Ole Andreas Engen, Professor

Universitetet i Stavanger

Endring i risikoaksept i forhold til usikkerhet de siste 10 årene

Sikringskonferansen 2021

29. oktober 2021

Meld.St 5: Samfunnssikkerhet i en usikker verden

«Ansvarsprinsippet innebærer at den organisasjon som har ansvar for et fagområde i en normalsituasjon også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området. *Ansvarlig instans må ta stilling til hva som er akseptabel risiko*.» (s. 35)

Ny lov om nasjonal sikkerhet 1. januar 2019

- Virksomheter som omfattes av den nye sikkerhetsloven, er forpliktet til å etablere et **forsvarlig sikkerhetsnivå**. Dette oppnås ved først å foreta en risikovurdering, for deretter å gjennomføre tiltak som reduserer risikoen til et forsvarlig nivå. Det kan være tiltak som reduserer risikoen for at uønskede hendelser inntreffer, eller som reduserer skadeomfanget dersom hendelsen inntreffer, eller gjerne en kombinasjon av disse.
- Virksomheten **plikter å etablere et styringssystem for sikkerhet**. Sikkerhetsarbeidet skal være en del av virksomhetens styringssystem, og sikkerhetstilstanden i virksomheten skal kontrolleres regelmessig. Ansvaret for virksomhetens sikkerhetsarbeid tilligger virksomhetens leder.
- Den generelle plikten til å **oppnå et forsvarlig sikkerhetsnivå** er i loven delt opp i beskyttelse av informasjon, informasjonssystemer og objekter og infrastruktur. Plikten til å sikre gjelder i den utstrekning det (litt forenklet sagt) kan skade nasjonale sikkerhetsinteresser dersom for eksempel uvedkommende får kjennskap til sensitiv informasjon, får tilgang til et IKT-system eller klarer å sette infrastruktur ut av spill. Kravene konkretiseres i forskrift om virksomhetssikkerhet.
- Virksomheten må **kunne dokumentere både risikovurderingen og sikkerhetstiltakene**. Virksomheten må dessuten varsle myndighetene dersom den er rammet av eller står i fare for å bli rammet av sikkerhetstruende virksomhet, eller hvis det har skjedd alvorlige sikkerhetsbrudd.

Risikoaksept og usikkerhet

4 fundamentale spørsmål:

1) Hva betyr dette i en risikostyrings sammenheng?
2) Hva betyr dette for risikoregulering?
3) Hvilke modeller er alternativer for håndtering av risikoaksept?
4) Hva betyr dette for håndtering av usikkerhet?

Drøftes utfra en risiko, - sikkerhet - og samfunnsfaglig perspektiv. *Ikke teknisk.*

Ansvarsprinsippet

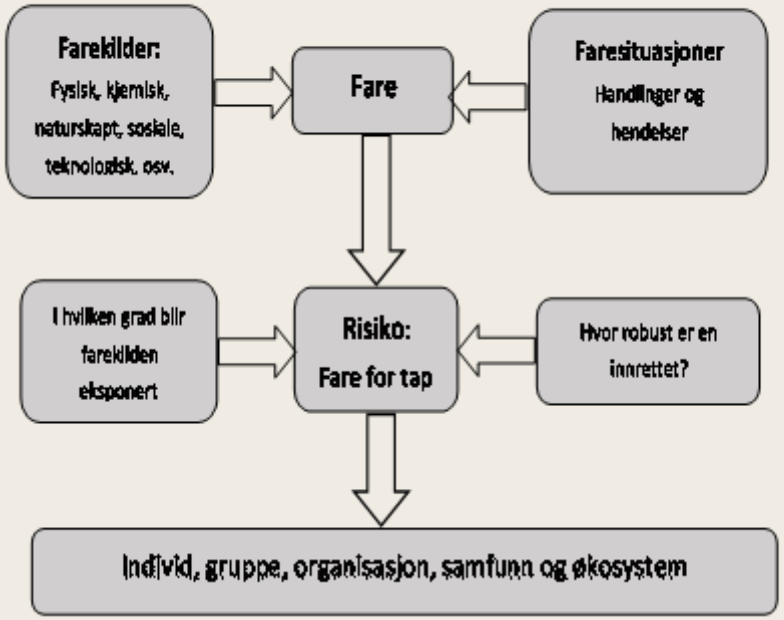
Likhetsprinsippet

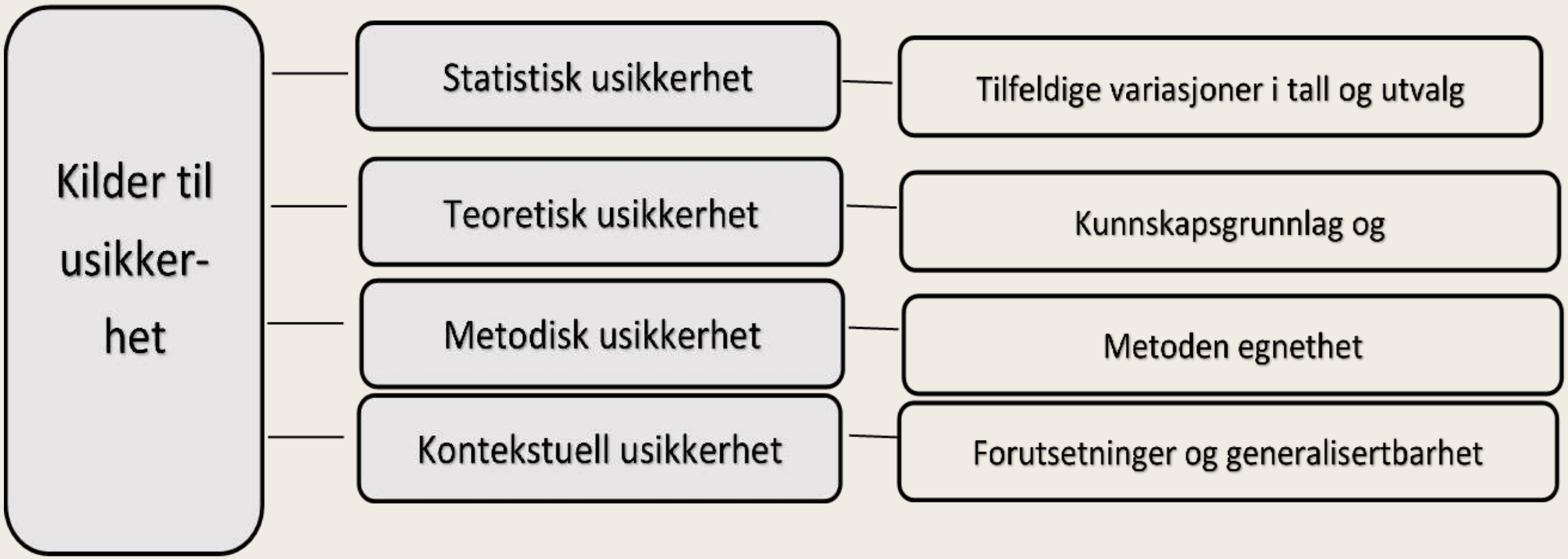
Nærhetsprinsippet

Samvirkeprinsippet

Risiko og Sikkerhet

- Farekilder og faresituasjoner
- Den risiko en kan beregne vil avhenge av hvordan farekilden er eksponert og hvor robust en innrettet seg

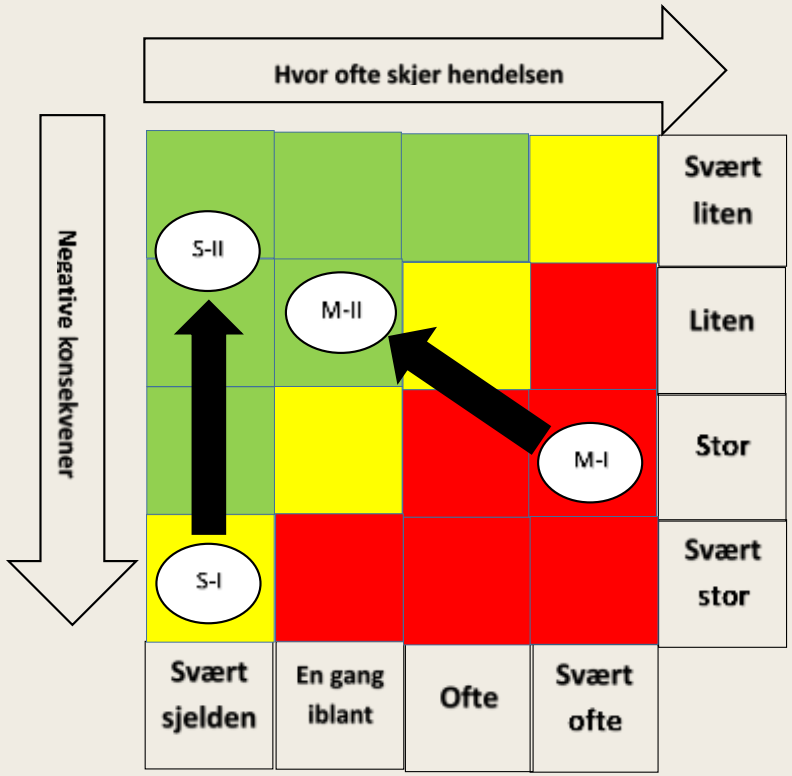


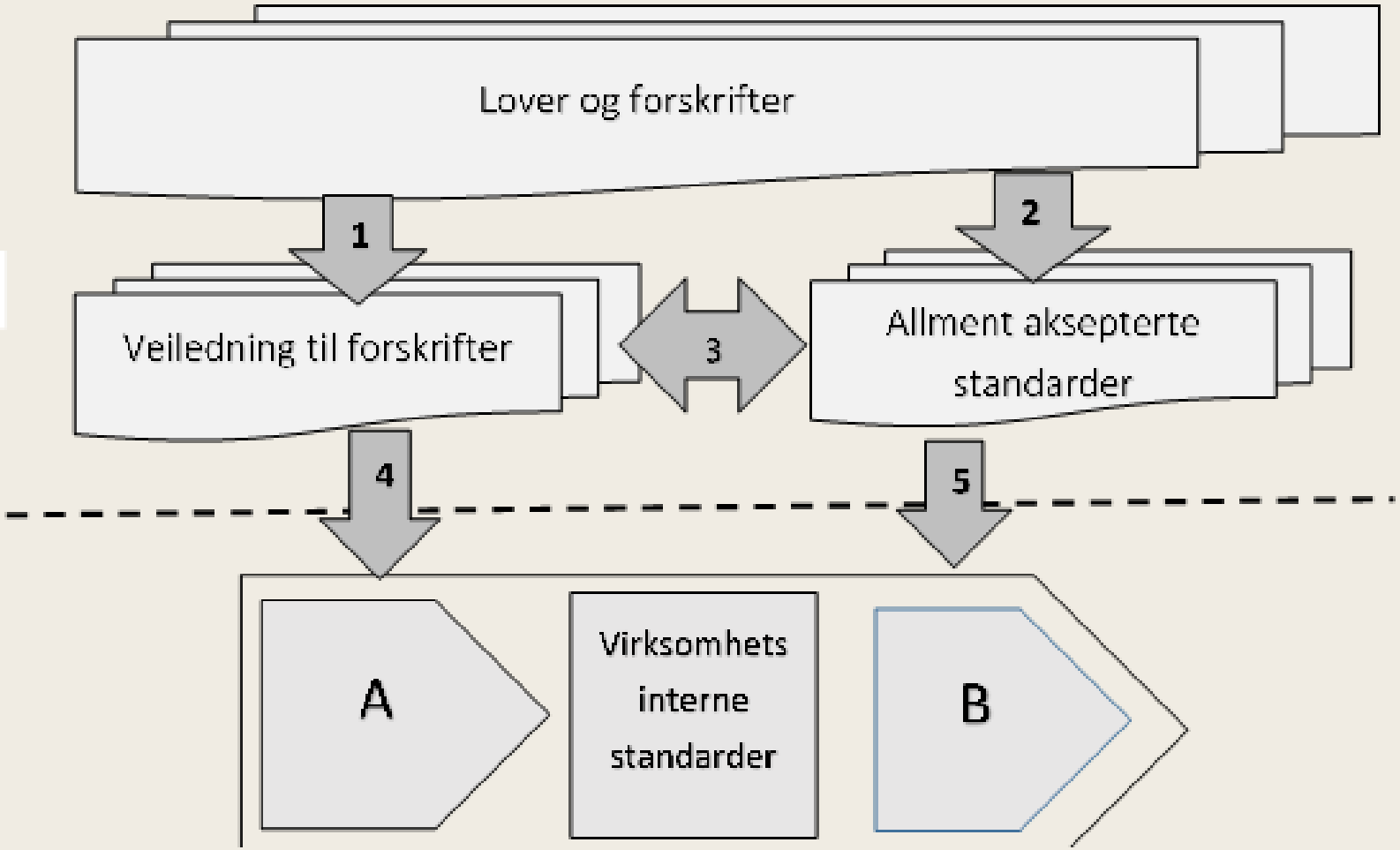

Kilder til usikker-het
Statistisk usikkerhet
Tilfeldige variasjoner i tall og utvalg
Teoretisk usikkerhet
Kunnskapsgrunnlag og
Metodisk usikkerhet
Metoden egnethet
Kontekstuell usikkerhet
Forutsetninger og generalisertbarhet

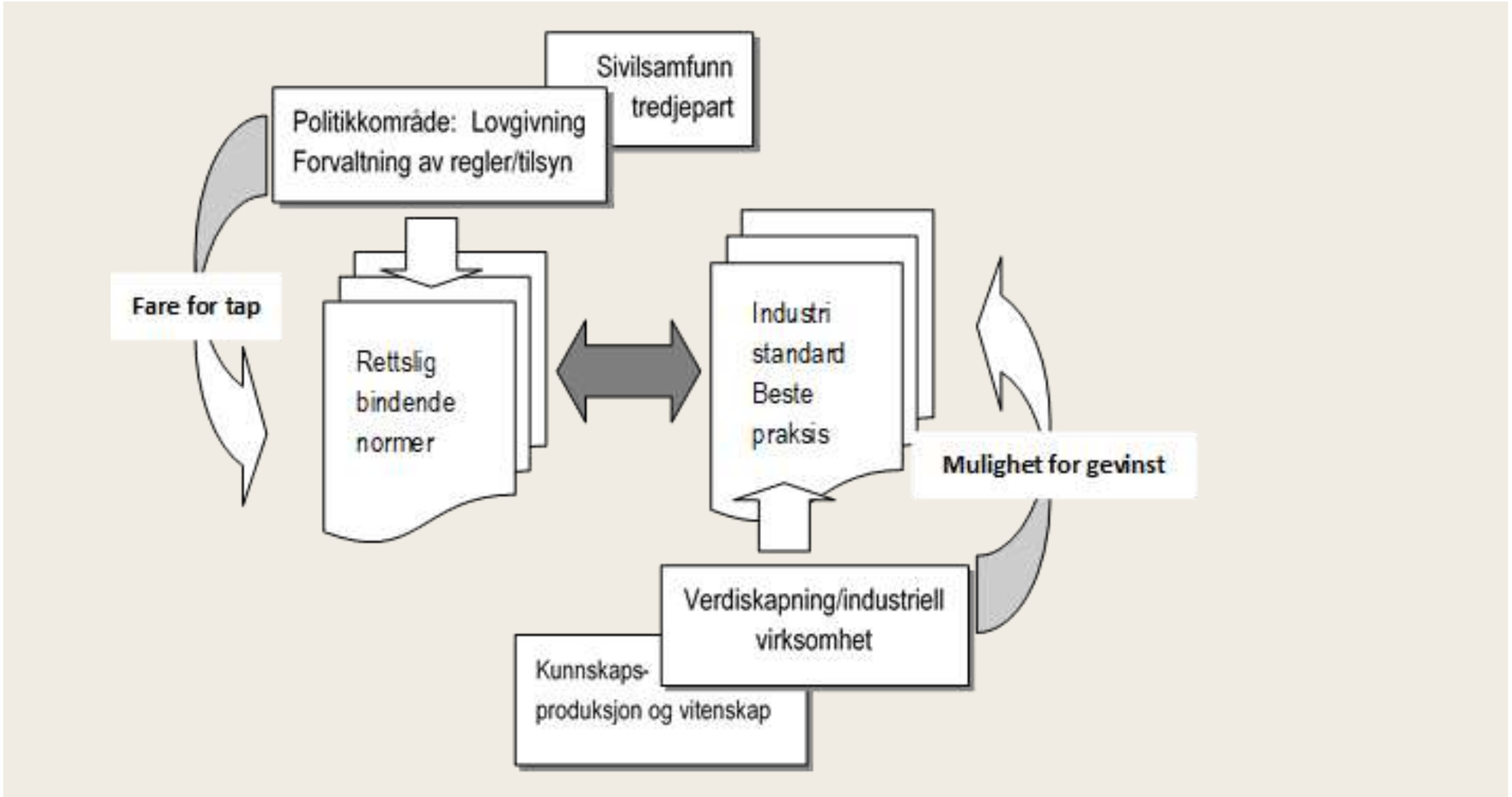
Risikomatrisen

Terje Aven, UiS om 22. juli rapporten:

- «Rapporten på dette området er skuffende lesning. Kommisjonens tanker i forhold til overordnet risikotenkning og samfunnssikkerhet bygger på et tenkesett som ble introdusert på 70-tallet. Det er fullstendig ubrukelig for å møte de trusler og farer vi står overfor i dag. Poenget er at kunnskaps- og usikkerhetsdimensjonen gis altfor liten vekt. En tror risiko kan fanges opp gjennom produktet av sannsynlighet og konsekvens/tap (som i fagspråket omtales som forventet verdi), men en slik tro bygger på en misforståelse, og den er meget alvorlig. Beslutningstakerne (herunder politikerne) villedes, og feil beslutninger tas, SA 2015




Lover og forskrifter
1
2
Veiledning til forskrifter
3
Allment aksepterte standarder
4
5
A
Virksomhets interne standarder
B


Sivilsamfunn
tredjepart
Politikkområde: Lovgivning
Forvaltning av regler/tilsyn
Fare for tap
Rettslig
bindende
normer
Industri
standard
Beste
praksis
Mulighet for gevinst
Verdiskapning/industriell
virksomhet
Kunnskaps-
produksjon og vitenskap

Risikoakseptkriterium:

et kjennetegn, et prinsipp, en regel, test eller en standard for hvordan foreta en vurdering av hva som er akseptabel (godkjent/godtatt) risiko eller beslutte hva som er en akseptabel (godkjent/godtatt) risiko

Kriterier som kan direkte relateres til risikoanalyser og deres resultater

Andre kriterier for risikostyringen (ALARP, design-prinsipper)

Kilde Abrahamsen, E.B., Aven, T., Flage,R., Engen, O.A., Røed,W., Wiencke, H.S., (2020) Petroleumstilsynet. Bruk av risikoakseptkriterier. En evaluering. Proactima

Et funksjonsbasert regelverk

Generelt har funksjonstenkning en sterk begrunnelse, med basis i internkontrollprinsippet og anerkjente prinsipper for regelverksutforming og risikostyring.

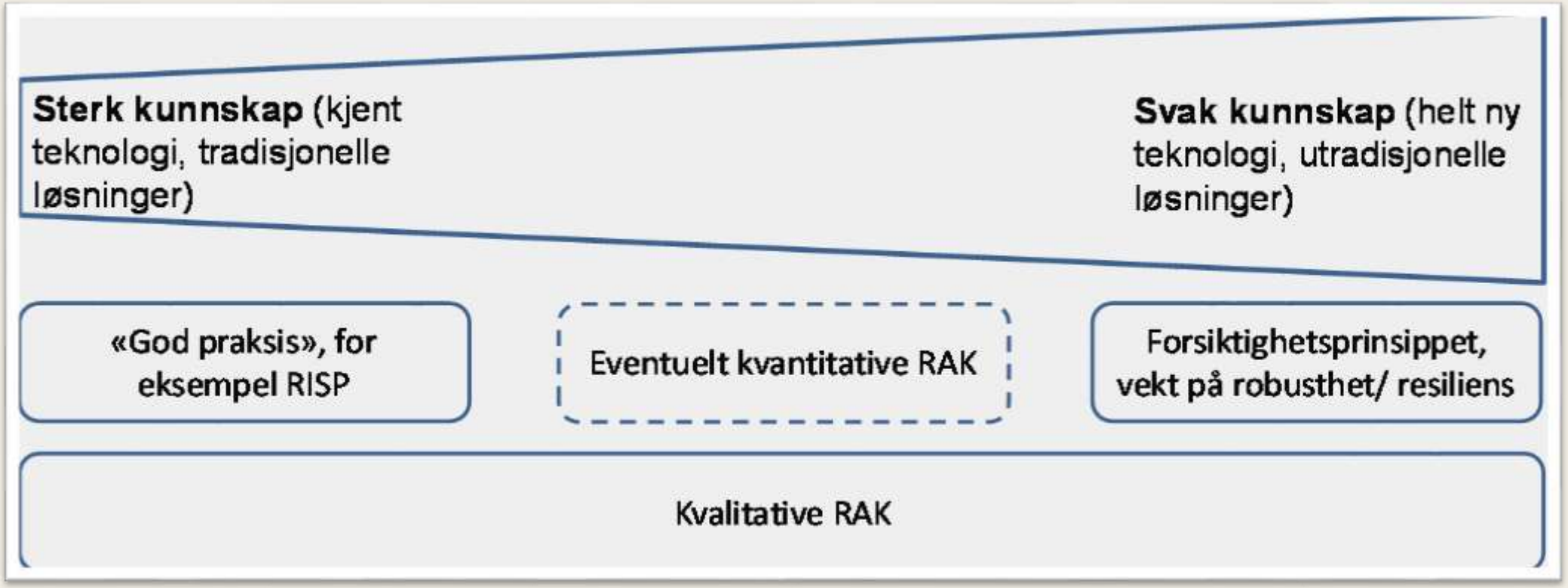
Kilde Abrahamsen, E.B., Aven, T., Flage,R., Engen, O.A., Røed,W., Wiencke, H.S., (2020) Petroleumstilsynet. Bruk av risikoakseptkriterier. En evaluering. Proactima

Ulike modeller for håndtering av risikoaksept

	Funksjonsbasert regime	«Mellomløsninger»	Dagens regime med forbedringer
Myndighetene	Definerer ikke RAK	Definerer noen RAK	Definerer noen RAK og stiller krav til at selskapene skal definere RAK
Selskapene	Kan velge å definere RAK på eget initiativ	RAK bestemt av myndighetene (samt eventuelle egne RAK)	RAK bestemt av myndighetene og selskapet selv

Kilde Abrahamsen, E.B., Aven, T., Flage,R., Engen, O.A., Røed,W., Wiencke, H.S., (2020) Petroleumstilsynet. Bruk av risikoakseptkriterier. En evaluering. Proactima

Illustrasjon av hvordan ulike former for kriterier og styringsprinsipper er knyttet til usikkerhet/ kunnskap



Kilde Abrahamsen, E.B., Aven, T., Flage,R., Engen, O.A., Røed,W., Wiencke, H.S., (2020) Petroleumstilsynet. Bruk av risikoakseptkriterier. En evaluering. Proactima

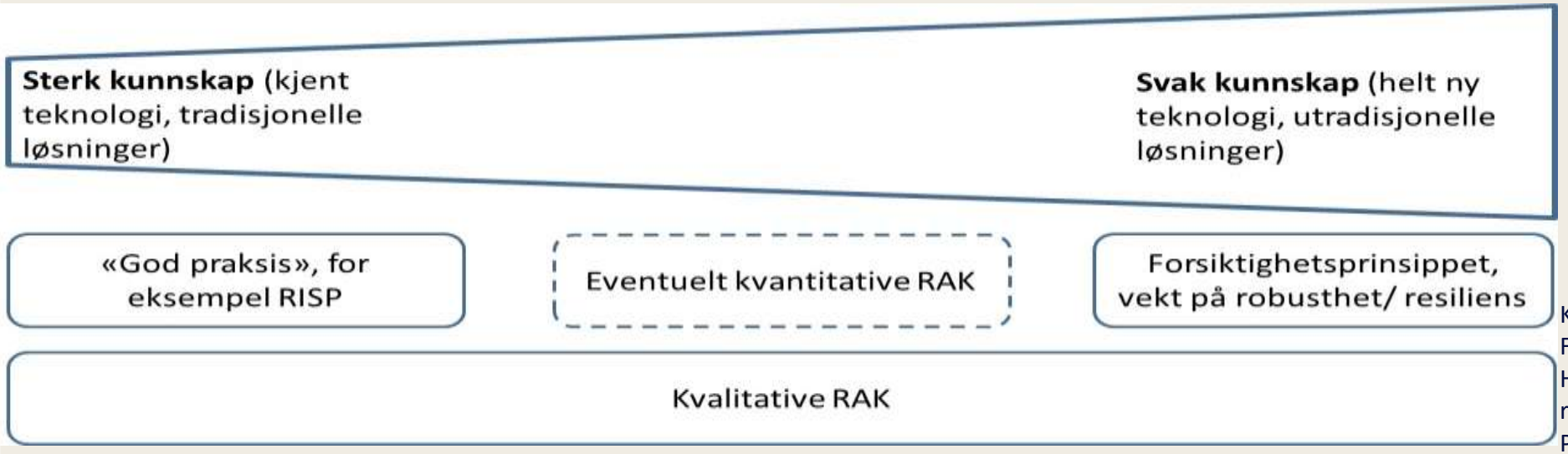
Hva betyr utviklingstrekkene i industrien/samfunnet for bruk av akseptkriterier ?

Utviklingstrekk

- Store teknologiske og organisatoriske endringer gjennom digitalisering
- Lange digitale verdikjeder der «alle systemer» er koblet sammen gjennom felles infrastruktur
- Integrasjon av kontroll systemer og IT
- Komplekst stakeholder bilde
- Autonome løsninger: stordata, maskinlæring, algoritmer

Utfordringer

- Store endringer gir mindre erfaringsbase og svakere kunnskap
- Økt system kompleksitet gir uklare systemgrenser for analysene
- Store endringer i trusselbildet: cyber security, supply chain attack, etc.
- Usikkerhet i samfunn og omgivelser: COVID19, klimaendringer, "digital pandemi ?",…….)
- Hvordan designe og etablere ytelseskrav for komplekse autonome systemer (ytelseskrav til lærende systemer)



Kilde: Abrahamsen, E.B., Aven, T., Flage,R., Engen, O.A., Røed,W., Wiencke, H.S., (2020) Petroleumstilsynet. Bruk av risikoakseptkriterier. En evaluering. Proactima

Risikoaksept – presisering av ansvarsprinsippet

- Meld. St 5 og sikkerhetsloven foreskriver endringer i beredskapen **som gir virksomhetene det hele og fulle ansvaret for å vurdere akseptabel risiko**, organisere sin beredskap og avgjøre hvor mye kostnadene med dette skal utgjøre i sine budsjetter.
- Vurdering av akseptabel risiko krever **omfattende kompetanse og ressurser**. For virksomheter som utfører kritiske samfunnsfunksjoner, krever dette romslige interne budsjetter knyttet til risikoanalyse og beredskapsaktiviteter.
- Utfordring er hvordan virksomhetene faktisk skal forholde seg til begrepet «akseptabel risiko» i en verden **hvor terrorisme, hybrid krigføring, spionasje og digitalisering dominerer risiko- og trusselbildet**.
- Trusselvurderinger forutsetter **kompliserte analysemetoder og kompetanse**. Svært mange av de aktuelle virksomhetene som har ansvaret for grunnleggende samfunnskritiske funksjoner, er private virksomheter. **Har de den nødvendige risikokompetansen, har de nødvendige ressurser?**

Litteratur

- Engen, O.A., Gould K.A.P., Kruke, B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E, (2021) *Perspektiver på samfunnssikkerhet*. Cappelen Damm Akademiske.
- Abrahamsen, E.B., Aven, T., Flage, R., Engen, O.A., Røed, W., Wiencke, H.S., (2020) Petroleumstilsynet. Bruk av risikoakseptkriterier. En evaluering. Proactima.
- Njå, O., Sommer, M., Rake E.L., og Braut, G.S., (2020) *Samfunnssikkerhet. Analyse, styring og evaluerin*g. Universitetsforlaget.
- Lindøe, P. (2018) Risiko, tillit og kontroll. Et aktørperspektiv på risikostyring. Gyldendal.
- Abrahamsen, E.B.; Aven, T., (2012) Why risk acceptance criteria need to be defined by the authorities and not the industry? Reliability engineering & system safety

Takk for oppmerksomheten