IN5080
Sikkerhets- og risikostyring

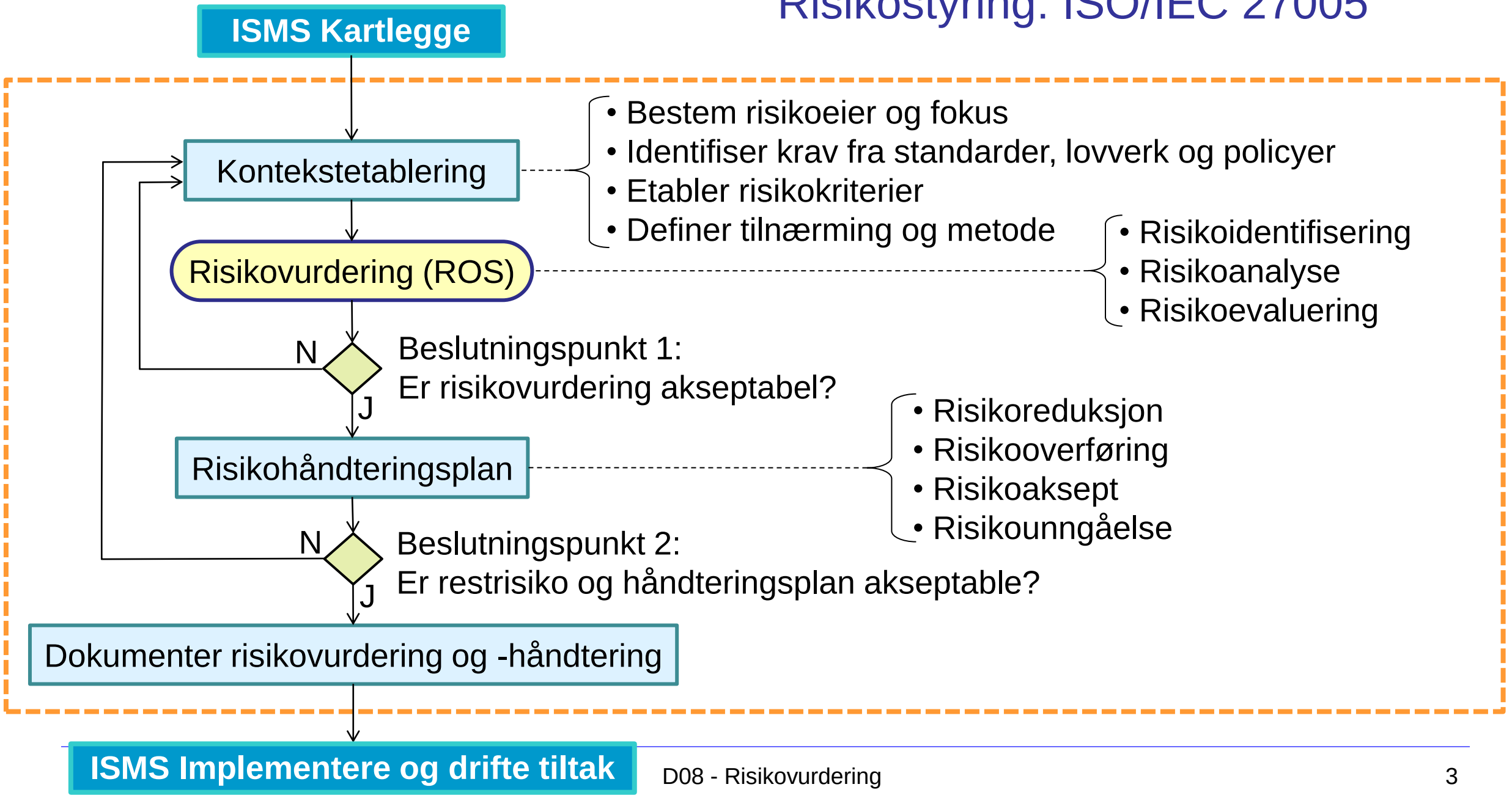
Del 8: Risikovurdering

Audun Jøsang
Universitetet i Oslo
Vår 2024

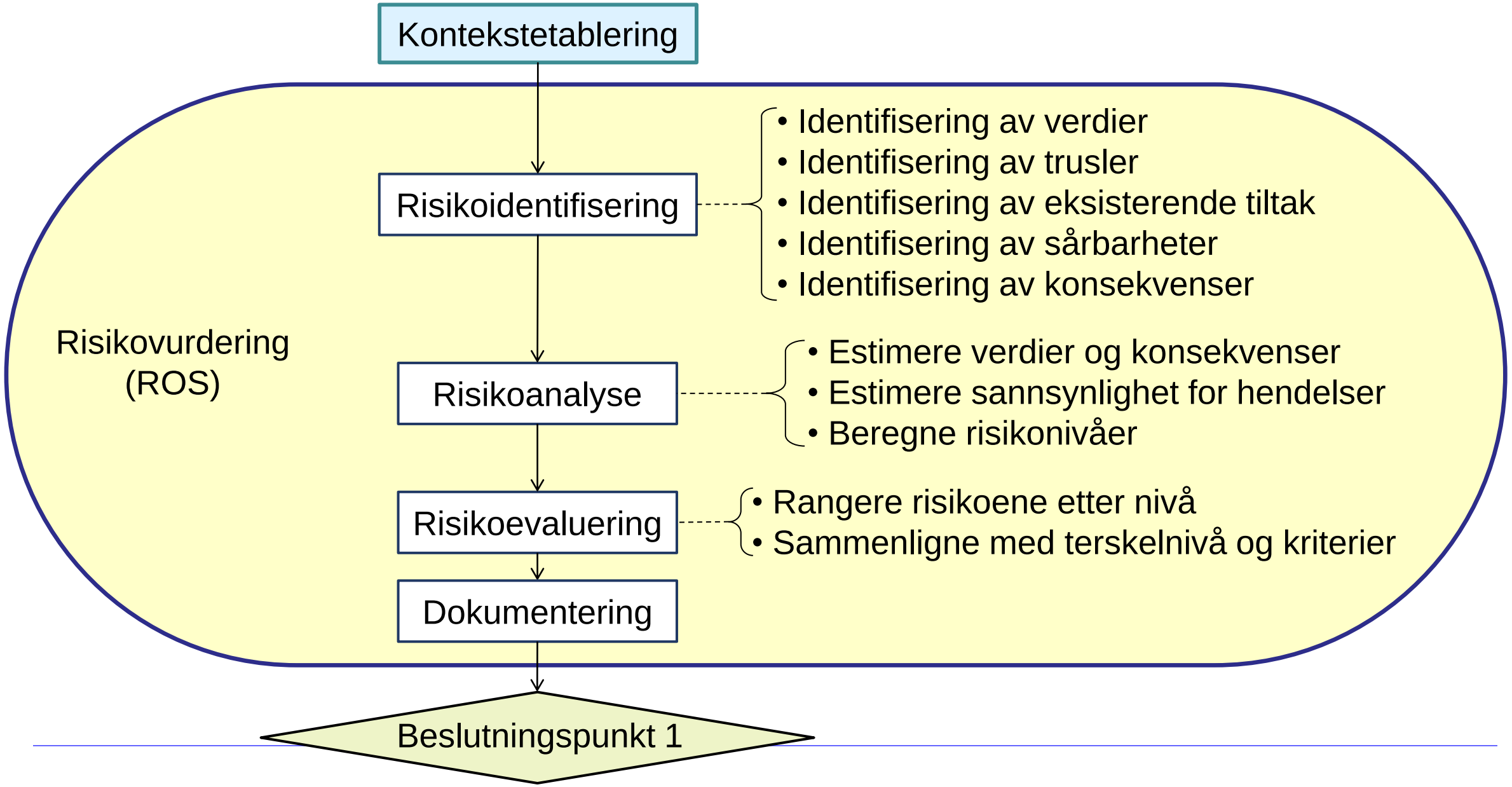
1. Risikoidentifisering
2. Risikoanalyse
3. Risikoevaluering
4. Regneark for risikovurdering

Del c: Risikovurdering (ROS-analyse)

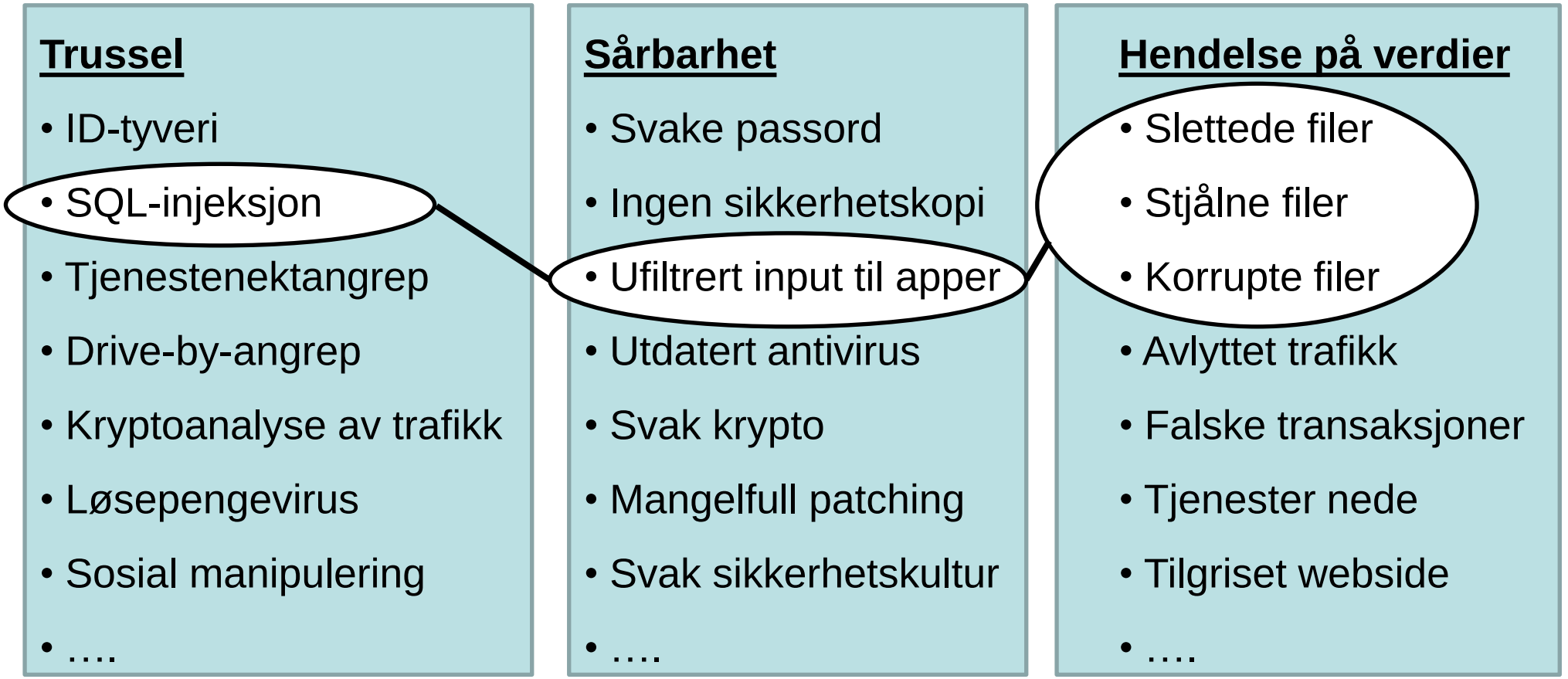
Risikostyring: ISO/IEC 27005



Prosess for risikovurdering – ISO/IEC 27005

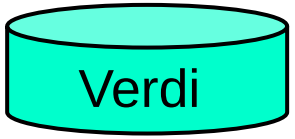


Risikoidentifisering



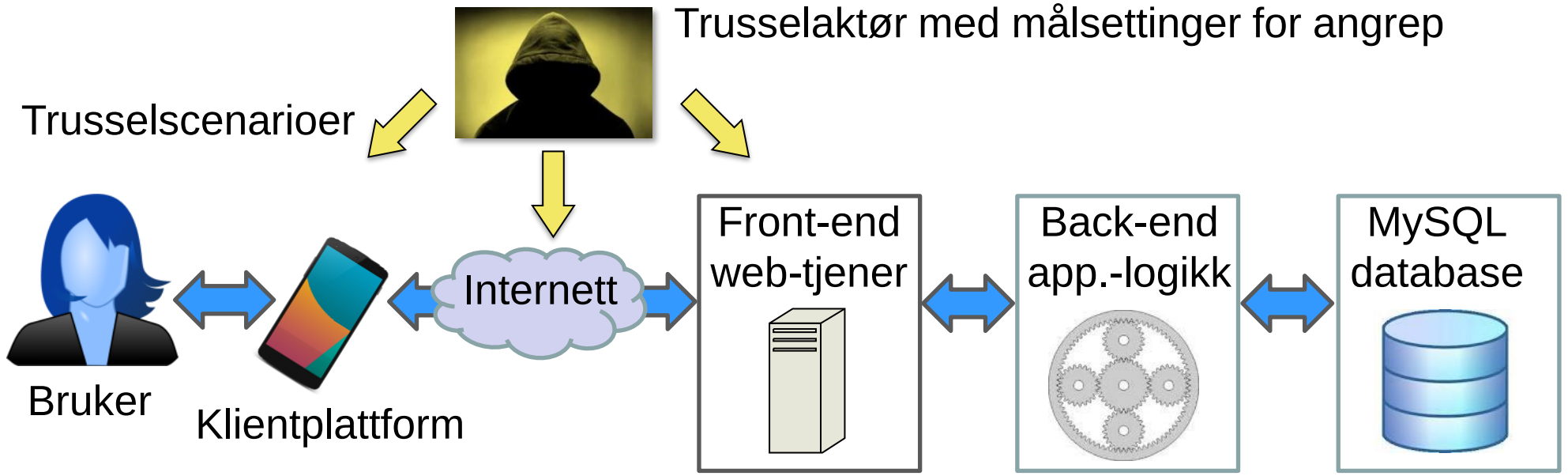
- Å identifisere en risiko betyr å finne en relevant kombinasjon av en trussel, sårbarhet(er) og hendelse(r) som kan skade verdier.

Kartlegging av verdier / ressurser



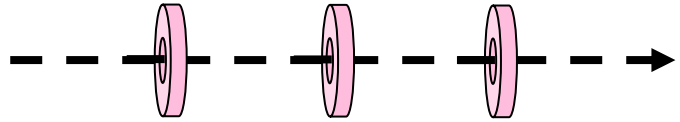
- Bredt spekter av verdier / ressurser
  - Driftsdata, persondata, system, nettverk, applikasjoner, prosesser, tjenester, etc.
- Umulig å skaffe total oversikt
  - Det er heller ikke viktig med total oversikt
  - Trusselmodelleringen vil peke ut relevante verdier
- Ansvar for å identifisere verdier ligger 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



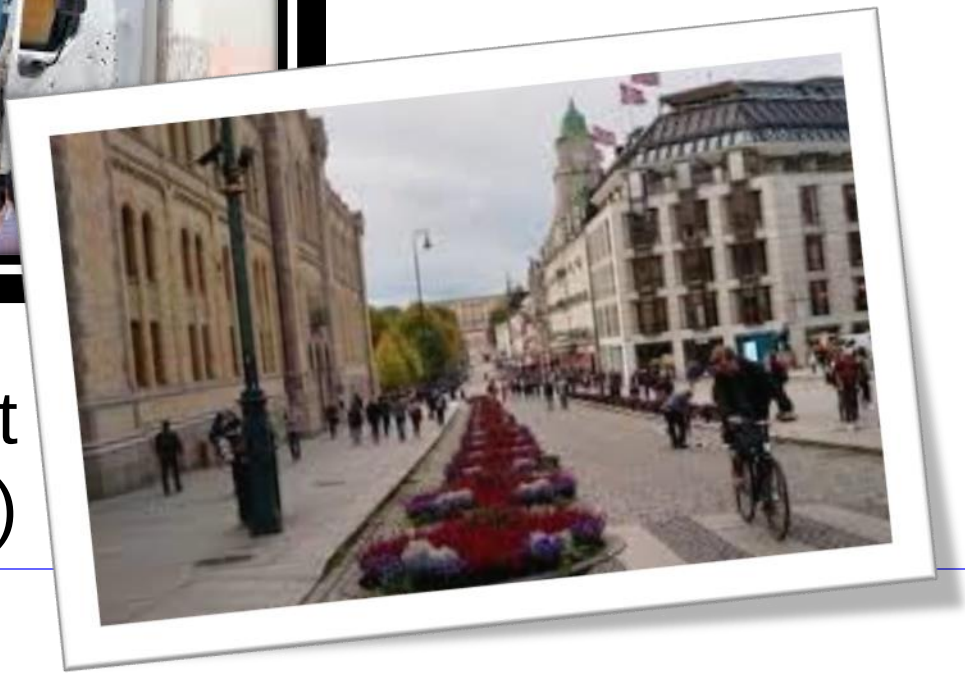
- Sårbarheter er muligheter som trusselaktører kan utnytte for å angripe systemer og informasjonsressurser.
- Generell identifisering av sårbarheter
  - Å identifisere en sikkerhetssårbarhet er det samme som å finne ut hvordan man kan stoppe et bestemt trusselscenario.
  - Fjerning av en sikkerhetssårbarhet 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

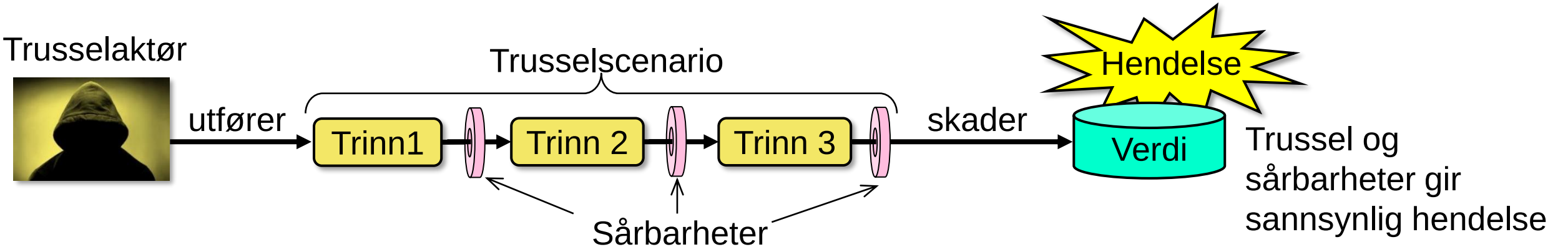
Nice
Berlin
London
Barcelona

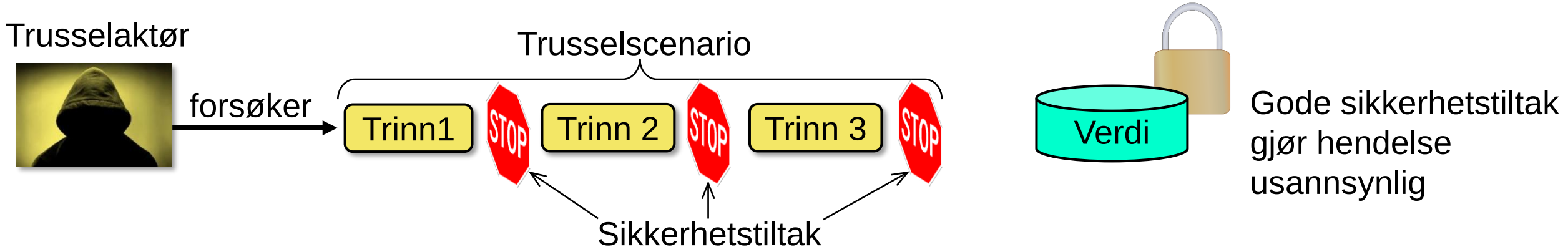
Ny trussel oppstod i 2016

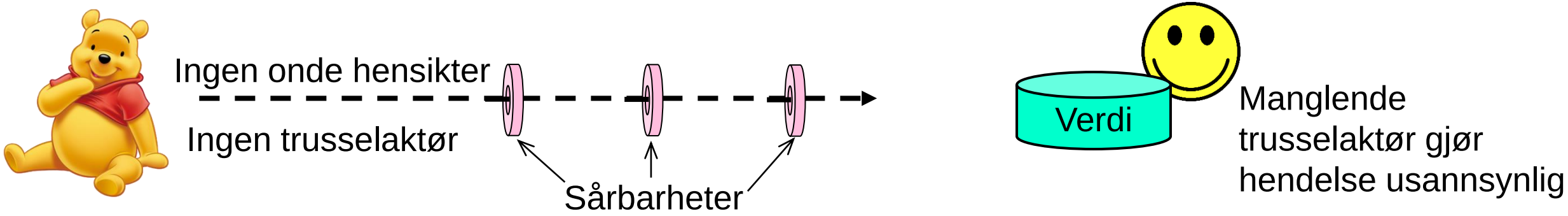


Trussel blokkert
(dvs. sårbarhet fjernet)

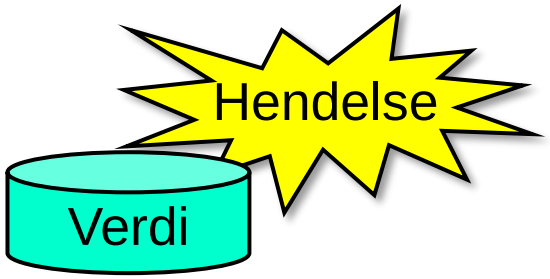
Sannsynlighet for at en hendelse inntreffer







Vurdering av konsekvenser



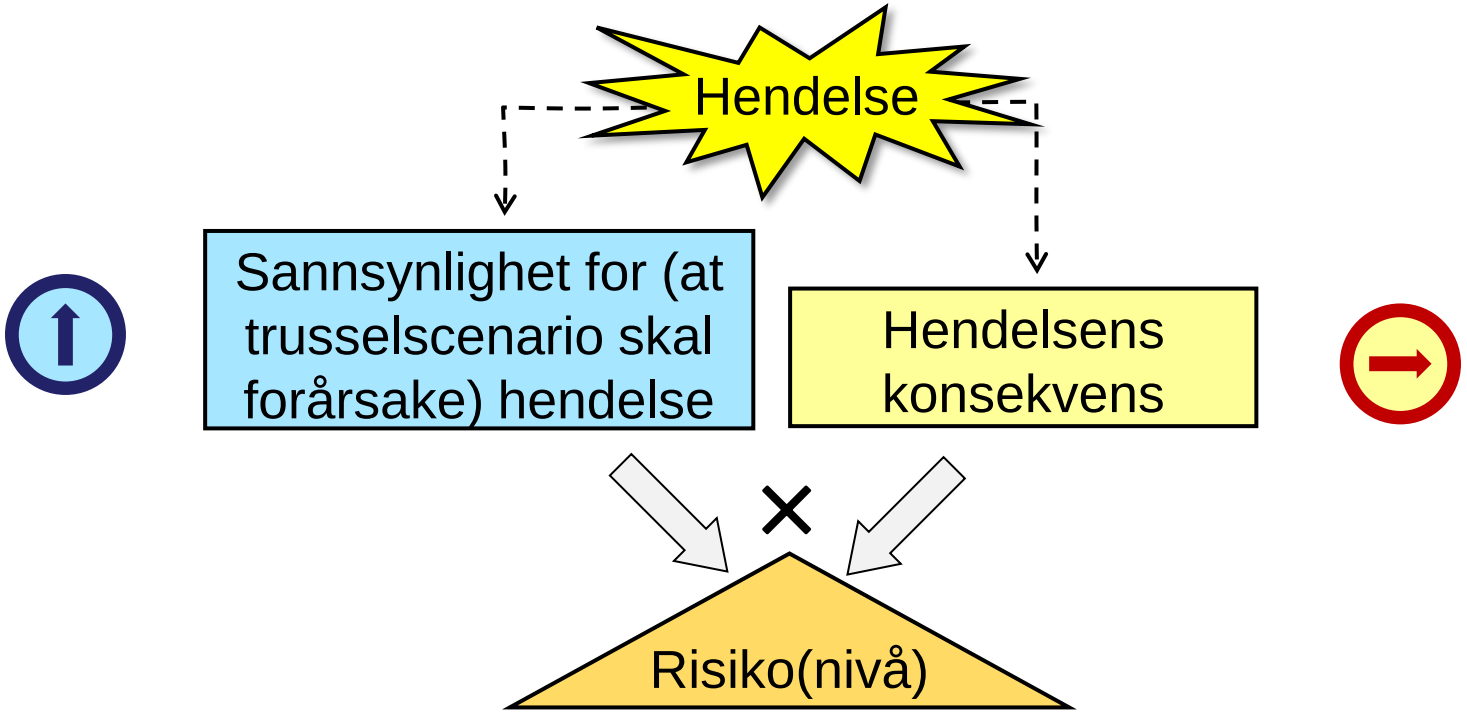
- En hendelse fører til brudd på sikkerhetsmål for verdier
  - **Brudd på sikkerhetsmål:** KIT + P for verdier
    (konfidensialitet, integritet, tilgjengelighet, personvern)
- Konsekvensnivået estimeres for hver type hendelse
- Konsekvenser kan bestå av ulike aspekter:
  - Redusert omsetning/profitt, 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.

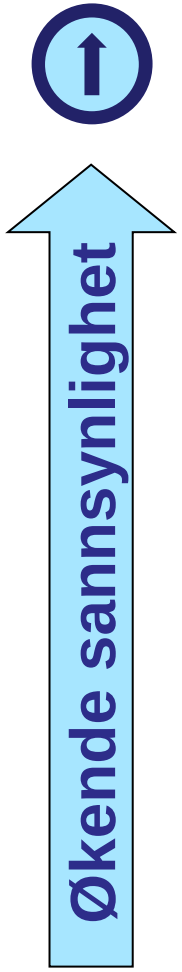
Risikoanalyse

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

Kvantitativ risikoberegning

NOK $ €

- Flere ulike metoder.
- Eksempel på enkel kvantitativ metode:
  - Sannsynlighet P uttrykkes i intervallet [0, 1]
    - tolkes som relative frekvens av hendelser per år
    - P = 0,5 betyr at hendelsen er forventet annethvert år
  - Konsekvens K uttrykkes som absolutt pengeverdi
    - konsekvens er summen av konsekvensaspekter.
    - anta fire konsekvensaspekter k_1, k_2, k_3, k_4

$$K = k_1 + k_2 + k_3 + k_4$$

  - Risikonivå R beregnes som forventet tap (per år)

$$R = P \times K$$

Eksempel kvantitativ beregning NOK $ €

Case: Hacking av webside

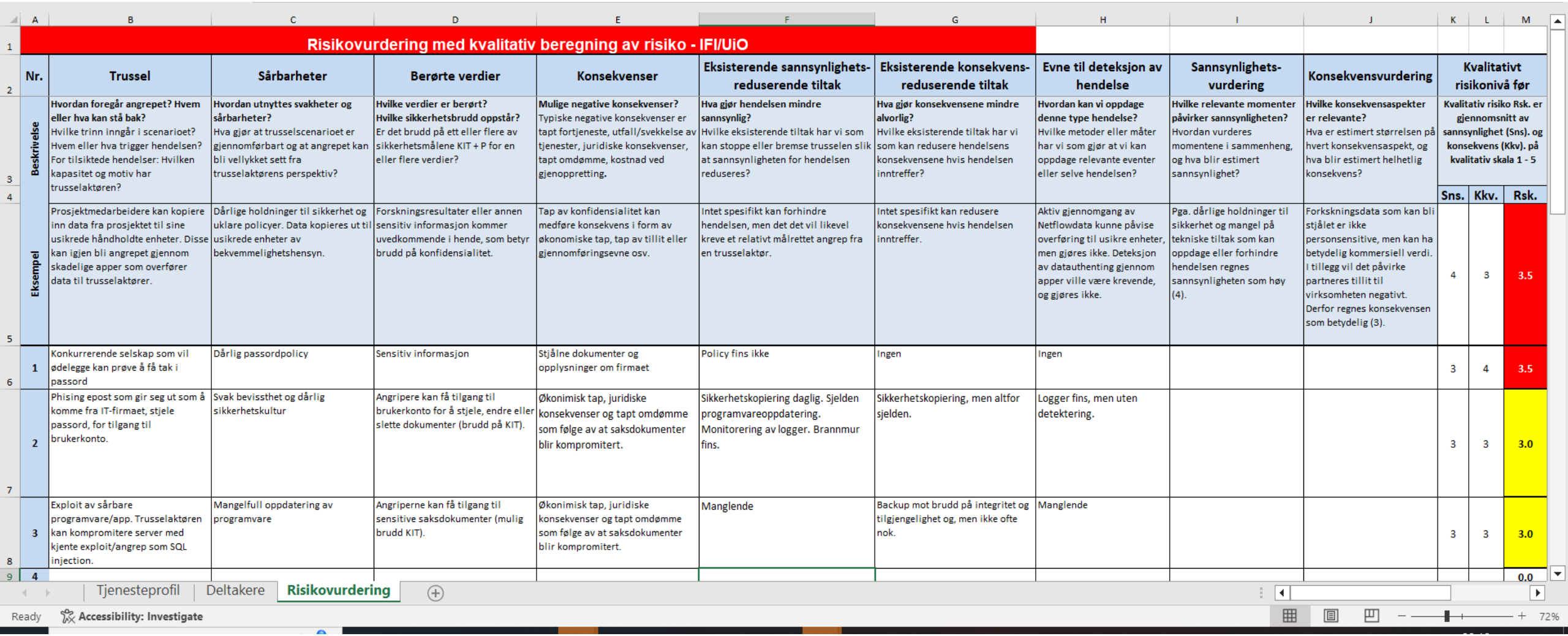
- Risiko: hacking med tilgrising og ødelagt webside
- Sannsynlighetsestimat
  - P = 0,5
- Konsekvensberegning
  - Tapt fortjeneste fordi websiden er nede, k_1 = NOK 500 000
  - Tapt omdømme k_2 = NOK 200 000
  - Kostnad med å rette opp websiden k_3 = NOK 100 000
  - $K = k_1 + k_2 + k_3$ = NOK 800 000
- Risikoberegning
  - $R = P \times K = 0,5 \times$ NOK 800 000 = NOK 400 000

- Kan berettige å bruke NOK 400 000 for å håndtere risiko
  - hvis risikonivået reduseres til NOK 0

Regneark for kvalitativ risikovurdering

- Mange ulike veiledere, maler og verktøy for risikovurdering
  - ➢ Ofte relativt komplisert, krever opplæring for å bruke
- Et enkelt regneark er lett å forstå.
- Kvalitative risikomatriser er tilnærmet additive
  - – Risikonivå = (Sannsynlighet + Konsekvens) / 2
  - ➢ Se regneark med kvalitativ risikoberegning:
- https://www.uio.no/studier/emner/matnat/ifi/IN5080/v24/oppgaver/uio-risikovurdering-kvalitativ.xlsx

Regneark for kvalitativ risikovurdering



Risikovurdering med kvalitativ beregning av risiko - IFI/UiO

Nr.	Trussel	Sårbarheter	Berørte verdier	Konsekvenser	Eksisterende sannsynlighets-reduserende tiltak	Eksisterende konsekvens-reduserende tiltak	Evne til deteksjon av hendelse	Sannsynlighets-vurdering	Konsekvensvurdering	Kvalitativt risikonivå før		
Beskrivelse	**Hvordan foregår angrepet? Hvem eller hva kan stå bak?** Hvilke trinn inngår i scenarioet? Hvem eller hva trigger hendelsen? For tilsiktede hendelser: Hvilken kapasitet og motiv har trusselaktøren?	**Hvordan utnyttes svakheter og sårbarheter?** Hva gjør at trusselscenarioet er gjennomførbart og at angrepet kan bli vellykket sett fra trusselaktørens perspektiv?	**Hvilke verdier er berørt? Hvilke sikkerhetsbrudd oppstår?** Er det brudd på ett eller flere av sikkerhetsmålene KIT + P for en eller flere verdier?	**Mulige negative konsekvenser?** Typiske negative konsekvenser er tapt fortjeneste, utfall/svekkelse av tjenester, juridiske konsekvenser, tapt omdømme, kostnad ved gjenoppretting.	**Hva gjør hendelsen mindre sannsynlig?** Hvilke eksisterende tiltak har vi som kan stoppe eller bremse trusselen slik at sannsynligheten for hendelsen reduseres?	**Hva gjør konsekvensene mindre alvorlig?** Hvilke eksisterende tiltak har vi som kan redusere hendelsens konsekvensene hvis hendelsen inntreffer?	**Hvordan kan vi oppdage denne type hendelse?** Hvilke metoder eller måter har vi som gjør at vi kan oppdage relevante eventer eller selve hendelsen?	**Hvilke relevante momenter påvirker sannsynligheten?** Hvordan vurderes momentene i sammenheng, og hva blir estimert sannsynlighet?	**Hvilke konsekvensaspekter er relevante?** Hva er estimert størrelsen på hvert konsekvensaspekt, og hva blir estimert helhetlig konsekvens?	**Kvalitativ risiko Rsk. er gjennomsnitt av sannsynlighet (Sns). og konsekvens (Kkv). på kvalitativ skala 1 - 5**		
										Sns.	Kkv.	Rsk.
Eksempel	Prosjektmedarbeidere kan kopiere inn data fra prosjektet til sine usikrede håndholdte enheter. Disse kan igjen bli angrepet gjennom skadelige apper som overfører data til trusselaktører.	Dårlige holdninger til sikkerhet og uklare policyer. Data kopieres ut til usikrede enheter av bekvemmelighetshensyn.	Forskningsresultater eller annen sensitiv informasjon kommer uvedkommende i hende, som betyr brudd på konfidensialitet.	Tap av konfidensialitet kan medføre konsekvens i form av økonomiske tap, tap av tillit eller gjennomføringsevne osv.	Intet spesifikt kan forhindre hendelsen, men det det vil likevel kreve et relativt målrettet angrep fra en trusselaktør.	Intet spesifikt kan redusere konsekvensene hvis hendelsen inntreffer.	Aktiv gjennomgang av Netflowdata kunne påvise overføring til usikre enheter, men gjøres ikke. Deteksjon av datauthenting gjennom apper ville være krevende, og gjøres ikke.	Pga. dårlige holdninger til sikkerhet og mangel på tekniske tiltak som kan oppdage eller forhindre hendelsen regnes sannsynligheten som høy (4).	Forskningsdata som kan bli stjålet er ikke personsensitive, men kan ha betydelig kommersiell verdi. I tillegg vil det påvirke partneres tillit til virksomheten negativt. Derfor regnes konsekvensen som betydelig (3).	4	3	3.5
1	Konkurrerende selskap som vil ødelegge kan prøve å få tak i passord	Dårlig passordpolicy	Sensitiv informasjon	Stjålne dokumenter og opplysninger om firmaet	Policy fins ikke	Ingen	Ingen			3	4	3.5
2	Phising epost som gir seg ut som å komme fra IT-firmaet, stjele passord, for tilgang til brukerkonto.	Svak bevissthet og dårlig sikkerhetskultur	Angripere kan få tilgang til brukerkonto for å stjele, endre eller slette dokumenter (brudd på KIT).	Økonimisk tap, juridiske konsekvenser og tapt omdømme som følge av at saksdokumenter blir kompromitert.	Sikkerhetskopiering daglig. Sjelden programvareoppdatering. Monitorering av logger. Brannmur fins.	Sikkerhetskopiering, men altfor sjelden.	Logger fins, men uten detektering.			3	3	3.0
3	Exploit av sårbare programvare/app. Trusselaktøren kan kompromitere server med kjente exploit/angrep som SQL injection.	Mangelfull oppdatering av programvare	Angriperne kan få tilgang til sensitive saksdokumenter (mulig brudd KIT).	Økonimisk tap, juridiske konsekvenser og tapt omdømme som følge av at saksdokumenter blir kompromitert.	Manglende	Backup mot brudd på integritet og tilgjengelighet og, men ikke ofte nok.	Manglende			3	3	3.0
4												0.0

Tjenesteprofil | Deltakere | Risikovurdering

Ready | Accessibility: Investigate | 72%

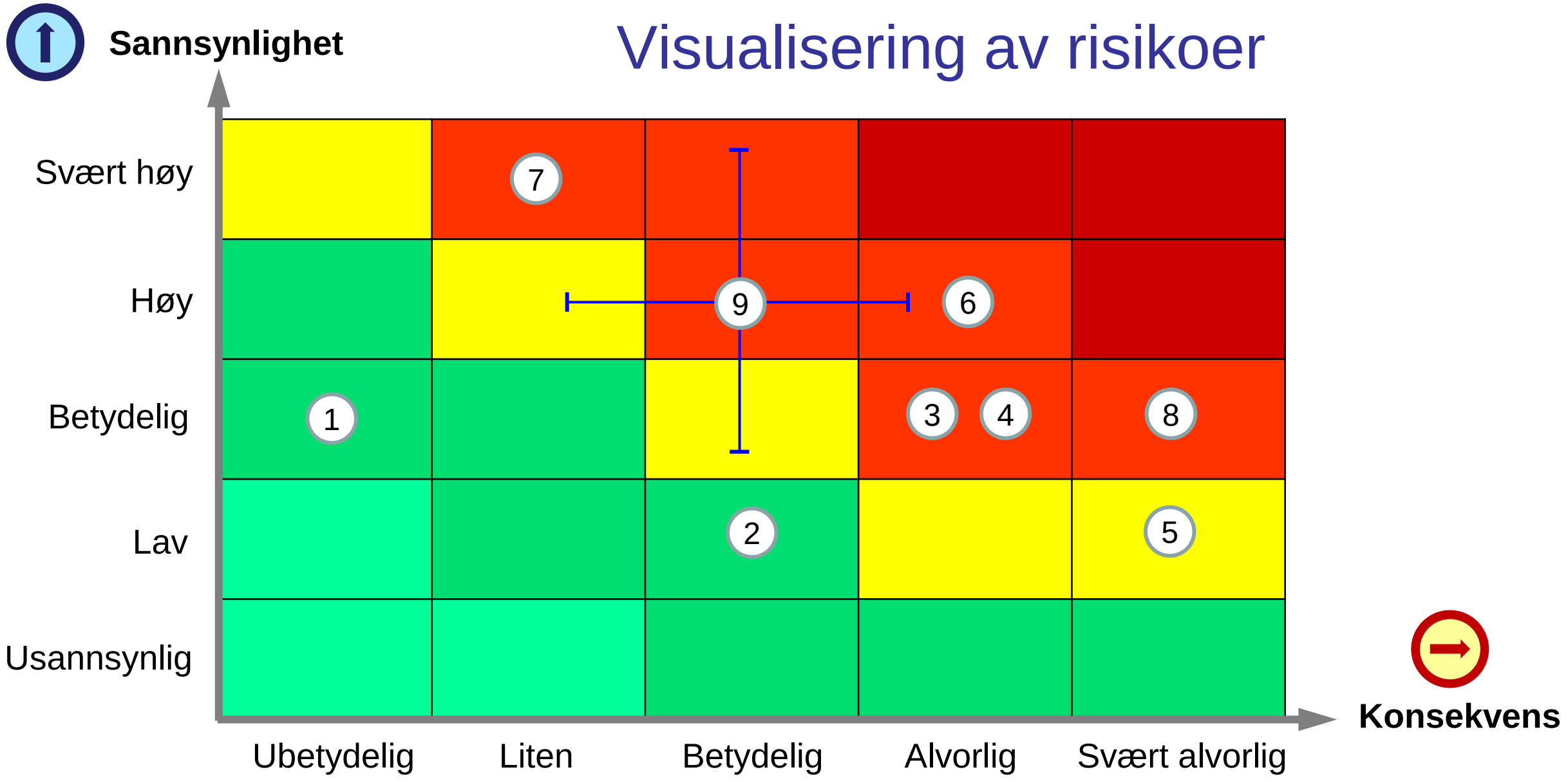
Forklaring av regneark

- Trussel
  - Trusselscenario og eventuelt trusselaktør
- Sårbarhet
  - Hvilke svakheter og feil som gjør at trusselscenarioet kan gjennomføres
- Berørte verdier
  - Beskriver hendelse på verdi(er) (brudd på sikkerhetsmål)
- Konsekvenser
  - Beskriv forventede konsekvenser av hendelsen
- Eksisterende sikkerhetstiltak
  - 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?
- Gi forklaring og estimer sannsynlighet og konsekvens
- Beregning av risikonivå
  - Kvalitativ risiko = (kvalitativ sannsynlighet + kvalitativ konsekvens)/2
- Nye tiltak
  - Forslag til nye sikkerhetstiltak for å forhindre hendelsen eller mitigere konsekvenser
- Beregning av risikonivå etter tiltak

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.

Visualisering av risikoer



Slutt på presentasjon