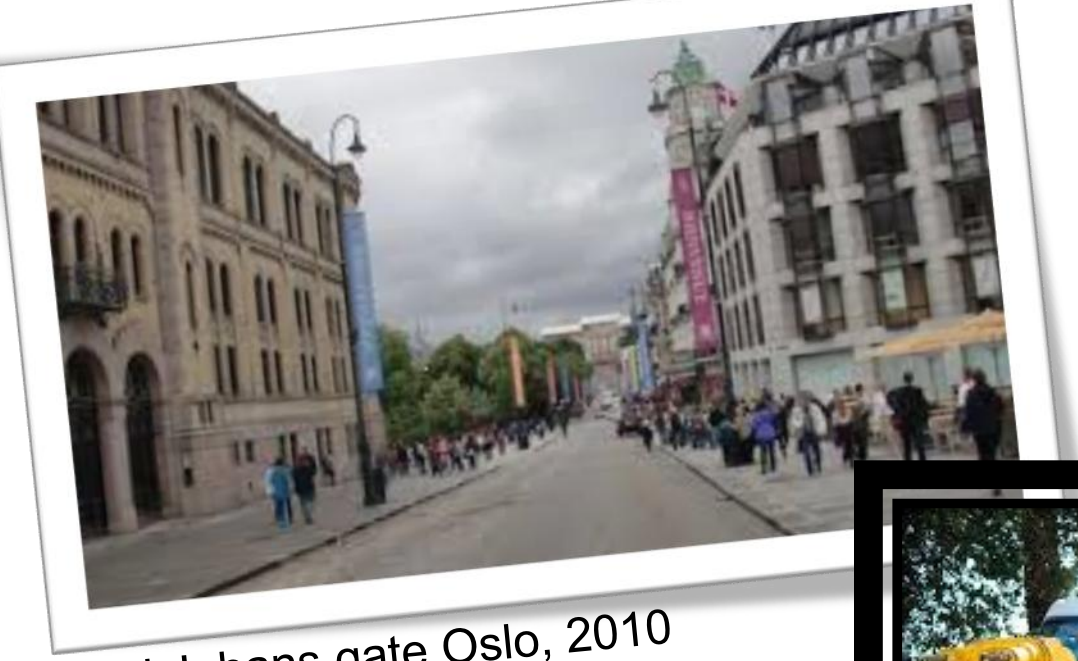
  Hvem kunne være interessert i å skade oss?

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, 2010

Nice 2016
Berlin 2016
Barcelona 2017
London 2017, 2018
Magdeburg 2024
New Orleans 2025
Munchen 2025



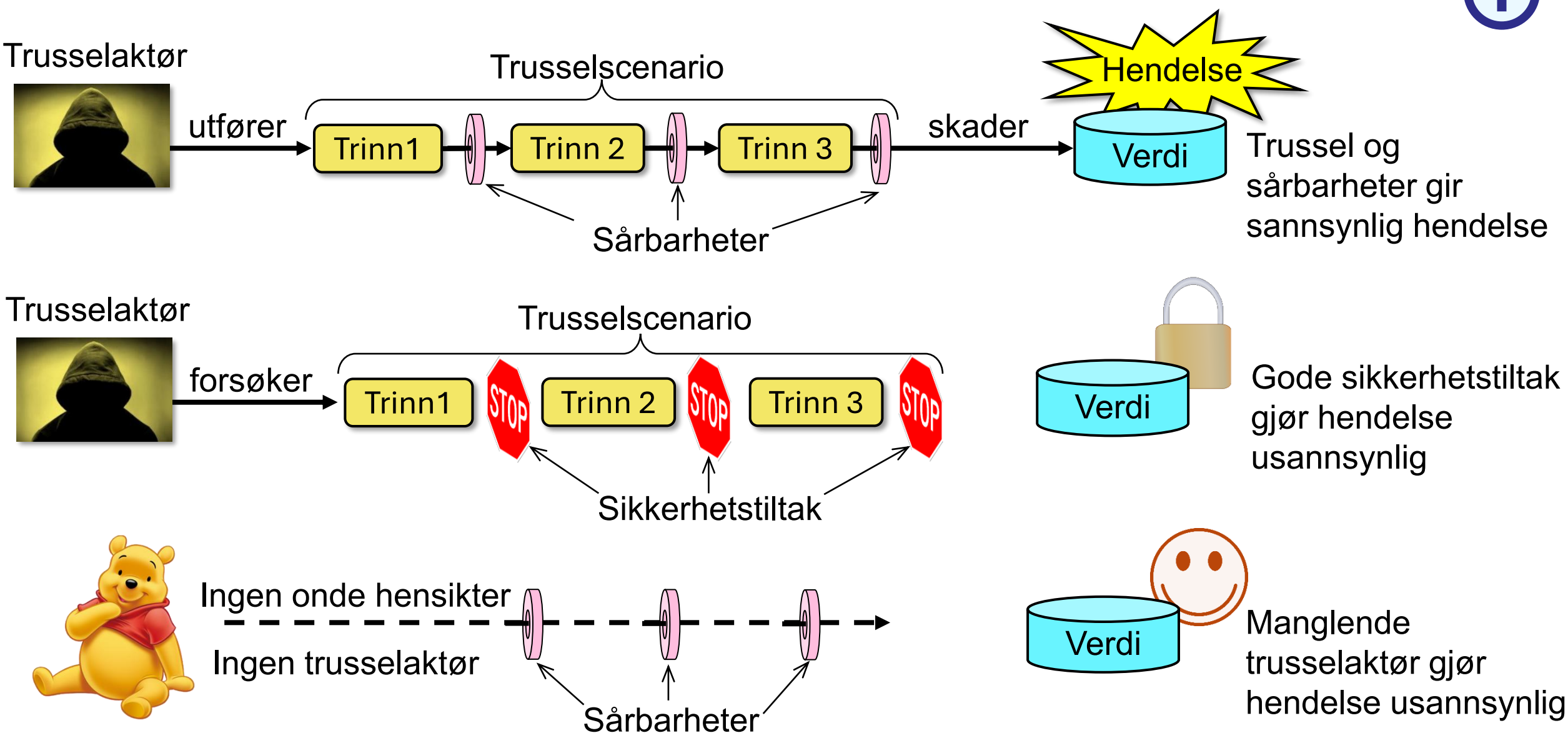
Ny trussel oppstod i 2016

Karl Johans gate Oslo, 2020

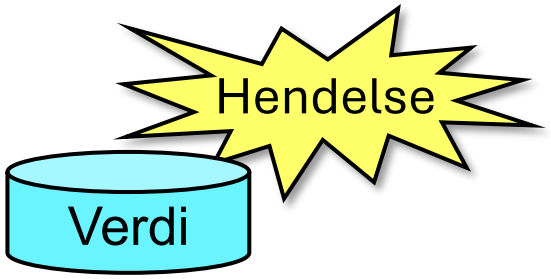


Trussel blokkert
(dvs. sårbarhet fjernet)

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

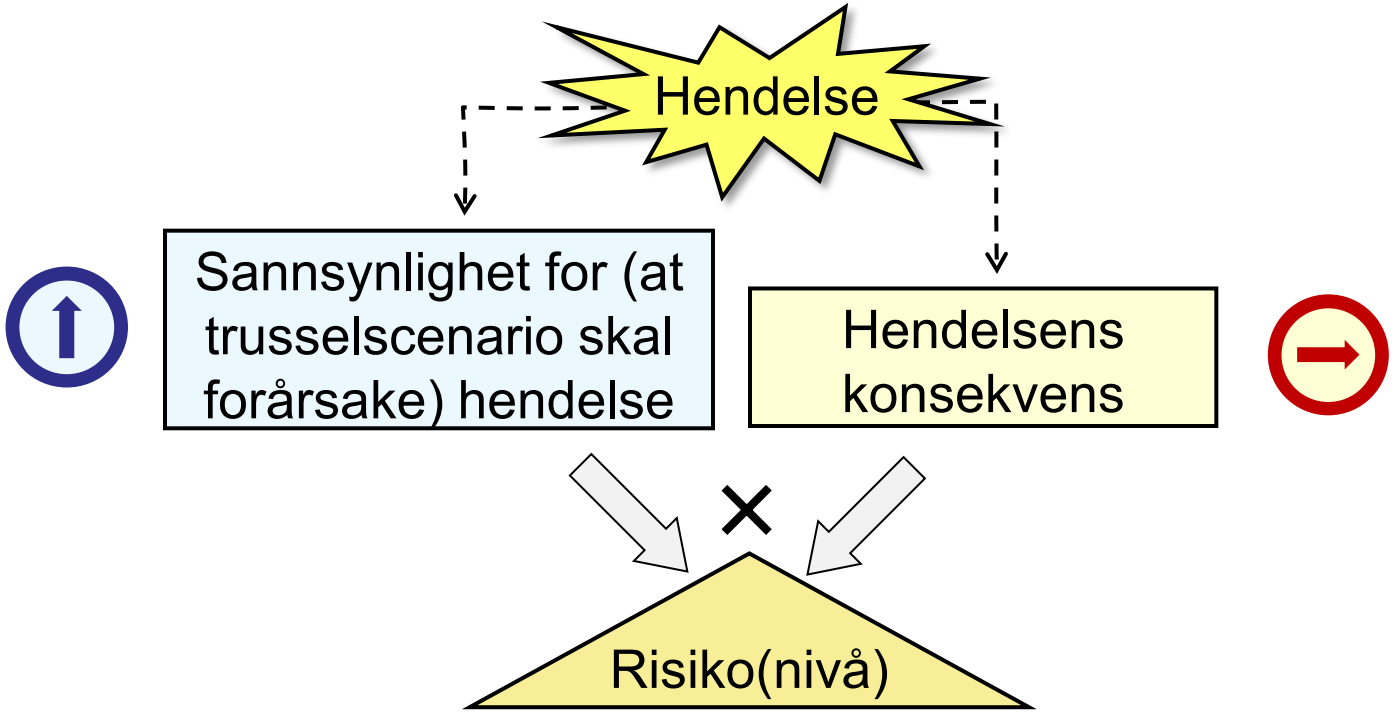
§

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

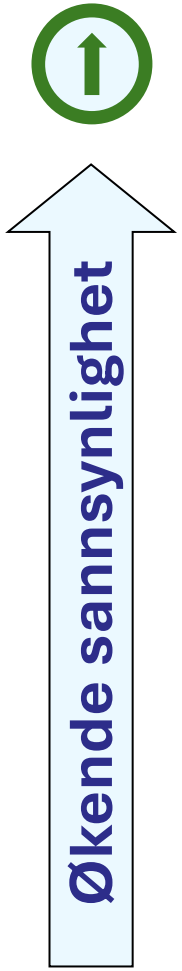


Hva er sannsynligheten for at verden går under?



- P = 1 innen 100 milliarder år
- Meningsløst å betrakte sannsynlighet med et uendelig tidsperspektiv
- Derfor må relevant tid må benyttes ved estimering av sannsynlighet for hendelser

Kvalitativ sannsynlighetsskala (med ordinalnivåer)



Sannsynlighet	Beskrivelse
(5) Snarest	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) Sannsynlig	Motiverte trusselaktører vil med høy sannsynlighet nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet. En hendelse kan inntreffe innen et par måneder.
(3) Mulig	Trusselaktører har en betydelig mulighet til å nå sitt mål ved å bruke det vurderte trusselscenarioet. En hendelse kan inntreffe innen et par år.
(2) Usannsynlig	Trusselaktører har relativt liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. En hendelse kan inntreffe innen et par tiår.
(1) Sjelden	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 kalibreres etter behov.

Kvalitativ konsekvensskala (med ordinalnivåer)



Konsekvensnivå	Beskrivelse
(5) Verst	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) Stor	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. Antall nivåer og fortolkning kalibreres etter behov.

Risikomatrise for kvalitativ risikoberegning (med ordinalnivåer)

Tolkning av (ordinale) risikonivåer:

- **(9 –10) E:** Ekstrem risiko; må håndteres med høyeste prioritet
- **(8) VH:** Veldig høy risiko, må håndteres med prioritet
- **(7) H:** Høy risiko; bør håndteres, men prioritet kan vurderes
- **(6) M:** Moderat; bør vanligvis håndteres, men kan aksepteres
- **(5) L:** Lav risiko; kan aksepteres, men håndtering kan vurderes
- **(3 – 4) VL:** Veldig lav risiko; kan umiddelbart aksepteres
- **(0 – 2) N:** Neglisjerbar eller ingen risiko

Kvalitativ sannsynlighet P

(5) Snarest	**(5) L**	**(6) M**	**(7) H**	**(8) VH**	**(9) E**	**(10) E**
(4) Sannsynlig	**(4) VL**	**(5) L**	**(6) M**	**(7) H**	**(8) VH**	**(9) E**
(3) Mulig	**(3) VL**	**(4) VL**	**(5) L**	**(6) M**	**(7) H**	**(8) VH**
(2) Usannsynlig	**(2) N**	**(3) VL**	**(4) VL**	**(5) L**	**(6) M**	**(7) H**
(1) Sjeldent	**(1) N**	**(2) N**	**(3) VL**	**(4) VL**	**(5) L**	**(6) M**
(0) Aldri	**(0) N**	**(1) N**	**(2) N**	**(3) VL**	**(4) VL**	**(5) L**
Kvalitative risikonivåer	(0) Ingen	(1) Ubetydelig	(2) Liten	(3) Betydelig	(4) Stor	(5) Verst

Kvalitativ konsekvens K

Logaritmisk sannsynlighet og konsekvense

- Prinsipp for logaritme: $\log(10^X \cdot 10^Y) = X + Y$

- Multiplikativ beregning av kvantitativ risiko: $sannsynlighet \cdot konsekvens$

- Additiv beregning av logaritmisk risiko: $sannsynlighet + konsekvens$

Eksponensiering og logaritme



- Eksponensiering betyr å "opphøye grunntall *G* i eksponent (potens) *X*"
- Opphøying betyr å multiplisere *G* med seg selv *X* antall ganger
- F.eks. grunntall 10 opphøyd i eksponent (potens) *X* skrives 10^X
- La *G*=10 og *X*=3, da har vi $10^3 = 10 \cdot 10 \cdot 10 = 1000$

- Logaritme betyr å beregne eksponent som grunntallet er opphøyd i: $\log(G^X) = X$
- F.eks. med grunntall *G*=10 har vi:
  - log(1000) = 3, fordi $1000 = 10^3$
  - log(0,001) = -3, fordi $0{,}001 = 10^{-3} = \frac{1}{1000}$
- Eksponensiering og logaritme er inverse funksjoner
- Logaritmisk skala er når trinnene i skalaen dannes av rekkefølge med eksponenter,
  - Trinnene 0,001; 0,01; 0,1; 1; 10; 100; 1000; er en logaritmisk skala dannet av, -3, -2, -1, 0, 1, 2, 3

Kalibrering av kvantitativ sannsynlighet

- Den kvantitative sannsynlighetsskalaen er logaritmisk.
- *S* er kalibreringsfaktoren for antatt snarest sannsynlig hendelse (høyest frekvens), tilsvarende høyeste kvalitative sannsynlighet (nivå 5).
- Lavere sannsynligheter bestemmes deretter med logaritmisk skala.
- P_{Kval} er ordinal kvalitativ sannsynlighet (intervall [0, 5]).
- Sett f.eks. *S* = 50 (snarest sannsynlighet, antagelig innen en uke, dvs. 50 ganger per år).
- Kvantitativ sannsynlighet: $P_{\text{Kvan}} = S \cdot 10^{X}$ der $X = P_{\text{Kval}} - 5$ (intervall [-5, 0])

Kvalitative ordinalnivåer av sannsynlighet (P_{Kval})	Kvantitative sannsynlighetsnivåer (P_{Kvan})	Fortolkning
Ordinalnivå 5 ($X = 5 - 5 = 0$)	$P_{\text{Kvan}} = S \cdot 10^{X} = 50 \cdot 10^{0} = 50$	Innen en uke = 50 ganger per år
Ordinalnivå 4 ($X = 4 - 5 = -1$)	$P_{\text{Kvan}} = S \cdot 10^{X} = 50 \cdot 10^{-1} = 5$	Innen 2 måneder = 5 ganger per år
Ordinalnivå 3 ($X = 3 - 5 = -2$)	$P_{\text{Kvan}} = S \cdot 10^{X} = 50 \cdot 10^{-2} = 0.5$	Innen et par år
Ordinalnivå 2 ($X = 2 - 5 = -3$)	$P_{\text{Kvan}} = S \cdot 10^{X} = 50 \cdot 10^{-3} = 0.05$	En gang per 20 år
Ordinalnivå 1 ($X = 1 - 5 = -4$)	$P_{\text{Kvan}} = S \cdot 10^{X} = 50 \cdot 10^{-4} = 0.005$	En gang per 200 år
Ordinalnivå 0 ($X = 0 - 5 = -5$)	$P_{\text{Kvan}} = S \cdot 10^{X} = 50 \cdot 10^{-5} = 0.0005$	En gang per 2000 år

Kalibrering av kvantitativ konsekvens



- Den kvantitative konsekvensskalaen er logaritmisk.
- *V* er kalibreringsfaktoren for verste mulige tap, tilsvarende høyest kvalitativ konsekvens (nivå 5)
- Lavere konsekvenser bestemmes deretter med logaritmisklogaritmisk skala.
- K_{Kval} er ordinal kvalitativ konsekvens (intervall [0, 5])
- Sett f.eks. *V* = \$10 millioner = $\$10^7$
- Kvantitativ konsekvens: $K_{\text{Kvan}} = V \cdot 10^{Y}$ der $Y = K_{\text{Kval}} - 5$ (intervall [-5, 0])

Kvalitative ordialnnivåer av konsekvens (K_{Kval})	Kvantitative konsekvens-nivåer (K_{Kvan})	Fortolkning
Ordinalnivå 5 ($Y = 5 - 5 = 0$)	$V \cdot 10^{Y} = 10^7 \cdot 10^0 = 10^7$	K_{Kvan} = \$10 millioner
Ordinalnivå 4 ($Y = 4 - 5 = -1$)	$V \cdot 10^{Y} = 10^7 \cdot 10^{-1} = 10^6$	K_{Kvan} = \$1 million
Ordinalnivå 3 ($Y = 3 - 5 = -2$)	$V \cdot 10^{Y} = 10^7 \cdot 10^{-2} = 10^5$	K_{Kvan} = \$100 000
Ordinalnivå 2 ($Y = 2 - 5 = -3$)	$V \cdot 10^{Y} = 10^7 \cdot 10^{-3} = 10^4$	K_{Kvan} = \$10 000
Ordinalnivå 1 ($Y = 1 - 5 = -4$)	$V \cdot 10^{Y} = 10^7 \cdot 10^{-4} = 10^3$	K_{Kvan} = \$1000
Ordinalnivå 0 ($Y = 0 - 5 = -5$)	$V \cdot 10^{Y} = 10^7 \cdot 10^{-5} = 10^2$	K_{Kvan} = \$100

Eksempel på kvantitativ risikoanalyse

$ € £ ¥

Case: Hacking av nettsted

- Risiko: Tilgriset og ødelagt nettsted
- Sannsynlighetsestimat
  - $\boldsymbol{P}_{\mathbf{Kvan}} = 0{,}5$, det vil si at det sannsynligvis vil skje hvert 2. år
- Konsekvensestimat med flere aspekter
  - Tapt fortjeneste fordi nettstedet er nede, k_1 = \$50 000
  - Tapt omdømme k_2 = \$20 000
  - Kostnad for å korrigere nettsiden k_3 = \$10 000
  - $K_1 = k_1 + k_2 + k_3$ = \$80 000
- Beregning av risiko
  - $\boldsymbol{R}_{\mathbf{Kvan}} = \boldsymbol{P}_{\mathbf{Kvan}} \cdot \boldsymbol{K}_{\mathbf{Kvan}} = 0.5 \times \$80{,}000 \;=\; \$40{,}000$ i forventet tap per år

- Gir grunnlag for å bruke \$40 000 på sikkerhetskontroller for å håndtere risikoen
  - hvis sikkerhetstiltakene vil redusere risikonivået til \$0

Eksempel på kvalitativ og kvantitativ risikoanalyse



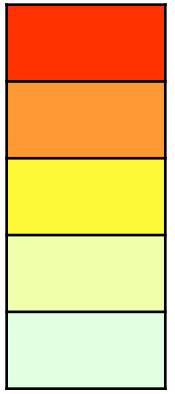
Case: Phishing-angrep for å stjele identiteter

- Risiko: Angriperen sender phishing-e-post for å lure offeret til å oppgi passord

- Estimering av sannsynlighet
  - Kalibreringsfaktor for snareste sannsynlighet $S = 50$ ganger per år, dvs. antagelig innen en uke.
  - Kvalitativt sannsynlighetsestimat $\boldsymbol{P}_{\mathbf{Kval}}$ = **Usannsynlig** (ordinalnivå 2)
  - Kvantitativt sannsynlighetsestimat $\boldsymbol{P}_{\mathbf{Kvan}} = S \cdot 10^{(2-5)} = S \cdot 10^{-3} = 50 \cdot 0.001 = 0.05$ (hvert 20. år)
- Estimering av konsekvens
  - Kalibreringsfaktor for verste konsekvens V = \$10 millioner = $\$10^7$
  - Kvalitativt konsekvensestimat $\boldsymbol{K}_{\mathbf{Kval}}$ = **Stor** (ordinalnivå 4)
  - Kvantitativt konsekvensestimat $\boldsymbol{K}_{\mathbf{Kvan}} = V \cdot 10^{(4-5)} = V \cdot 10^{-1} = 10^7 \cdot 0.1 = \$10^6 =$ \$1 million
- Beregning av risiko
  - $\boldsymbol{R}_{\mathbf{Kvan}} = \boldsymbol{P}_{\mathbf{Kvan}} \cdot \boldsymbol{K}_{\mathbf{Kvan}}$ = 0.05 × \$1,000,000 = \$50,000

- Gir grunnlag for å bruke \$50 000 på sikkerhetstiltak for å håndtere risikoen
  - hvis sikkerhetstiltaket vil redusere risikonivået til \$0

Regneark for risikovurdering



- Mange forskjellige veiledere, maler og verktøy for risikovurdering
  - ➢ Ofte relativt komplisert, krever opplæring for å bruke
- Ordinale kvalitative estimater av sannsynlighet og konsekvens er logaritmiske
- Logaritmiske nivåer gjør kvalitativ risikoberegning additiv

$$R_{\text{Kval}} = P_{\text{Kval}} + K_{\text{Kval}}$$

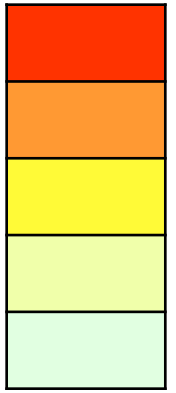
- Kvantitativ risikoberegning er multiplikativ

$$R_{\text{Kvan}} = P_{\text{Kvan}} \cdot K_{\text{Kvan}}$$

➢ UiOs regneark for kvalitativ og kvantitativ cyberrisikovurdering:

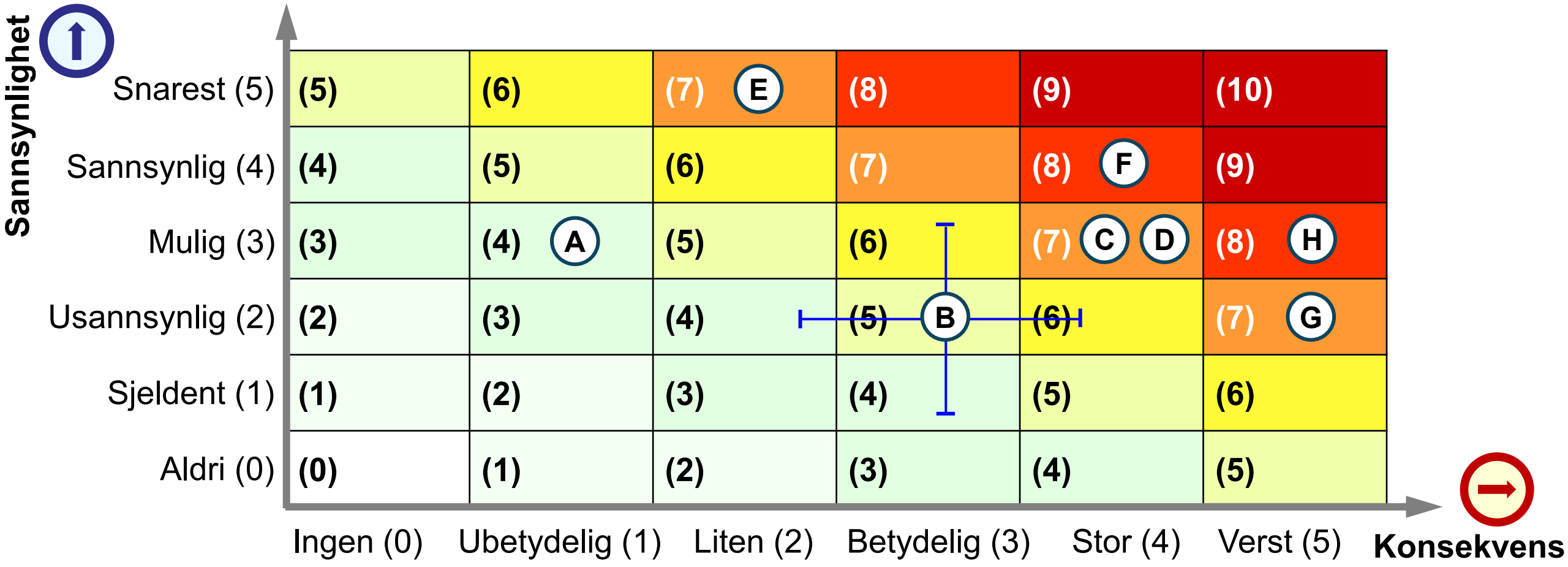
➢ uio-risikovurdering.xlsx

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, både før og etter foreslåtte sikkerhetstiltak
  - a) kvalitativ risiko = kvalitativ sannsynlighet + kvalitativ konsekvens
  - b) kvantitativ risiko = kvantitativ sannsynlighet × kvantitativ konsekvens
    - Forutsetter å bestemme antatt snarest sannsynlighet *S* og verst tenkelig konsekvens *V*
- Anbefalte nye tiltak
  - Forslag til nye sikkerhetstiltak for å forhindre hendelsen eller mitigere konsekvenser

Visualisering av risikoer



Slutt på presentasjonen