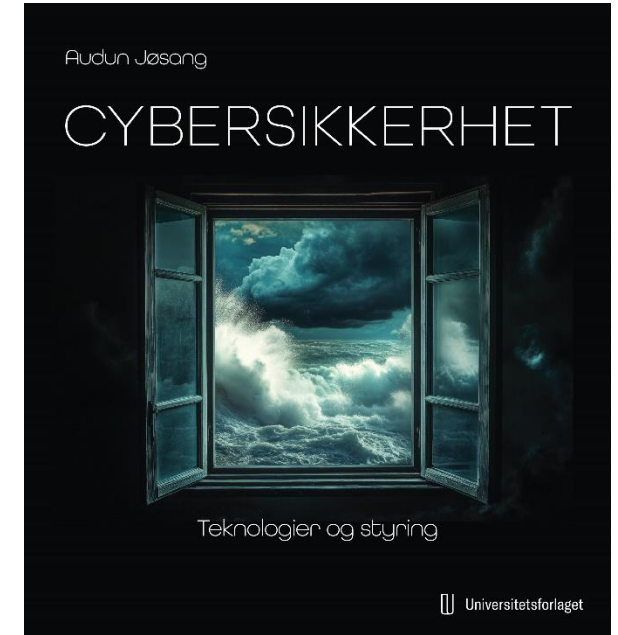


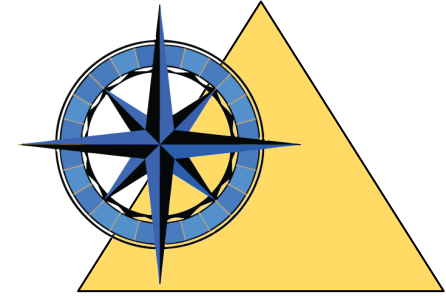
Kapittel 19:

Risikostyring for cybersikkerhet

Cybersikkerhet: Teknologier og styring
Audun Jøsang
3. utg. 2025
Universitetsforlaget



Oversikt: Risikostyring



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

Typer av Risiko



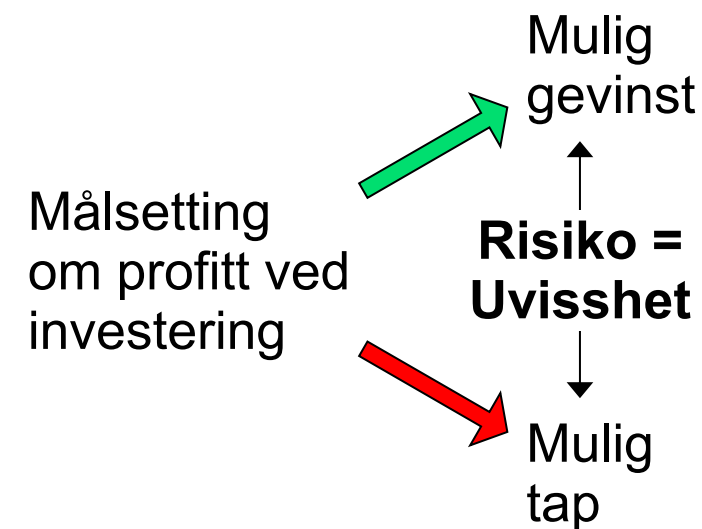
Hva er risiko, og IS-risiko?

- ISO 31000 Risikostyring og ISO 27000 Oversikt og begreper
 - **“Risiko er effekten av uvisshet (aka. usikkerhet) 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.”**

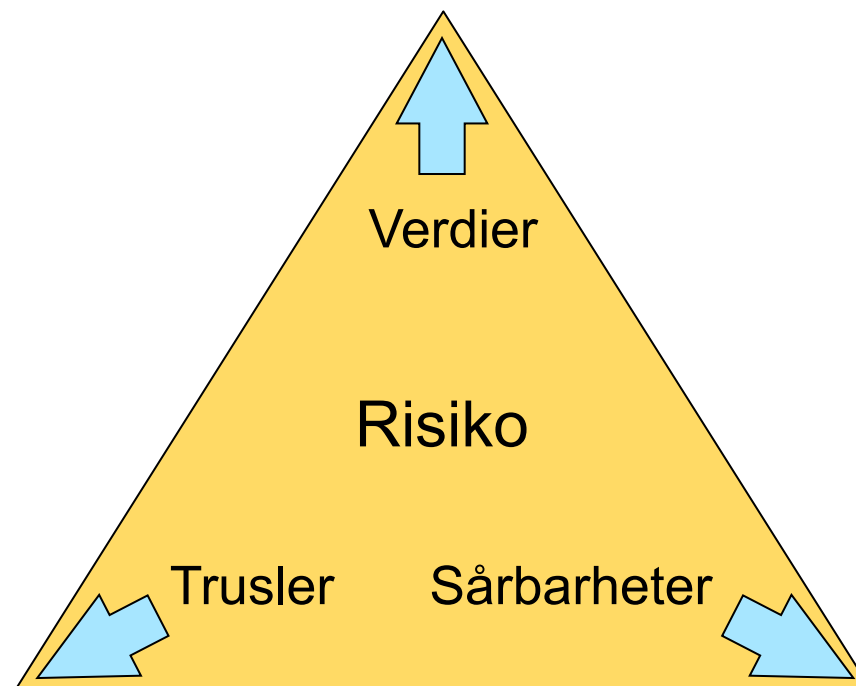


Tolkninger av risiko

1. Risiko = Avstand mellom antatt mulig gevinst og tap
 - Eksempel: Finansrisiko ved investering er høy når man anser det for mulig at investeringen kan gi høyt utbytte eller stort tap.
 - Uvissheten ligger i at det er vanskelig å forutsi forventet resultat.
2. Risiko = Grad av forventet tap ved drift (operasjon)
 - Eksempel: Cyberrisiko er høy når cybersikkerhet gir sannsynlighet for cyberhendelse med stor negativ konsekvens som medfører tap.
 - Risikoen er ikke nødvendigvis befengt med uvisshet.
 - Det kan være uvisshet rundt estimering av sannsynlighet og konsekvens, men risikoen er ikke proporsjonal med uvissheten.
 - Cyber-risiko øker proporsjonalt med økende cybersikkerhet (mangel på beskyttelse av digitale verdier mot skade).



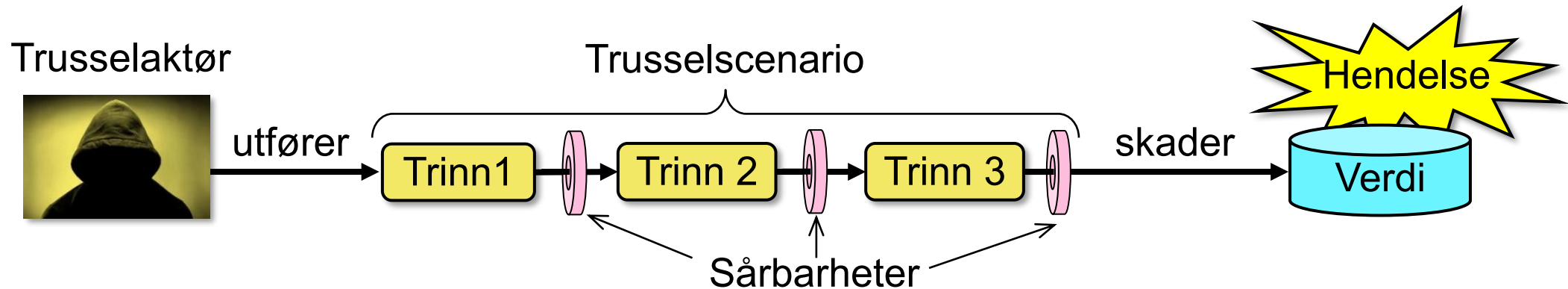
Generell risikomodell (NSM)



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

Trusler

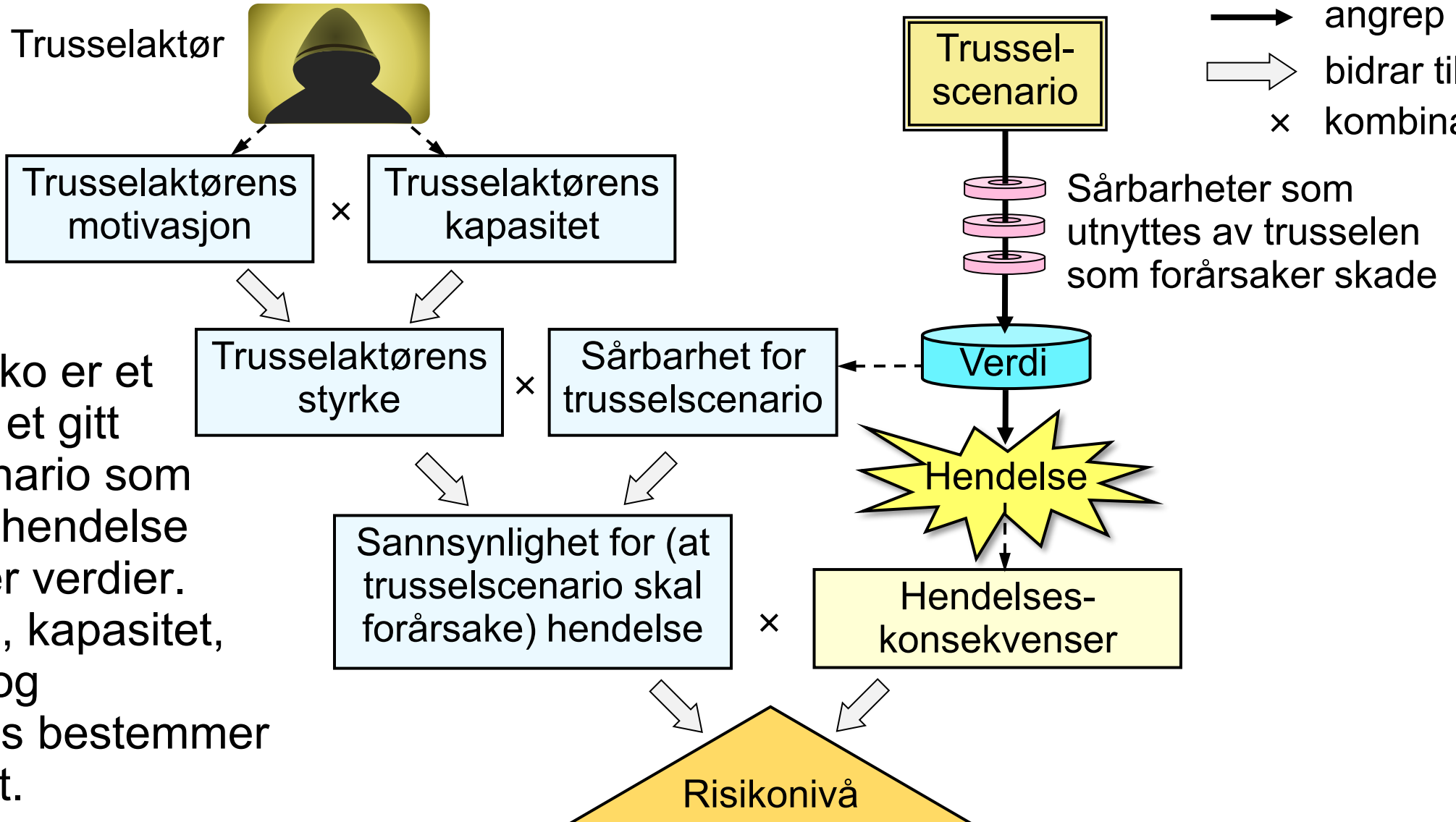
- **Trusselscenario:** En sekvens av trinn eller hendelser som kan styres eller utløses av en trusselaktør, og som kan skade verdier/ressurser. Et trusselscenario er mulig å gjennomføre når det fins sårbarheter (svakheter) som kan utnyttes.
- **Trusselaktør:** En aktiv entitet som kan styre eller utløse trusselscenarioer. 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

Forklaring:

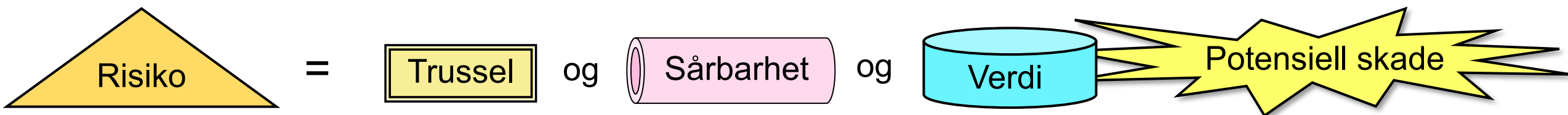
---> har
—> angrep
⇒ bidrar til
× kombinasjon



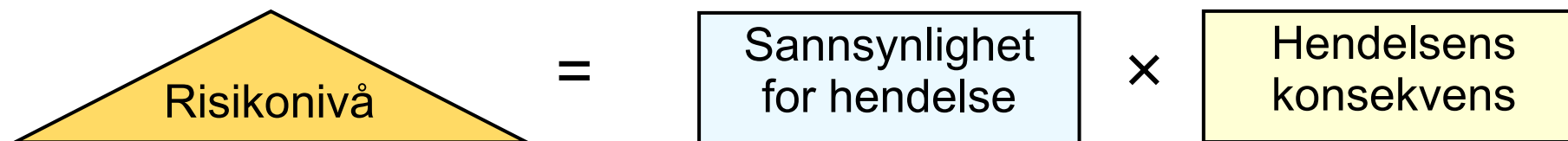
- Enhver risiko er et resultat av et gitt trusselsscenario som fører til en hendelse som skader verdier.
- Motivasjon, kapasitet, sårbarhet og konsekvens bestemmer risikonivået.

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.

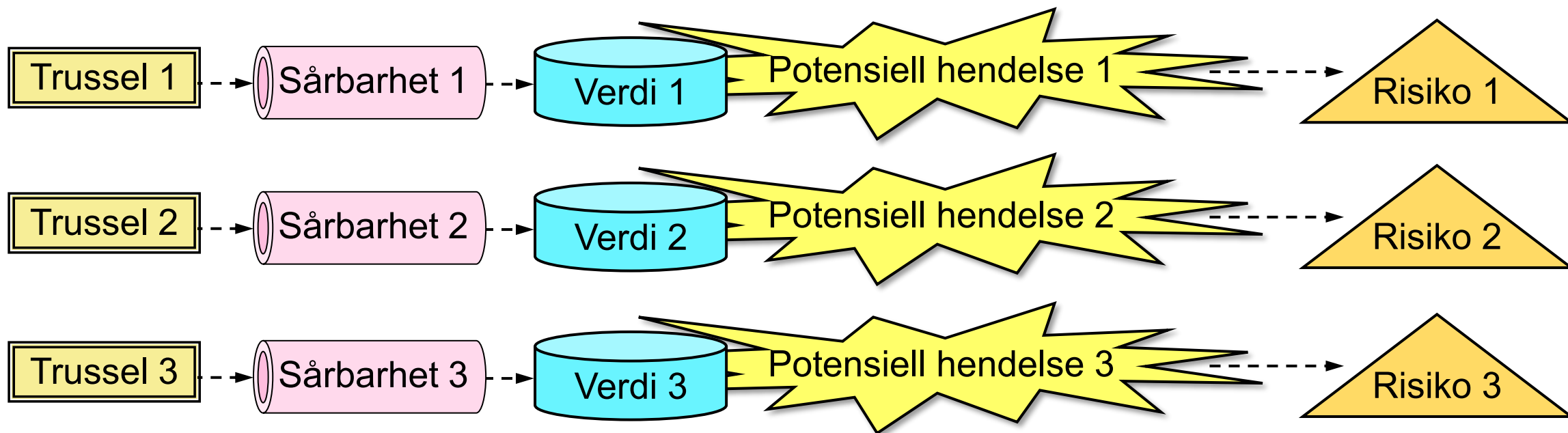


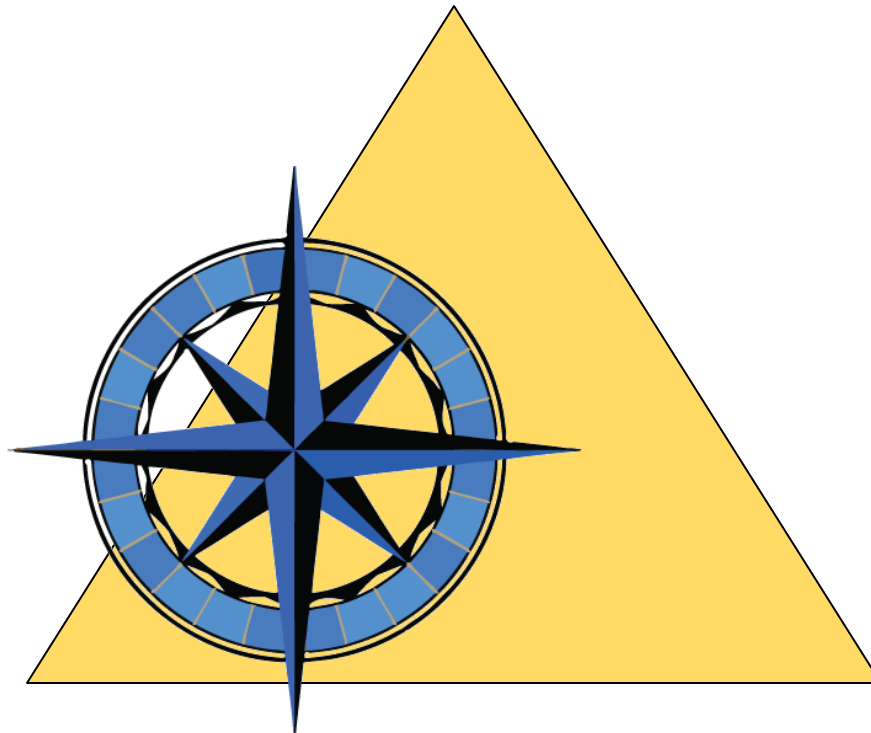
- **Risikonivå** (også kalt risikoeksponering) er kombinasjonen av hendelsens sannsynlighet og konsekvens. Risikonivå beregnes med risikoanalyse.



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 $\Rightarrow$ mange risikoer





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



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

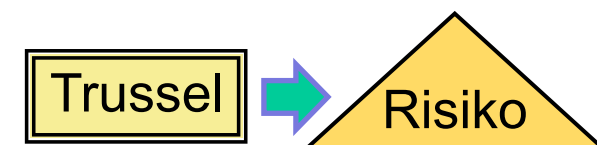
- Aktiviteter innen risikostyring kan ha ulike målsettinger. Det kan f.eks. være en eller flere av følgende:

- å få oversikt over digitale eiendeler og deres 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 digitale 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 eiendeler, estimere deres verdier og forstå deres beskyttelsesbehov.
- 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 digitale eiendeler og ansvar for å håndtere de identifiserte risikoene.

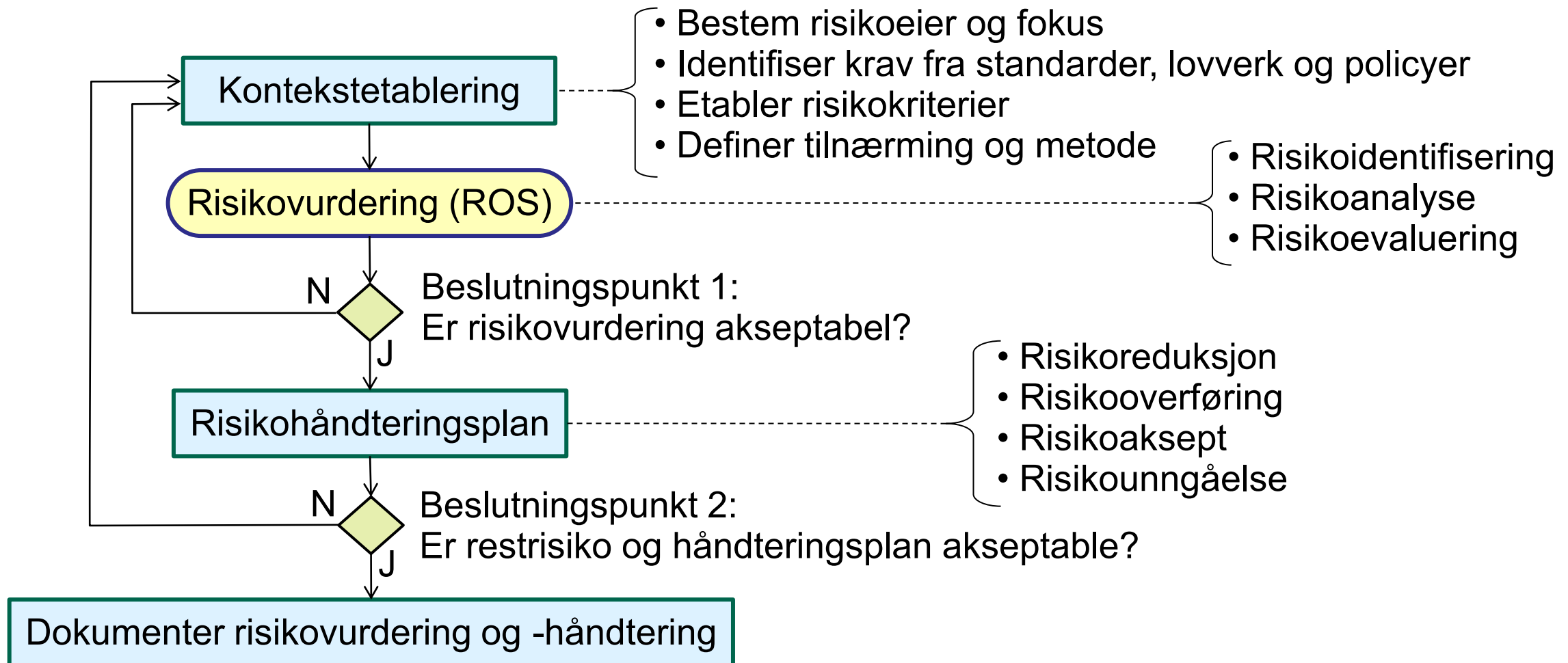
Roller involvert i risikovurdering og risikohåndtering



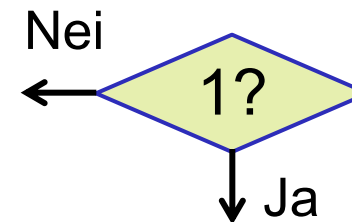
Ledelse, eiere, brukere og fageksperter må samarbeide.

- Eiere må hjelpe til med å
 - lage oversikt over digitale eiendeler, og spesifisere sikkerhetsbehov (KIT+P)
 - vurdere konsekvens av brudd på sikkerhetsmål og behov
- 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

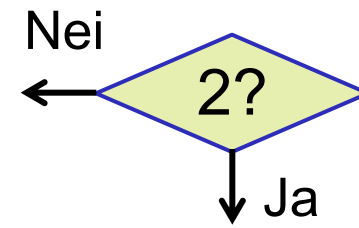


Er risikovurderingen tilfredsstillende?

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

- a. Relativt dårlig spredning av risikonivåer.
 - Spredningen kan forbedres med rekalkibrering 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.

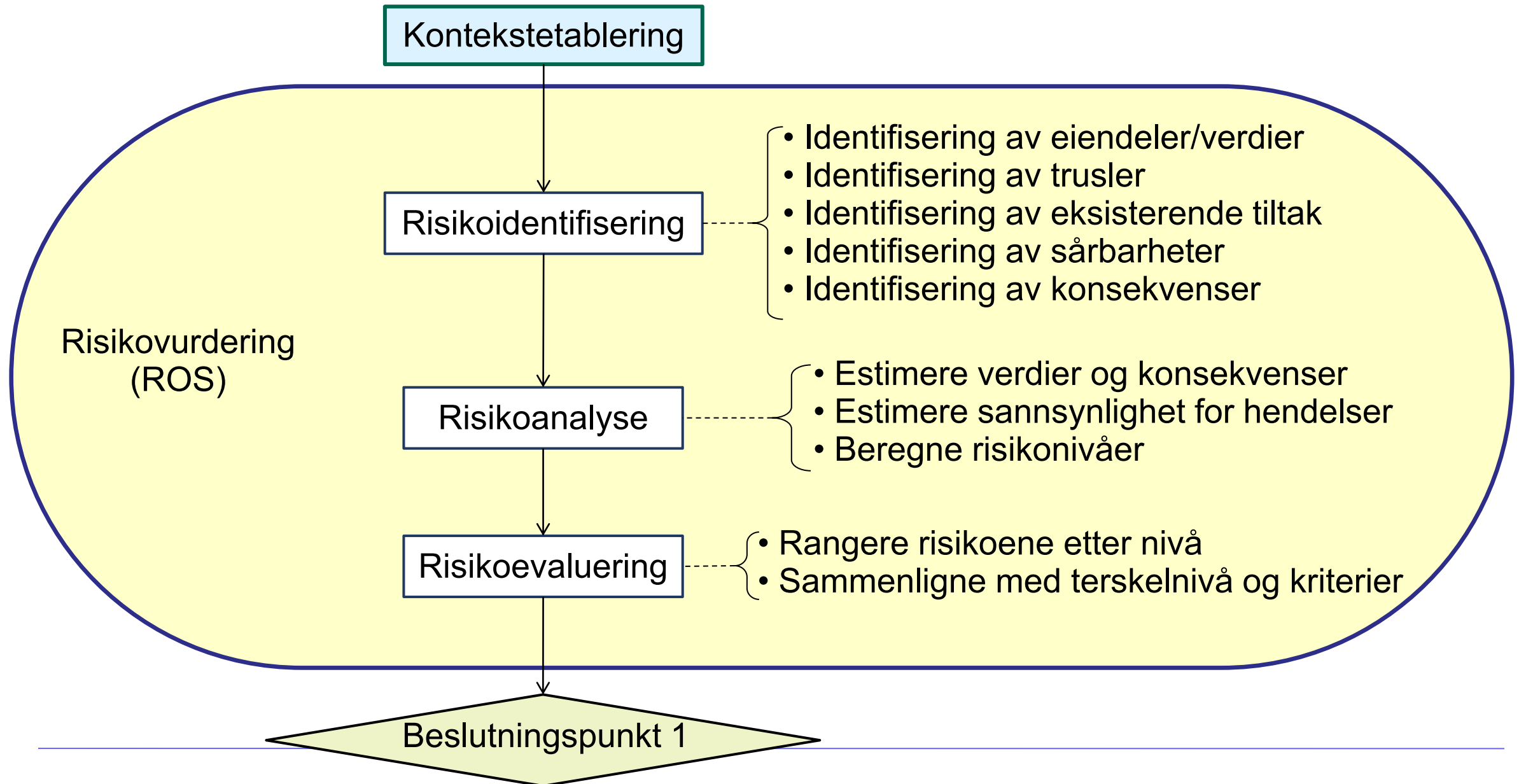
- Tilpass budsjett ved å øke budsjettet eller kutte tiltak.



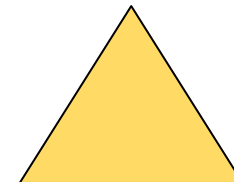
1. Risikoidentifisering
2. Risikoanalyse
3. Risikoevaluering
4. Regneark for risikovurdering

Del c: Risikovurdering (ROS-analyse)

Prosess for risikovurdering – ISO/IEC 27005



Risikoidentifisering



Trussel

- ID-tyveri
- SQL-injeksjon
- Tjenestenektangrep
- Drive-by-angrep
- Kryptoanalyse av trafikk
- Løsepengevirus
- Sosial manipulering
-

Sårbarhet

- Svake passord
- Ingen sikkerhetskopi
- Ufiltrert input til apper
- Utdatert antivirus
- Svak krypto
- Mangelfull patching
- Svak sikkerhetskultur
-

Hendelse på verdier

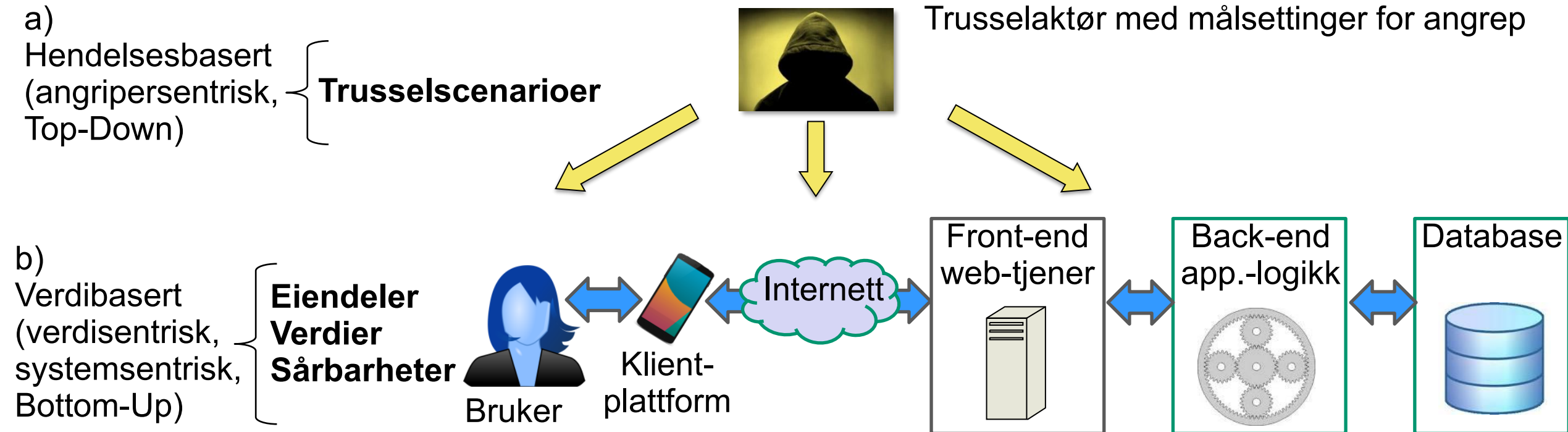
- Slettede filer
- Stjalne filer
- Korrupte filer
- Avlyttet trafikk
- Falske transaksjoner
- Tjenester nede
- Tilgriset webside
-

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



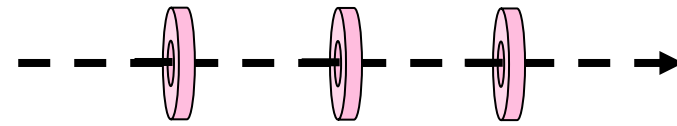
- Bredt spekter av verdier / ressurser
 - Digitale eiendeler ENHETER, APPER, NETTVERK, DATA og BRUKERE fra cyberforsvarsmatrisen er et utgangspunkt (kap. 18).
 - Vurder også ulike kategorier data, samt forretningsprosesser, tjenester, etc.
- Umulig å skaffe total oversikt
 - Det er heller ikke viktig med total oversikt
 - Trusselmodellering bidrar til å peke ut relevante digitale eiendeler
- Ansvar for å identifisere eiendeler/verdier ligger hos eiere
 - Derfor må eiere delta i risikovurdering
- For hver verdi bør det spesifiseres
 - Viktighet av sikkerhetsmålsettinger (KIT + P)
 - Mulige konsekvenser for brudd på sikkerhetsmål

Risikoidentifisering / Trusselmodellering (ISO/IEC 27005 7.2.1)



- Risikoidentifisering består av å kartlegge, analysere og beskrive relevante risikoer/trusselscenarier.
- Utfordringen er å identifisere relevante risikoer
- 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 og skade digitale eiendeler/verdier.
- 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)

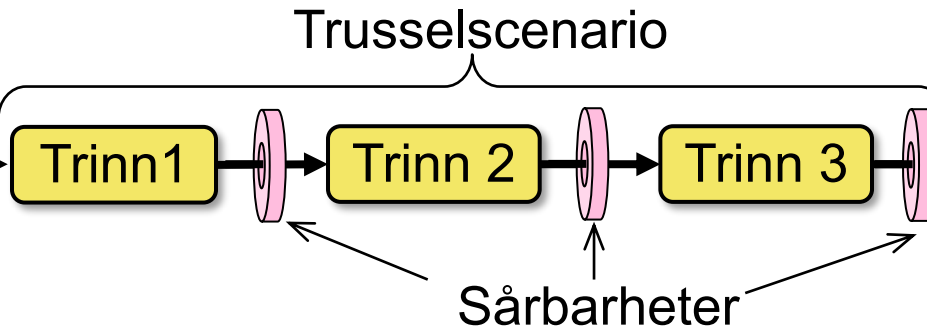
Sannsynlighet/trolighet for at en hendelse inntreffer



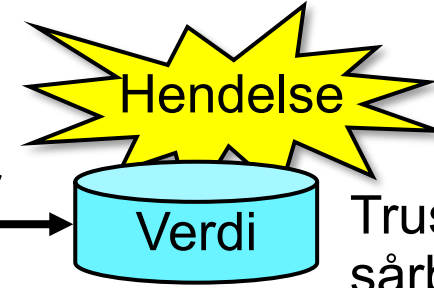
Trusselaktør



utfører



skader

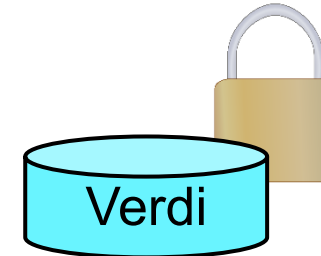
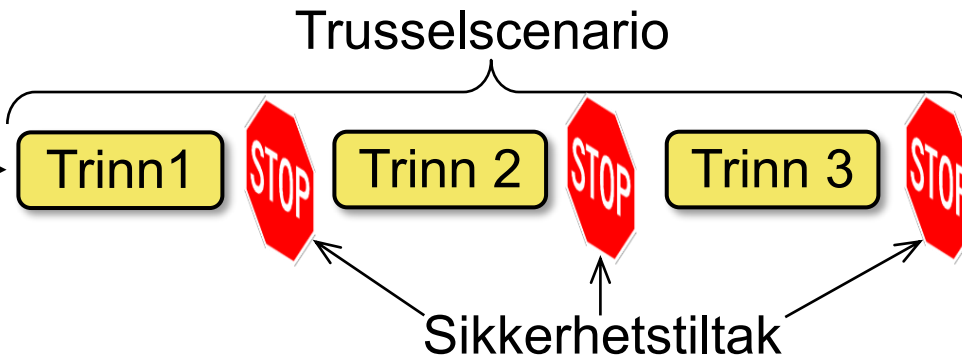


Trussel og sårbarheter gir sannsynlig hendelse

Trusselaktør



forsøker

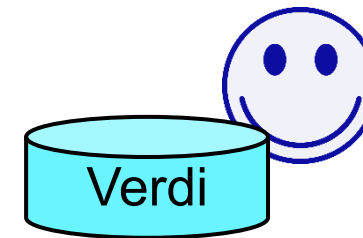
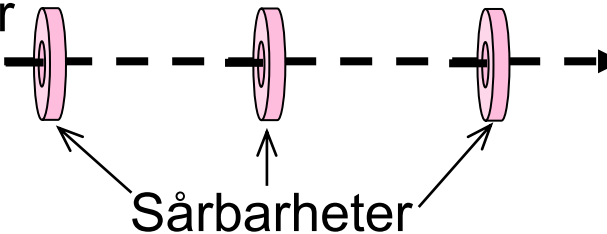


Gode sikkerhetstiltak gjør hendelse usannsynlig



Ingen onde hensikter

Ingen trusselaktør

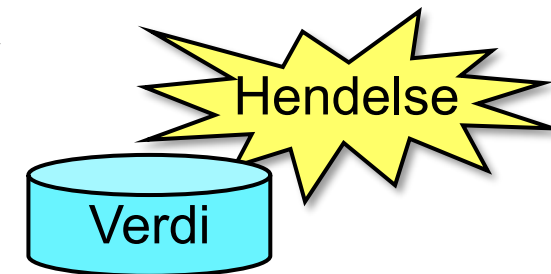


Manglende trusselaktør gjør hendelse usannsynlig

Vurdering av konsekvenser (ISO/IEC 6.4.3.2)



- En hendelse fører til brudd på sikkerhetsmål for verdier
 - **Brudd på sikkerhetsmål:** KIT + P for digitale verdier (konfidensialitet, integritet, tilgjengelighet, personvern)
- Konsekvenser kan bestå av ulike aspekter:



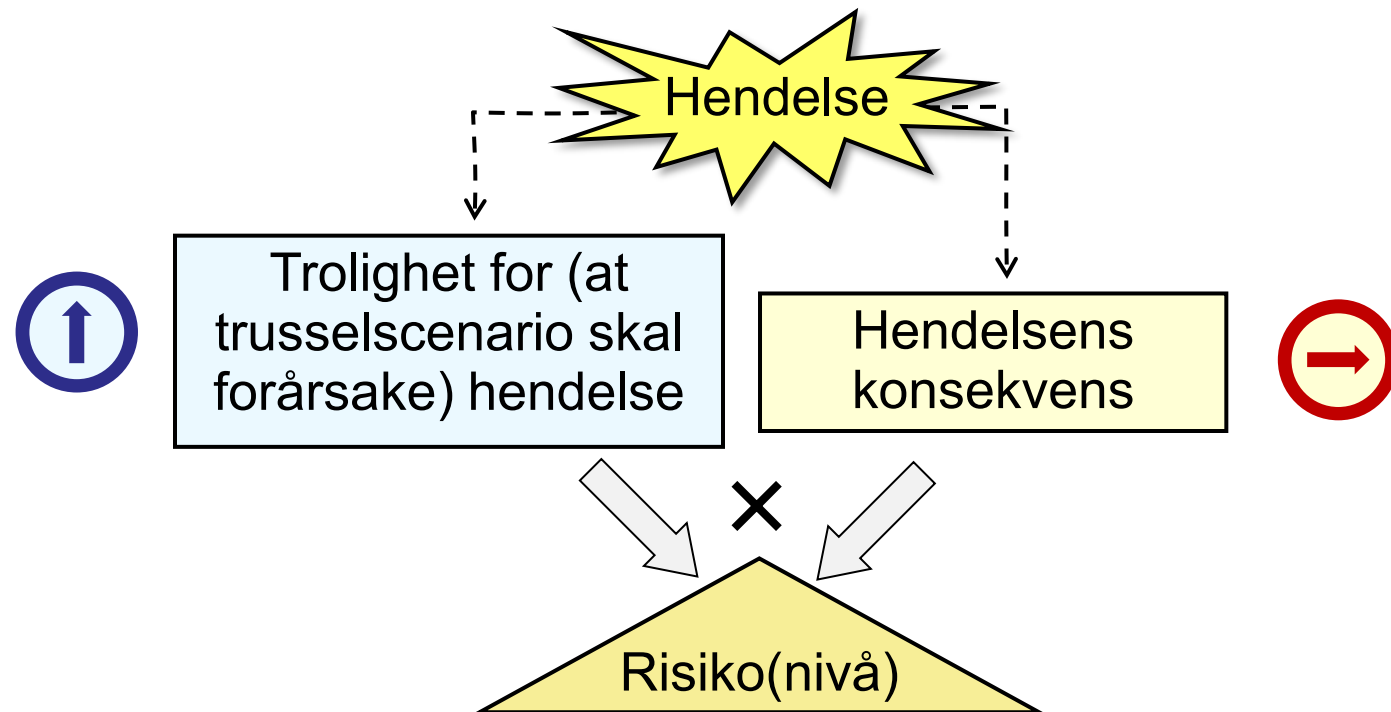
- Redusert omsetning/profitt, tap 
- Svekket ytelse av tjeneste 
- Brudd på juridisk etterlevelse, advokatutgifter, erstatning, bøter §
- Skadet omdømme 
- Kostnader ved håndtering og gjenoppretting 
- Belastning og skade på liv og helse for ansatte og brukere 
- Tap av frihet, verdighet eller retten til personvern; 

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

- Trolighet (eng. likelihood) (frekvens eller sannsynlighet) av hver type hendelse
- Konsekvens for verdier som følge av hver type hendelse



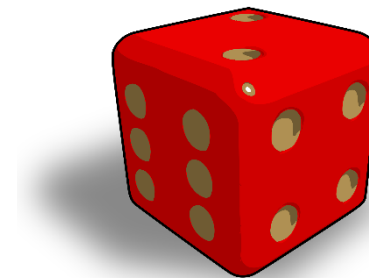
Frekvens eller sannsynlighet

- Trolighet (eng. likelihood) for en hendelse kan uttrykkes som
 - Frekvens F (antall hendelser per tidsperiode)
 - Sannsynlighet P for at hendelse skjer innen en tidsperiode.
- Ved risikovurdering er det vanligst å bruke frekvens.
- Det er meningsløst å betrakte sannsynlighet P uten et tidsperspektiv
- Sannsynligheten for at verden går under innen evigheten er $P = 1$.



Frekvens eller sannsynlighet

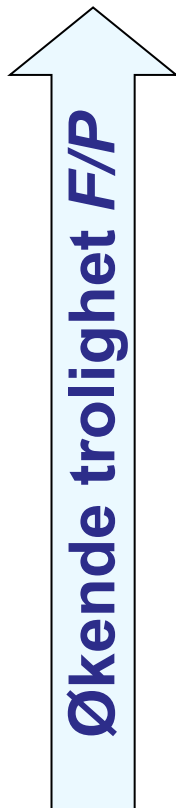
Case: Kaste terning



Anta at du kaster en terning hvert 10. sekund.

- Frekvens for å kaste «2» er ca.
 - $F = \frac{1}{6}$ per 10 sekunder,
 - $F = 1$ per minutt, og
 - $F = 60$ per time.
- Sannsynlighet for å kaste «2» er ca.
 - $P = \frac{1}{6}$ innen 10 sekunder,
 - $P = 1 - (1 - \frac{1}{6})^6$ innen 1 minutt
 - $P = 1 - (1 - \frac{1}{6})^{60}$ innen 1 time
- Konklusjon: Det er mye enklere å beregne frekvenser enn sannsynligheter.

Trolighetsskala (ISO/IEC 27005 6.4.3.3; 7.3.1.c; Tab.A.2 og A4)



Frekvens	Beskrivelse
(5) Snarest 1 gang per dag	Det fins motiverte trusselaktører som med letthet kan nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet for denne risikoen.
(4) Sannsynlig 1 gang per uke	Motiverte trusselaktører vil med høy sannsynlighet nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet.
(3) Mulig 1 gang/2 mndr	Trusselaktører har en betydelig mulighet til å nå sitt mål ved å bruke det vurderte trusselscenarioet.
(2) Usannsynlig 1 gang/2 år	Trusselaktører har relativt liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet.
(1) Sjelden 1 gang/20 år	Trusselaktører har svært liten mulighet til å nå angrepsmålet med det vurderte trusselscenarioet.
(0) Aldri 1 gang/200 år	Det er antagelig umulig for trusselaktører å nå angrepsmålet med det vurderte trusselscenarioet.

- Skalaen over er et eksempel. Nivåer og fortolkning kan kalibreres etter behov.

Konsekvensskala (ISO/IEC 27005 6,4,3,2 eks.1; 7.3.1.c, Tab.A.1 og A5)



Økende konsekvens

Konsekvensnivå	Beskrivelse
(5) Verst \$10 millioner	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 \$1 million	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 \$100 000	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 \$10 000	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 \$1000	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. Nivåer og fortolkning kan 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 trolighet F/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



Logaritmisk sannsynlighet og konsekvens

(Norsk utgave av ISO/IEC 27005 Tillegg A.1.1.3.1, øverst s.45)

- Prinsipp for logaritme: $\log(10^X \cdot 10^Y) = X + Y$
- Multiplikativ beregning av kvantitativ risiko: *trolighet* · *konsekvens*
- Additiv beregning av logaritmisk risiko: *trolighet* + *konsekvens*

Eksponeisering og logaritme



- Eksponeisering 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 $0,001 = 10^{-3} = \frac{1}{1000}$
- Eksponeisering 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 frekvens



- Den kvantitative frekvensskalaen er logaritmisk.
- F_{Max} er kalibreringsfaktoren for antatt maksimal frekvens (snarest), tilsvarende høyeste kvalitative nivå (nivå 5).
- Lavere frekvenser bestemmes deretter etter logaritmisk skala.
- F_{Kval} er ordinal kvalitativ frekvens (intervall $[0, 5]$).
- Sett f.eks. $F_{\text{Max}} = 500$ ganger/år, dvs ca. hver dag
- Kvantitativ frekvens: $F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X$ der $X = F_{\text{Kval}} - 5$ (intervall $[-5, 0]$)

Kvalitative ordinalnivåer av frekvens (F_{Kval})	Kvantitative frekvensnivåer (F_{Kvan}) (antall hendelser/år)	Fortolkning
Ordinalnivå 5 ($X = 5 - 5 = 0$)	$F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X = 500 \cdot 10^0 = 500$	Omtrent hver dag
Ordinalnivå 4 ($X = 4 - 5 = -1$)	$F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X = 500 \cdot 10^{-1} = 50$	Omtrent hver uke
Ordinalnivå 3 ($X = 3 - 5 = -2$)	$F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X = 500 \cdot 10^{-2} = 5$	1 gang per 2 måneder
Ordinalnivå 2 ($X = 2 - 5 = -3$)	$F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X = 500 \cdot 10^{-3} = 0,5$	1 gang per 2 år
Ordinalnivå 1 ($X = 1 - 5 = -4$)	$F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X = 500 \cdot 10^{-4} = 0,05$	En gang per 20 år
Ordinalnivå 0 ($X = 0 - 5 = -5$)	$F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^X = 500 \cdot 10^{-5} = 0,005$	En gang per 200 år

Kalibrering av kvantitativ konsekvens

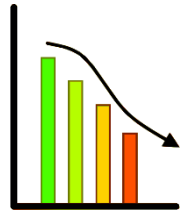


- Den kvantitative konsekvensskalaen er logaritmisk.
- K_{Max} er kalibreringsfaktoren for antatt maksimalt tap, tilsvarende verst konsekvens (nivå 5)
- Lavere konsekvenser bestemmes deretter etter logaritmisk skala.
- K_{Kval} er ordinal kvalitativ konsekvens (intervall [0, 5])
- Sett f.eks. $K_{Max}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

Kvalitative ordinalnivåer av konsekvens (K_{Kval})	Kvantitative konsekvensnivåer (K_{Kvan}) (tap/hendelse)	Fortolkning
Ordinalnivå 5 ($Y = 5 - 5 = 0$)	$K_{Kvan} = K_{Max} \cdot 10^Y = 10^7 \cdot 10^0 = 10^7$	$K_{Kvan} = \$10 \text{ millioner}$
Ordinalnivå 4 ($Y = 4 - 5 = -1$)	$K_{Kvan} = K_{Max} \cdot 10^Y = 10^7 \cdot 10^{-1} = 10^6$	$K_{Kvan} = \$1 \text{ million}$
Ordinalnivå 3 ($Y = 3 - 5 = -2$)	$K_{Kvan} = K_{Max} \cdot 10^Y = 10^7 \cdot 10^{-2} = 10^5$	$K_{Kvan} = \$100 \text{ 000}$
Ordinalnivå 2 ($Y = 2 - 5 = -3$)	$K_{Kvan} = K_{Max} \cdot 10^Y = 10^7 \cdot 10^{-3} = 10^4$	$K_{Kvan} = \$10 \text{ 000}$
Ordinalnivå 1 ($Y = 1 - 5 = -4$)	$K_{Kvan} = K_{Max} \cdot 10^Y = 10^7 \cdot 10^{-4} = 10^3$	$K_{Kvan} = \$1000$
Ordinalnivå 0 ($Y = 0 - 5 = -5$)	$K_{Kvan} = K_{Max} \cdot 10^Y = 10^7 \cdot 10^{-5} = 10^2$	$K_{Kvan} = \$100$

- Kvantitativ risiko: $R_{Kvan} = F_{Kvan} \cdot K_{Kvan}$
 $= F_{Max} \cdot 10^X \cdot K_{Max} \cdot 10^Y$, hvor $X = (F_{Kval} - 5)$; og $Y = (K_{Kval} - 5)$
 $= F_{Max} \cdot K_{Max} \cdot 10^Z$, hvor $Z = X + Y = (R_{Kval} - 10)$
hvor F_{Max} = snarest frekvens, K_{Max} = verst konsekvens
- For en gitt risiko, anta at den estimerte konsekvensen K_{Kvan} er konkurs, og den estimerte frekvens F_{Kvan} er en gang i uken. Det betyr selvfølgelig ikke at selskapet går konkurs hver uke.
 - Det viser bare at konsekvensen «konkurs» kan inntreffe allerede etter en uke.
- Dessuten, noen typer hendelser vil bare skje én gang, siden selskapet vil lære av hendelsen og vil innføre tiltak for å etablere en sikrere tilstand.
 - For slike risikoer er det forventede tapet «bare» lik den estimerte konsekvensen K_{Kvan} , der den estimerte frekvens F_{Kvan} indikerer hvor snart tapet forventes å materialisere seg.
- Uansett vil $R_{Kvan} = F_{Kvan} \cdot K_{Kvan}$ uttrykke størrelsen av denne risikoen i forhold til andre risikoer.

Konsekvensestimering med flere aspekter



- En enkelt risiko kan ha flere forskjellige konsekvenser
- For kvalitativ og relativ effektestimering bruker vi vanligvis den høyeste blant de relevante konsekvensene for den spesifikke risikoen
- For kvantitativ estimering kan samlet konsekvens K_{Kvan} uttrykkes som en absolutt pengeverdi
 - Samlet konsekvens for en gitt risiko er summen av konsekvensene for de respektive aspektene.
 - Anta fire konsekvenser av ulike aspekter k_1 , k_2 , k_3 , k_4
Samlet kvantitativ konsekvens er: $K_{Kvan} = k_1 + k_2 + k_3 + k_4$

Eksempel på kvantitativ risikoanalyse \$ € £ ¥

Case: Hacking av nettsted

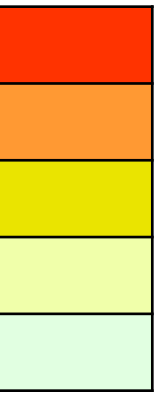
- Risiko: Tilgriset og ødelagt nettsted
- Sannsynlighetsestimat
 - $F_{K_{van}} = 0,5$, det vil si at det sannsynligvis vil skje hvert 2. år
- Konsekvensestimater med flere aspekter
 - Tapte fortjenester fordi nettstedet er nede, $k_1 = \$50\,000$
 - Tapte omdømme $k_2 = \$20\,000$
 - Kostnad for å korrigere nettsiden $k_3 = \$10\,000$
 - $K_1 = k_1 + k_2 + k_3 = \$80\,000$
- Beregning av risiko
 - $R_{K_{van}} = F_{K_{van}} \cdot K_{K_{van}} = 0.5 \times \$80,000 = \$40,000$ i forventet tap per år
- Gir grunnlag for å bruke \$40 000 på sikkerhetstiltak 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 frekvens/sannsynlighet
 - Kalibreringsfaktor for snarest frekvens $F_{\text{Max}} = 500$ ganger per år, dvs. omtrent hver dag.
 - Kvalitativt frekvensestimat $F_{\text{Kval}} = \text{Usannsynlig}$ (ordinalnivå 2)
 - Kvantitativt frekvensestimat $F_{\text{Kvan}} = F_{\text{Max}} \cdot 10^{(2-5)} = F_{\text{Max}} \cdot 10^{-3} = 500 \cdot 0.001 = 0.5$ (hvert 2. år)
- Estimering av konsekvens
 - Kalibreringsfaktor for verst konsekvens $K_{\text{Max}} = \$10 \text{ millioner} = \$10^7$
 - Kvalitativt konsekvensestimat $K_{\text{Kval}} = \text{Stor}$ (ordinalnivå 4)
 - Kvantitativt konsekvensestimat $K_{\text{Kvan}} = K_{\text{Max}} \cdot 10^{(4-5)} = K_{\text{Max}} \cdot 10^{-1} = 10^7 \cdot 0.1 = \$10^6 = \$1 \text{ million}$
- Beregning av risiko
 - $R_{\text{Kvan}} = F_{\text{Kvan}} \cdot K_{\text{Kvan}} = 0.5 \times \$1,000,000 = \$500,000$ forventet tap per år
- Gir grunnlag for å bruke \$500 000 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 estimer av sannsynlighet og konsekvens er logaritmiske
- Logaritmiske nivåer gjør kvalitativ risikoberegning additiv

$$R_{Kval} = F_{Kval} + K_{Kval}$$

- Kvantitativ risikoberegning er multiplikativ

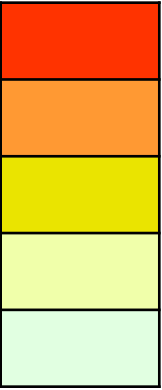
$$R_{Kvan} = F_{Kvan} \cdot K_{Kvan}$$

- UiOs regneark for kvalitativ og kvantitativ cyberrisikovurdering:

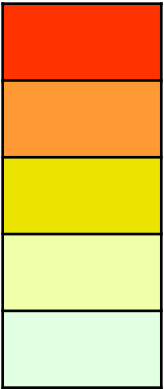
<https://www.mn.uio.no/ifi/forskning/grupper/sec/laeringsressurser/uio-risikovurdering.xlsx>

Forklaring av regneark

- Trussel: Trusselscenario og eventuelt trusselaktør
- Sårbarhet: Hvilke svakheter og feil som gjør at trusselscenarioet kan gjennomføres
- Berørte digitale eiendeler/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 nye sikkerhetstiltak
 - a) kvalitativ risiko = kvalitativ frekvens + kvalitativ konsekvens
 - b) kvantitativ risiko = kvantitativ frekvens $\times$ kvantitativ konsekvens
 - Forutsetter å fastsette antatt snarest frekvens F_{Max} og verst konsekvens K_{Max}
- Anbefalte nye tiltak
 - Forslag til nye sikkerhetstiltak for å forhindre hendelsen eller mitigere konsekvenser
- Beregning av kvantitativ risikoreduksjon R_{Δ} som følge av nye sikkerhetstiltak
- Beregning av kost/nytte ROSI (Return On Security Investment) ved nye sikkerhetstiltak
 - Basert på kvantitativ risikoreduksjon R_{Δ} og investeringskostnad I_{Tiltak} for nye sikkerhetstiltak.

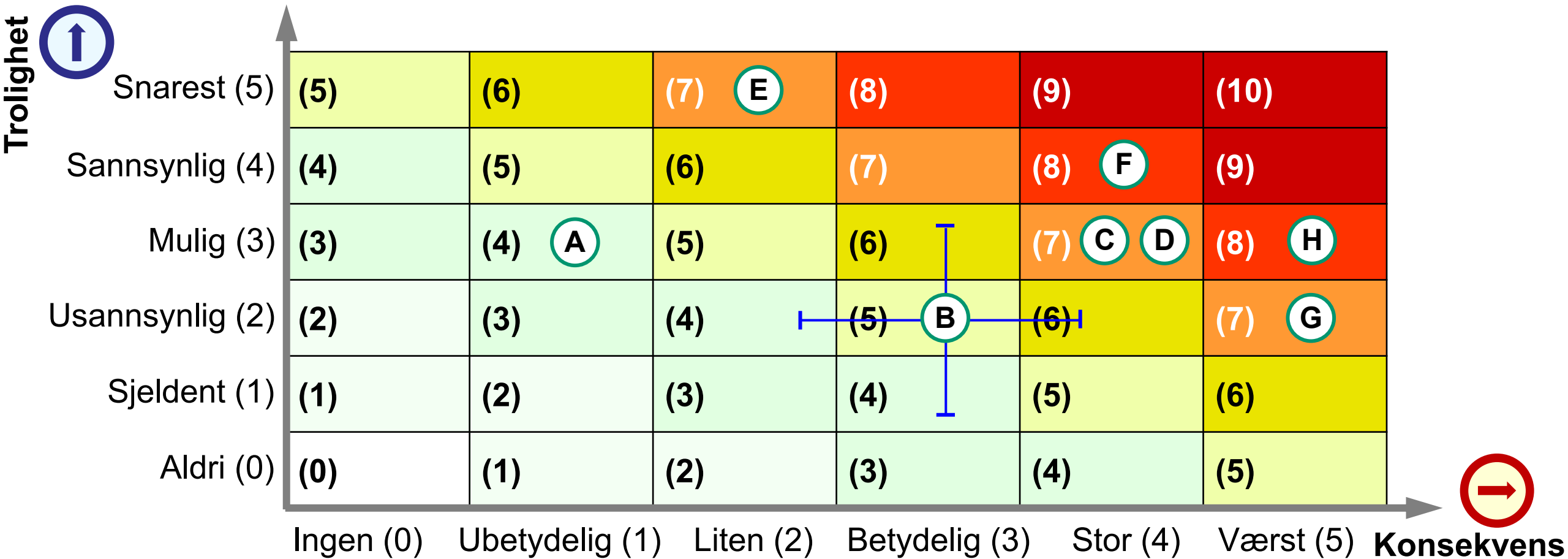


Bruk av regneark



- Top-Down eller Bottom-Up
 - Top-Down (hendelsesbasert) risikovurdering starter med å identifisere trusler, og deretter verdier og sårbarheter
 - Bottom-Up (verdibasert) risikovurdering starter med å identifisere verdier og sårbarheter, og deretter trusler
- Risikoberegning gjøres både før og etter nye sikkerhetstiltak
- Beregnet kvantitativ risiko tolkes som forventet tap per år
 - Hvis frekvensen F_{Kvan} er høy (mange ganger per år) kan den kvantitative risikoen være større en verste konsekvens, som virker kontraintuitivt fordi den verste konsekvens (f.eks. konkurs) kanskje bare kan skje én eneste gang. Risikoen må da tolkes slik at konsekvensen vil inntreffe snart (proporsjonalt med F_{Kvan}), dvs. snarere enn en gang per år.
- Kost/Nytte (ROSI: Return On Investment) kan være positiv eller negativ.
 - Tiltak bør velges hvis $ROSI > 0$, tiltak bør ikke velges hvis $ROSI < 0$.

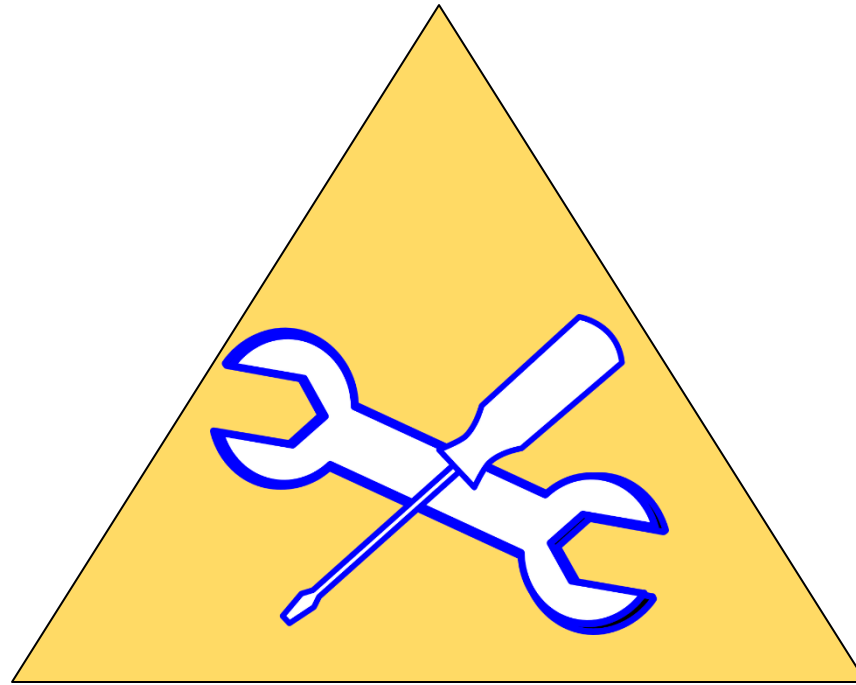
Visualisering av risikoer



Kriterier for risikoaksept (ISO/IEC 27005 6.4.2)

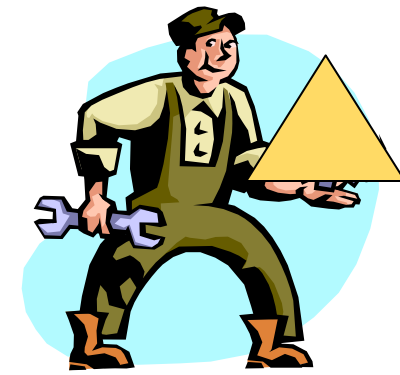
Ved risikohåndtering kan kriterier for risikoaksept brukes for å avgjøre om den foreslåtte risikohåndteringen er tilstrekkelig for å oppnå et akseptabelt risikonivå.

- Kriterier for risikoaksept kan baseres på risikonivå alene eller kan også ta hensyn til kost/nytte-balansen mellom potensielle tap og kostnaden ved sikkerhetstiltak.
- En annen mulighet er at aksept av en sjelden hendelse som utsletter et selskaps aksjeverdi, eller en kontinuerlig tapping av ressurser for å håndtere hyppige mindre overtredelser av en policy, vurderes etter hvilke av de to faktorene som har størst virkning på organisasjonen.



Del d: Risikohåndtering

Håndtering av risiko



- Sorter de identifiserte og vurderte risikoene etter nivå/alvorlighet.
- For hver uakseptable risiko, velg en av fire måter å håndtere risikoen.
 1. Reduser risikoen ved å implementere sikkerhetstiltak. Kan velges fra tiltaksbanker som ISO/IEC 27002, NIST CSF, CIS Controls, NSMs Grunnprinsipper, eller andre kilder.
 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)

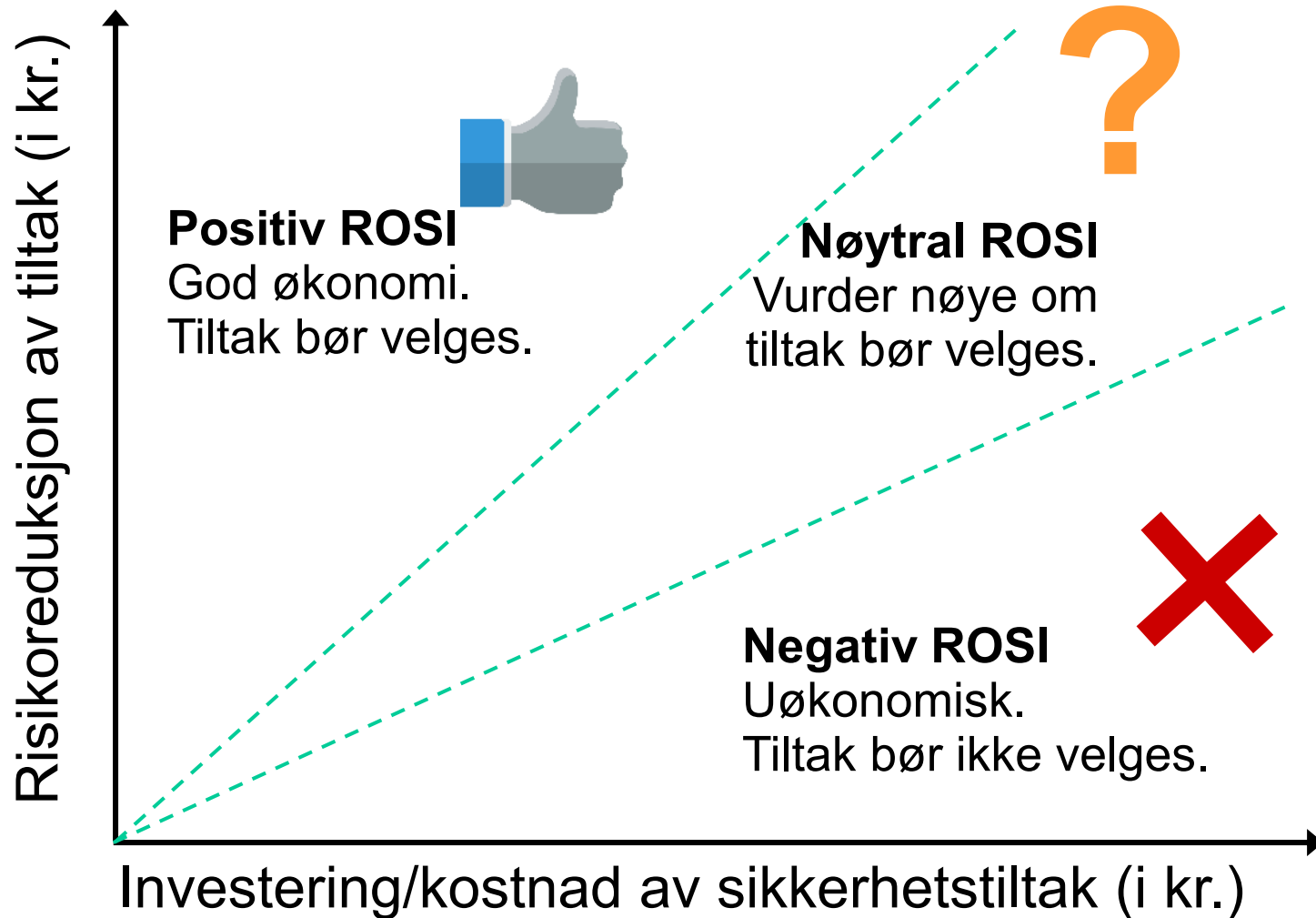
1. Valg av sikkerhetstiltak: Vurder de fire P-ene (ITIL)

- ITILs fire P'er tilsvarer omtrent de tradisjonelle "People + Process + Technology" (PPT)-aspektene ved cyberstyring beskrevet for eksempel av NIST CSF, men med "Partner"-aspektet lagt til.



- People:** Personalet må ha nødvendig ferdighetstrening for å drive og administrere cybersikkerhet, som inkluderer en god sikkerhetskultur i organisasjonen.
- Product (Technology):** Organisasjoner må nøye vurdere hvilke produkter/teknologi som på den mest optimale måten kan støtte målet om å redusere risiko til et akseptabelt nivå.
- Partner:** Organisasjoner må engasjere seg med partnere når de kjøper produkter og tjenester fra leverandører. Det kan være bortkastet penger å kjøpe et dyrt sikkerhetsprodukt hvis leverandøren eller andre parter ikke er i stand til å gi tilstrekkelig støtte for drift av produktet.
- Process:** All bruk av teknologi (produkt) består av prosesser, så når en organisasjon anskaffer eller implementerer sikkerhetsteknologi, må de sørge for at det er en tilstrekkelig prosess for å betjene teknologien. Hvis prosessen er ineffektiv eller ineffektiv, har teknologien liten verdi.

Vurdere kost/nytte av tiltak (ROI: Return on Security Investment)



I finans:

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

I cyberrisiko:

$$\text{ROSI} = \frac{\text{Risikoreduksjon} - \text{Investering}}{\text{Investering}}$$

Anvendelseserklæring (SoA: Statement of Applicability)

- ISO/IEC 27005 8.5 sier at anvendelseserklæringen bør inneholde:
 - a) de nødvendige sikkerhetstiltakene;
 - b) begrunnelse for at disse tiltakene er inkludert;
 - c) om de er implementert eller ikke;
 - d) begrunnelse for utelatelse av sikkerhetstiltak fra ISO/IEC 27001:2022, tillegg A.
- Bør dermed inneholde alle sikkerhetstiltakene fra ISO/IEC 27001:2022, tillegg A

A	B	C	D	E	F	G
ISMS STATEMENT OF APPLICABILITY						
Document Reference:						
Version :						
Date:						
#	Control Objective / Control	Control Description	Controls Included	Control Applicable	Control Implemented	Legal Requirements
		Established in accordance with the organization's information security requirements				
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.				
5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents				
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.				
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.				

2. 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.

3. 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.

4. Risikounngåelse



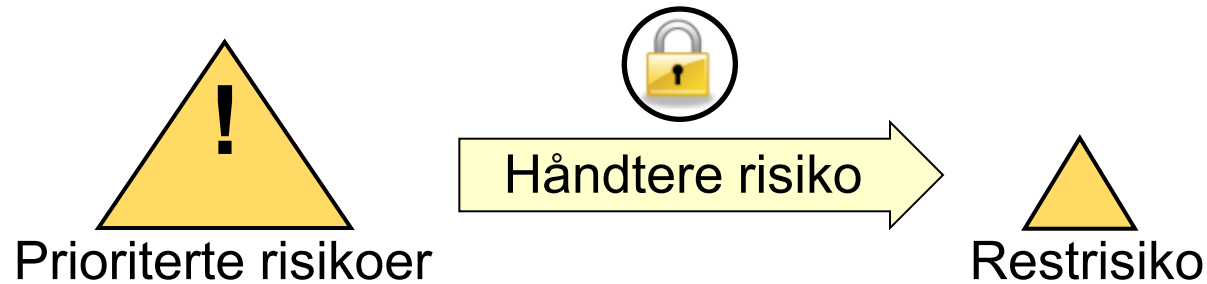
- Enhver forretningsaktivitet medfører en viss risiko, men nytten og fortjeneste oppveier normalt risikoen.
- I tilfelle risikoen er for høy sammenlignet med nytten og fortjenesten, og det ikke er mulig å redusere, mitigere, overføre eller beholde risikoen, er siste utvei å stoppe forretningsaktiviteten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

Risikohåndteringsplan (ISO/IEC 27005 8.6)

- Er en prosjektplan for implementering av organisasjonens nødvendige sikkerhetstiltak.
- Bør godkjennes av risikoeierne så snart planen er utarbeidet. Risikoeiere bør også avgjøre om restrisiko skal aksepteres. Denne beslutningen bør baseres på definerte kriterier for risikoaksept.
- Risikoaksept kan omfatte en prosess for å få godkjennelse av gjennomførte tiltak før det tas en endelig beslutning om risikoaksept.
- Risikokriterier kan tillate at risikoer overskrider en ønsket terskel innenfor et definert omfang hvis det finnes en plan for å redusere risikoen innenfor et akseptabelt tidsrom.

Risikohåndtering og restrisiko

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



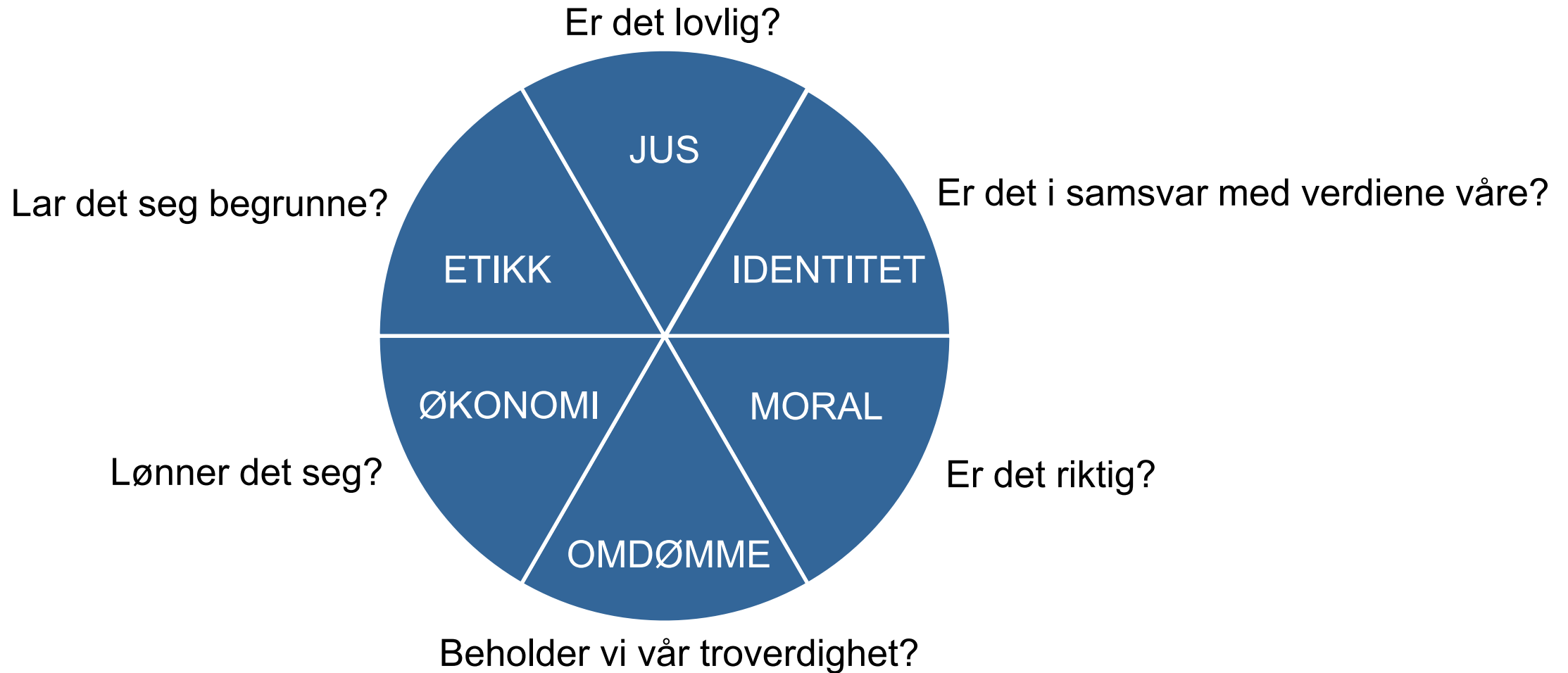
- Restrisiko er den risiko som gjenstår etter håndtering.
- Det er en ledelsesbeslutning å akseptere restrisiko. Den aksepterte restrisiko skal være forsvarlig i henhold til virksomhetens risikostrategi.

Mitigering av restrisiko



- Forsøk på å redusere negative virkningen av sikkerhetshendelser gjennom planlegging og beredskap
- Tilnærminger for mitigering av restrisiko:
 - Plan for hendelseshåndtering (IRP: Incident Response Plan)
 - Plan for katastrofeshåndtering (DRP: Disaster Recovery Plan)
 - Plan for driftskontinuitet (BCP: Business Continuity Plan)

Helhetlig beslutningstaking om risiko

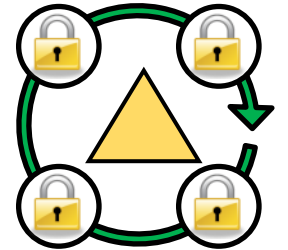


Kilde: Navigasjonshjulet

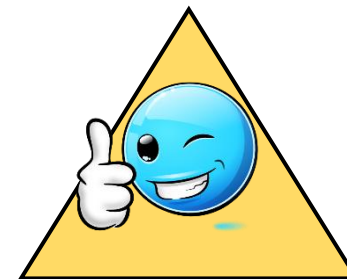
<https://www.bi.no/forskning/business-review/articles/2020/08/slik-kan-ledere-fa-hjelp-til-a-navigere-etisk/>

Overvåking og gjennomgang av risiko (ISO/IEC 27005 10.5)

- Implementering av tiltak for å redusere risiko er ikke slutten på prosessen.
- Håndtering og tilhørende tiltak må driftes og evalueres fortløpende for å bestemme effektiviteten og beregne den estimerte restrisikoen mer nøyaktig
- Prosessen fortsetter så lenge organisasjonen fortsetter å ha forretningsaktiviteter som medfører risiko.
- Risikostyring er en prosess, ikke en endetilstand!



Positiv betrakning på risiko



- Identifiser alternativer for risikobehandling ved å søke alternative forretningsmodeller som kan øke positiv nytte og fortjeneste uten å øke risikoen tilsvarende.
- Alternativene inkluderer:
 - Aktivt søke forretningsmuligheter, selv om det innebærer risiko
 - Øke nytten og fortjenesten uten å øke risikoen tilsvarende
 - Dele forretningsmuligheter og risiko med andre aktører
 - Kjenn restrisikoen, og vær forberedt på å håndtere hendelser
 - Kjenn restrisikoen, og vær forberedt på å begrunne denne hvis det skjer en hendelse

Slutt på presentasjon