

2020:01001 - Åpen

Rapport

Metode for vurdering av resiliensnivået i kritisk infrastruktur – veileder

Forfatter(e)

Knut Øien

Jannicke Fiskvik, Anita Øren



SINTEF Digital

Sikkerhet og pålitelighet

2021-11-20

Rapport

Metode for vurdering av resiliensnivået i kritisk infrastruktur – veileder

EMNEORD:
Resiliens
Indikatorer
Metode
Kritisk infrastruktur

VERSJON
1.0

DATO
2021-11-20

FORFATTER(E)
Knut Øien
Jannicke Fiskvik, Anita Øren

OPPDRAGSGIVER(E)
Intern SEP

OPPDRAGSGIVERS REF.
Maria Bartnes

PROSJEKTNR
102022154-03

ANTALL SIDER OG VEDLEGG:
132 (9 vedlegg)

SAMMENDRAG

Formålet med denne veilederen er å beskrive hvordan resiliensnivået, og dermed evnen til å verne seg mot og håndtere forventede og uventede hendelser, kan vurderes og måles i kritiske infrastrukturer i Norge.

Hensikten med resiliensvurderinger er å fremskaffe kunnskap som kan bidra til å opprettholde kritiske samfunnsfunksjoner både når kjente og ukjente/uventede hendelser inntreffer, og bidra til god håndtering gitt at hendelsene inntreffer. Dette vil redusere risiko for tap av kritiske samfunnsfunksjoner.

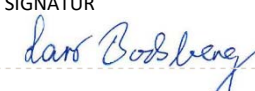
Metoden kan anvendes på ulike områder fra håndtering av ekstreme hendelser for én enkelt kritisk infrastruktur på lokalt nivå, til flere kritiske infrastrukturer innenfor et område eller region, og opp til nasjonalt nivå.

Eksempler inkluderer eksplosjon i kjemisk industri, pandemi i Norge (covid-19), nettangrep og ekstremvær.

UTARBEIDET AV
Knut Øien

SIGNATUR


KONTROLLERT AV
Lars Bodsberg

SIGNATUR


GODKJENT AV
Anita Øren

SIGNATUR


RAPPORTNR
2020:01001

ISBN
978-82-14-07718-6

GRADERING
Åpen

GRADERING DENNE SIDE
Åpen

Historikk

VERSJON	DATO	VERSJONSBEKRIVELSE
0.1	2020-11-21	Første utkast med to eksempler: eksplosjon i kjemisk anlegg og pandemi i Norge (covid-19).
0.2	2021-02-20	Nettangrep lagt til som nytt eksempel.
0.3	2021-03-03	Ekstremvær lagt til som nytt eksempel.
1.0	2021-11-20	Åpen versjon.

Innholdsfortegnelse

1	INNLEDNING.....	5
1.1	Formålet med veilederen.....	5
1.2	Resiliens i kritisk infrastruktur	5
1.3	Nytteverdi	7
1.4	Definisjoner og forkortelser	8
1.5	Oppbygging av veilederen	9
2	METODEBESKRIVELSE.....	10
2.1	Oversikt	10
2.2	Metodetrinn.....	11
	Trinn 1: Velg område.....	11
	Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon).....	11
	Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene	12
	Trinn 4: Vurder hver fase for hver fare/trussel/hendelse	13
	Trinn 5: Velg forhold for hver fase	13
	Trinn 6: Velg indikatorer for hvert forhold	14
	Trinn 7: Fastsett grenseverdiene for hver indikator og angi vektor	16
	Trinn 8: Angi måleverdier for indikatorene (utfør målingen)	18
	Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)	18
	Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.....	18
3	ANVENDELSESOMRÅDER, TILPASNINGER OG BEGRENSNINGER.....	21
4	EKSEMPLER	23
4.1	Ekspløsjon i kjemisk anlegg	23
4.2	Pandemi i Norge (covid-19)	34
4.3	Nettangrep	50
	4.3.1 Inkludere NSMs grunnprinsipper for IKT-sikkerhet.....	50
	4.3.2 Oppfølging av NSMs grunnprinsipper for IKT-sikkerhet.....	54
4.4	Ekstremvær	61
	Referanser	75
	Vedlegg A: Resiliens generelt	81
	Vedlegg B: Resiliens og risiko	84
	Vedlegg C: Kritiske infrastrukturer i Norge	93
	Vedlegg D: Definisjoner og forkortelser	96

Vedlegg E: Generelle karakteristika og bakgrunn for metoden	101
Vedlegg F: Forslag til forhold som påvirker resiliensen i hver fase (trinn 5).....	102
Vedlegg G: Generelle formler for beregning av skårverdier	110
Vedlegg H: Verktøy for beregninger og visualisering av resultater	112
Vedlegg I: Påkrevde analyser og planer	120

1 INNLEDNING

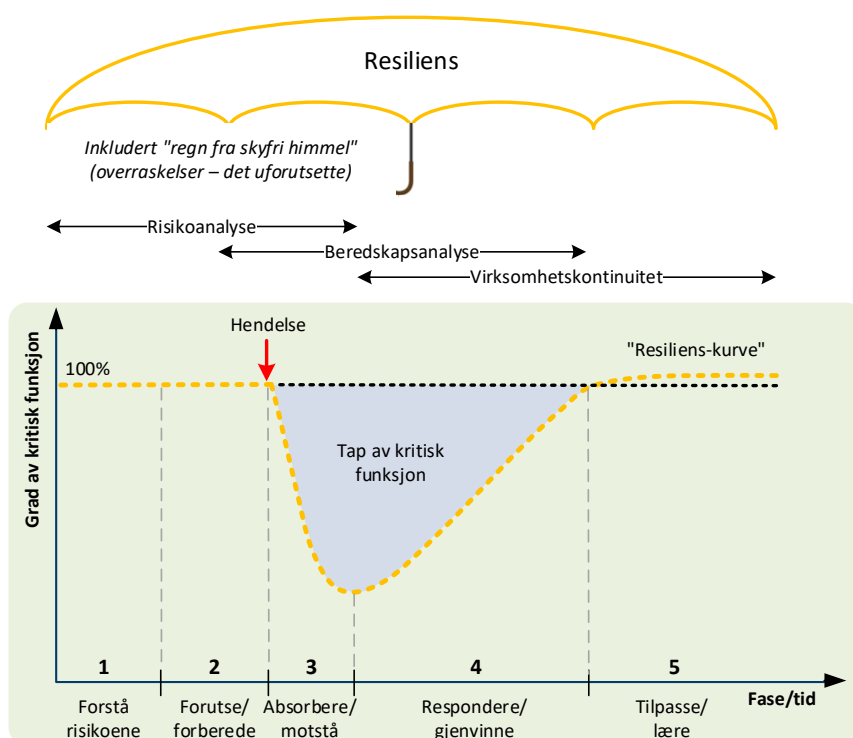
1.1 Formålet med veilederen

Formålet er å beskrive hvordan resiliensnivået, og dermed evnen til å verne seg mot og håndtere forventede og uventede hendelser, kan vurderes og måles i kritiske infrastrukturer i Norge. Metoden som beskrives tar utgangspunkt i resultater fra EU-prosjektet SmartResilience (Øien m.fl., 2018; Øien m.fl., 2019a, b), men er tilpasset norske forhold. Metoden (*Critical Infrastructure Resilience Assessment Method – CIRAM*), og begrepet *resiliens*, skal kunne forstås og anvendes av brukere som ikke har deltatt i utviklingen av metoden. Aktuelle brukere innbefatter infrastruktureiere, beredskapsansvarlige og tilsynsmyndigheter, herunder tilretteleggere for gjennomføring av resiliensvurderinger og beslutningstakere.

1.2 Resiliens i kritisk infrastruktur

Innenfor kritisk infrastruktur har man lenge benyttet begrepet "beskyttelse" (*Critical Infrastructure Protection – CIP*), men etter hvert som systemene har blitt stadig mer komplekse med både ensidige og gjensidige avhengigheter har man innsett at man ikke kan beskytte seg mot alle tenkelige og utenkelige hendelser (HSAC, 2006). Det er også behov for å kunne håndtere de hendelser man ikke klarer å forhindre, og derfor er resiliens i kritisk infrastruktur (*Critical Infrastructure Resilience – CIR*) innført som en naturlig videreføring av CIP (Setola m.fl., 2016).

Resiliens er et begrep som benyttes innenfor en rekke fagområder, hvor forståelsen og definisjonen av resiliens spriker både innad og mellom områdene (se vedlegg A). Her legger vi til grunn en forståelse av resiliens som et paraplybegrep (Setola m.fl., 2016; Tiernan m.fl., 2019) som dekker ulike faser før, under og etter en hendelse, hvor målet er å begrense tapet av kritisk funksjon (kritisk for *samfunnet* – som er årsaken til at infrastrukturen er vurdert som kritisk i utgangspunktet). Dette er illustrert i figur 1.1 (Øien m.fl., 2018).



Figur 1.1 Resiliens som et paraply-begrep (basert på Øien m.fl., 2018)

Resiliens i kritisk infrastruktur dekker et bredt tidsperspektiv som favner det som typisk dekkes av risikoanalyse, beredskapsanalyse og virksomhetskontinuitet (angitt omtrentlig under paraplyen i figur 1.1) og vi har delt dette inn i fem faser¹: (1) forstå risikoene, (2) forutse/forberede, (3) absorbere/motstå, (4) respondere/gjenvinne, og (5) tilpasse/lære. De to første fasene er før en hendelse inntreffer, og den siste er etter at funksjonen er gjenvunnet, som illustrert av den stiplede funksjonskurven ("resiliens-kurven").

Figuren illustrerer også at resiliens dekker uforutsette hendelser, gjennom metaforen "regn fra skyfri himmel", noe som skiller resiliensvurderinger fra risikoanalyser, som er avgrenset til forutsette hendelser.²

Den stiplede kurven ("kritisk funksjonskurve") betegnes ofte som "resilienskurve" (Poulin & Kane, 2021) og er en konseptuell illustrasjon, gitt at en hendelse inntreffer. Den vil kunne anta mange ulike former. Grunnen til at den er stiplet er at selve formen på kurven er uten betydning for den indirekte metoden vi her beskriver for å måle nivået på resiliens, og hvor vi benytter indikatorer for å måle resiliensnivået. Dette er i motsetning til en direkte vurdering/beregning av selve kurven. Resiliensnivået vil da kunne måles uavhengig av hvordan formen på kurven er, og ved gjentakende målinger vil vi se hvordan resiliensnivået endres over tid enten hendelser har inntruffet eller ikke.

Kritisk infrastruktur

Kritisk infrastruktur i Norge er definert av DSB (2016) og er nært knyttet til kritiske samfunnsfunksjoner. Disse forbeholdes funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at dette truer befolkningens sikkerhet og/eller trygghet. Hva som er kritisk infrastruktur, er nærmere beskrevet i vedlegg C. I tillegg skal "skjermingsverdige informasjonssystemer, objekter og infrastrukturer" med betydning for grunnleggende nasjonale funksjoner identifiseres i henhold til sikkerhetsloven (2019).

Det er imidlertid ikke noen forutsetning at en infrastruktur skal være kritisk, viktig eller skjermingsverdig for å benytte metoden beskrevet i denne veilederen.

Ekstreme hendelser

Metoden kan som nevnt innledningsvis benyttes for å måle evnen til å verne seg mot og håndtere forventede og uforutsette hendelser/utvikling.³ Dette kan være både utilsiktede hendelser (naturhendelser som ekstremvær) og tilsiktede hendelser (eksempelvis terrorangrep og cyberangrep/nettangrep), som illustrert i figur 1.2.

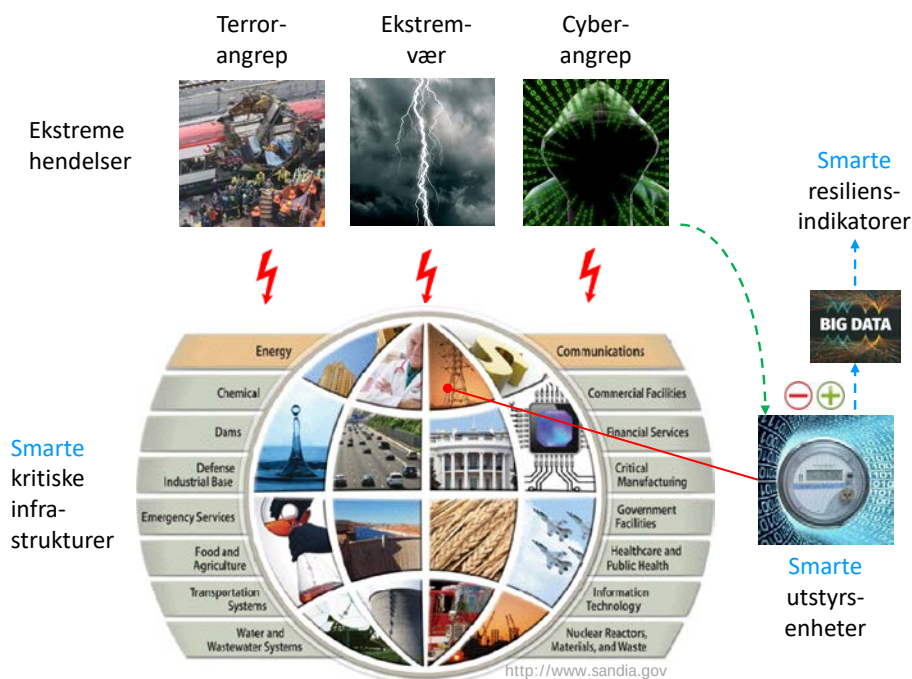
Figuren viser også bakgrunnen for navnet på EU-prosjektet SmartResilience. Økt bruk av smarte enheter som smartmålere gjør kritisk infrastruktur (her illustrert med de infrastrukturene som er definert som kritiske i USA) i økende grad smart. Dette muliggjør hacking/nettangrep, men gir også mye data (big data), som kan brukes til indikatorer – smarte (resiliens-) indikatorer.

Resiliensvurderingen tar kun for seg én eller et fåtall ekstreme hendelser/scenarioer, typisk den eller de hendelsene man er mest bekymret for. Det vurderes da om man har god (nok) evne til å verne seg mot og håndtere denne/disse. Man vil ha behov for ulike typer av beskyttelse avhengig av om hendelsen er en naturhendelse som ekstremvær/flom, et terrorangrep eller et nettangrep, eksempelvis demning, mur/gjerde eller brannmur i datanettverk. Samtidig vil det være mange forhold (tiltak, ressurser, osv.) som anvendes for alle hendelser, eksempelvis planverk, kommunikasjonssystemer, og systemer for læring etter hendelser.

¹ Andre metoder har tilsvarende faseinndelinger, men antallet faser kan variere – typisk mellom tre og syv faser.

² Forholdet mellom resiliens og risiko er utdypet i vedlegg B.

³ En totalt uforutsett hendelse er det naturlig nok ikke mulig å vurdere på forhånd, men visse resilienssegenskaper (fleksibilitet, improvisasjon, tilpasning, osv.) vil kunne bidra i håndteringen av en uventet utvikling av en hendelse.



Figur 1.2 Illustrasjon av ekstreme hendelser (og betegnelsen "smart")

Dersom man vurderer mer enn én hendelse, så kan disse sammenliknes for å se hvilke hendelser man er mest/minst resilient for og man kan også sammenstille disse for å få en aggregert verdi for resiliensnivået. Resiliensnivået vil imidlertid alltid være betinget på de hendelsene man har inkludert i vurderingen.

Gjennom å være resilient mot ekstreme hendelser som man er mest bekymret for, uansett hvilke hendelser dette er, så er det en underliggende antakelse at man også vil være bedre rustet (mer resilient) mot andre hendelser, inkludert ukjente og uforutsette hendelser, fordi mange av de samme forholdene (tiltak, ressurser, osv.) vil inngå. God håndtering av disse felles forholdene vil også være viktig for håndteringen av ukjente og uforutsette hendelser. Resiliensvurderingen av ekstreme kjente hendelser vil derfor i stor grad være relevant også for ukjente hendelser. Eksakt hvor resilient man er mot en ukjent hendelse er imidlertid umulig å si på forhånd.

Et naturlig utgangspunkt for identifisering av ekstreme hendelser i Norge er de fire offentlige trussel- og risikovurderingene som utgis av DSB (2019), Nasjonal sikkerhetsmyndighet (NSM, 2020a), Politiets sikkerhetstjeneste (PST, 2020) og Etterretningstjenesten (E-tjenesten, 2020). De tre sistnevnte i årlige rapporter, mens DSB utgir sin rapport med noen års mellomrom (sist i 2019).

Når det gjelder forhold (tiltak, ressurser, osv.) som er viktig for å være resilient mot ekstreme hendelser, så kan det for nettangrep være aktuelt å inkludere NSMs grunnprinsipper for IKT-sikkerhet (NSM, 2020b). Mer overordnede prinsipper og tiltak kan man finne i Nasjonal strategi for digital sikkerhet (Departementene, 2019). Generelt, og sektorspesifikt, er det en rekke dokumenter som kan være relevante, både i forhold til analyser og planer som er påkrevd, og også mer spesifikke tiltak. Dette er videre beskrevet i kapittel 3.

1.3 Nytteverdi

Hensikten med resiliensvurderinger er å fremskaffe kunnskap som kan bidra til å opprettholde kritiske samfunnsfunksjoner både når kjente og når ukjente/uventede hendelser inntreffer, og bidra til god håndtering gitt at hendelsene inntreffer. Dette vil redusere risiko for tap av kritiske samfunnsfunksjoner.

Vurdering av resiliensnivået (RIL)⁴ gir innsikt i status og forbedringsbehov (og -muligheter) på ulike nivå – fra lokalt til nasjonalt.

De fleste kritiske infrastrukturer har aldri, og vil trolig aldri, erfare en ekstrem hendelse (terrorangrep, nettangrep, ekstremvær, osv.)⁵, men allikevel er det mulig og nødvendig å vurdere resiliensen skulle en ekstrem hendelse inntreffe. Med andre ord, det å vurdere nivået på å forstå risikoene, forutse og forberede, evnen til å absorbere og motstå, til å respondere og gjenvinne, og evnen til å lære og tilpasse seg. Med et høyt resiliensnivå (høy RIL), er det mindre trolig å erfare skadelige konsekvenser som følge av en ekstrem hendelse, og skulle den inntreffe så vil forstyrrelsene/avbruddene trolig være mindre omfattende.

Normalt vil en risikovurdering (risikoanalyse, ROS-analyse, osv.) være langt mer detaljert enn en resiliensvurdering, spesielt i analysen av fysiske systemer og utstyr, men også i omfanget av type hendelser som inngår. Motsatt så går en resiliensvurdering lengre enn tradisjonelle risikovurderinger (og tilgrensede analyser som beredskapsanalyser og analyser av virksomhetskontinuitet) blant annet gjennom vektlegging av både kjente og ukjente farer/trusler/hendelser, årvåkenhet, og læring og tilpasning etter hendelser. Den kan også dekke forhold ut over rene tekniske forhold, gjennom ulike dimensjoner (samfunnsmessige, politiske, osv.).

Man tar typisk utgangspunkt i ekstreme hendelser, som i en risikoanalyse ofte blir neglisjert på grunn av lav sannsynlighet, slik at vurderingen blir en form for "stress-test" av virksomhetens evne til å opprettholde kritisk funksjon og håndtere hendelsene.

En resiliensvurdering av kritisk infrastruktur er mer utadrettet ved at det er de indirekte konsekvensene for samfunnet – ved tap av samfunnskritiske funksjoner – som er hovedfokuset, ikke de direkte konsekvensene for virksomheten, selv om disse henger sammen. Her er vi først og fremst ute etter "samfunnskontinuitet", ikke en snever virksomhetskontinuitet. Kritisk infrastrukturresiliens bidrar dermed til samfunnsresiliens.

En resiliensvurdering kompletterer risikovurderinger (og tilgrensede analyser) gjennom innhenting av kunnskap ut fra et annet perspektiv; det er ikke en erstatning for risikovurderinger. Risikovurderinger gir også verdifull informasjon til en resiliensvurdering, spesielt i forhold til forståelse av (de kjente) risikoene, dvs. at risikoanalyser/risikovurderinger inngår som et viktig *forhold* i en resiliensvurdering (i fase 1 – forstå risikoene). Resiliensvurderinger utføres derfor ofte på et høyere nivå enn en risikoanalyse/risikovurdering.

Sammenhengen mellom resiliens og risiko er beskrevet i vedlegg B, mens en nærmere gjennomgang av risikovurderinger og andre tilgrensede analyser, og klargjøring av sammenhenger mellom disse og resiliensvurderinger, er beskrevet i kapittel 3. Her utdypes merverdien med resiliensvurderinger sammenliknet med risikovurderinger og andre tilgrensede analyser som ansvarlige for kritiske samfunnsfunksjoner / kritisk infrastruktur ofte er pålagt å gjennomføre gjennom lover og forskrifter.

Resiliensperspektivet oppleves også som et mer positivt perspektiv, i motsetning til risiko som er negativt assosiert (Sachs m.fl., 2019).

1.4 Definisjoner og forkortelser

Det å definere noe har både fordeler og ulemper. Hovedformålet er at man skal ha lik forståelse av et begrep for å unngå at man snakker forbi hverandre. Ulempen er at definisjoner ofte er veldig eksakte og avgrensede,

⁴ RIL – Resilience Level (inspirert av SIL – Safety Integrity Level – for instrumenterte sikkerhetssystemer).

⁵ Dog er det en økende mulighet for dette, spesielt knyttet til cyberangrep og ekstremvær (som følge av klimaendring).

og dermed gir en lite utfyllende forklaring og forståelse av et begrep. Derfor er noen begreper beskrevet mer utfyllende i egne vedlegg, bl.a. resiliens (vedlegg A), risiko (vedlegg B) og kritisk infrastruktur (vedlegg C). Dessuten er det ikke noen fasit på hva som er den riktige definisjonen. I hovedsak velges definisjoner fra anerkjente nasjonale og internasjonale standarder, eventuelt gjøres det tilpasninger til disse. Definisjoner og forkortelser inngår i vedlegg D (i tillegg til de utvalgte begrepene i vedlegg A-C).

Tre nærliggende begreper som brukes ofte i CIRAM er *fare*, *trussel* og *hendelse*. Farer og trusler kan føre til en hendelse, som underforstått er en uønsket hendelse. Vi betrakter farer som utilsiktede handlinger eller forhold, mens trusler er knyttet til tilsiktede handlinger.⁶ Farer og trusler er relevante i fase 1 og 2 før en hendelse inntreffer, og i fase 5 hvor man kan lære av disse i tillegg til hendelsene. Hendelser inntreffer mellom fase 2 og 3, og er særlig relevant i fase 3 og 4 ved at de kan føre til tap av kritisk funksjon.

1.5 Oppbygging av veilederen

Kapittel 2 beskriver metoden trinn for trinn, kapittel 3 tar for seg aktuelle anvendelsesområder, tilpasninger og begrensninger, mens kapittel 4 gir eksempler på bruk av metoden.

I tillegg er det ni vedlegg hvor vedlegg A gir forklaring til begrepet resiliens, vedlegg B beskriver sammenhengen mellom resiliens og risiko, vedlegg C beskriver hva som er kritisk infrastruktur, vedlegg D gir definisjoner og forkortelser, vedlegg E beskriver generelle karakteristika og bakgrunn for metoden, vedlegg F gir forslag til forhold som har betydning for resiliens, vedlegg G gir formler for beregning av skårverdier, vedlegg H beskriver verktøyet for beregning og visualisering av resultater, og vedlegg I gir en oversikt over lov- og forskriftspålagte analyser og planer.

⁶ Dette avviker noe fra definisjonene i NS 5830:2012, men er i overenstemmelse med NS 5814:2021.

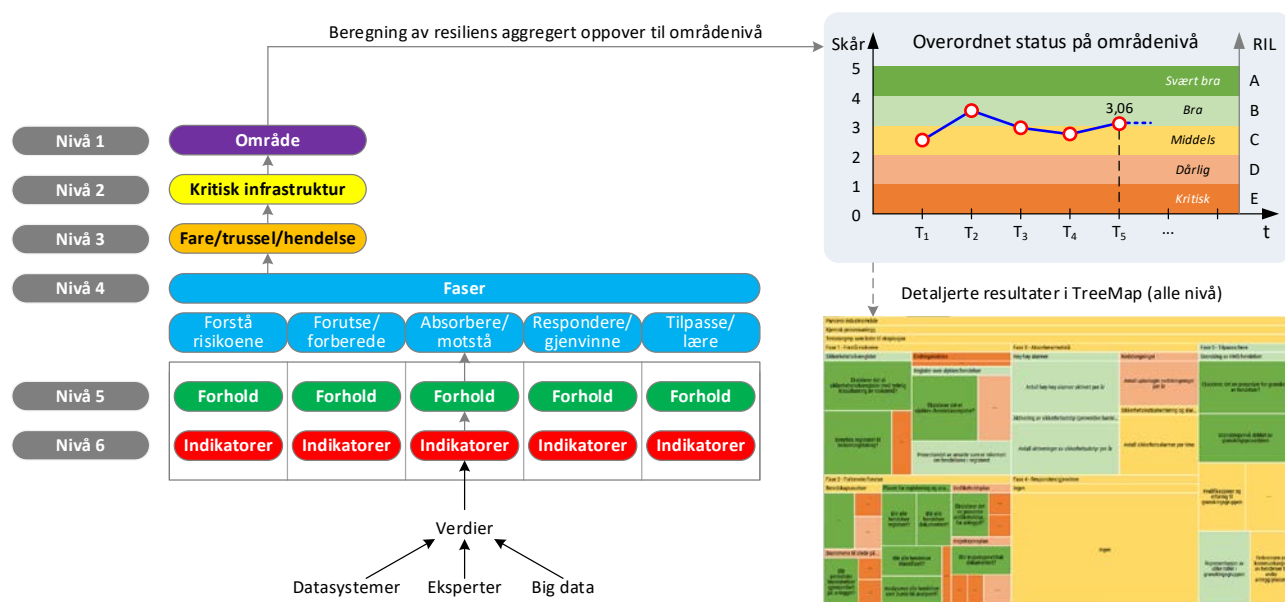
2 METODEBESKRIVELSE

2.1 Oversikt

Kort fortalt så tar metoden (*Critical Infrastructure Resilience Assessment Method – CIRAM*) utgangspunkt i de fem fasene i figur 1.1 og kartlegger og bedømmer hvor godt en kritisk infrastruktur (eller flere kritiske infrastrukturer i et område) vil kunne verne seg mot og håndtere en alvorlig fare, trussel eller hendelse, slik at man kan opprettholde (dvs. begrense tapet av) funksjoner som er kritisk for samfunnet. Dette gjøres ved hjelp av indikatorer som måler forhold som er viktig i hver av de fem fasene.

Omfanget av resiliensvurderingen fastsettes gjennom området som skal dekkes, for eksempel nasjonalt, regionalt (landsdel, fylke, osv.), lokalt (kommune, by, bydel, industriområde, osv.), eller én enkelt kritisk infrastruktur, samt antall og type fare/trussel/hendelse (for eksempel terrorangrep, nettangrep, ekstremvær).

Metoden består dermed av seks nivå i et hierarki, som ovenfra og ned (til venstre) i figur 2.1 er: 1) område, 2) kritisk infrastruktur, 3) fare/trussel/hendelse, 4) faser, 5) forhold, og 6) indikatorer. Indikatorverdien gir en skår på en skala 0-5, hvor 5 er best. Hvert trinn representerer et resiliensnivå (Resilience Level - RIL). Vekting kan angis på alle nivå, og beregninger med bruk av vektet skår aggregeres oppover fra indikatornivå til områdenivå. På alle seks nivåene vil man dermed få både en (vektet) skår (0-5) og det tilsvarende resiliensnivået angitt som en karakter (E=kritisk, D=dårlig, C=middels, B=bra, og A=svært bra).⁷ Dette viser, på alle nivå, hva som er status og hvor det er størst behov for forbedring. Ved bruk over tid får man også en trend på utviklingen (vist for områdenivå opp til høyre i figuren).



Figur 2.1 Oversikt over metoden (CIRAM)

Figur 2.1 viser også at indikatorverdier kan hentes fra ulike datasystemer, eksperter eller fra big data (nederst i figuren), og at detaljerte resultater kan vises grafisk i et såkalt "TreeMap" ("trestruktur-diagram"). I dette diagrammet (vist ned til høyre i figuren) er ikke teksten lesbar, men en større versjon er vist i figur 2.3 i kapittel 2 og figur 4.13 i kapittel 4. Fargene har samme betydning som i grafen over, mens størrelsen på rektanglene angir relativ viktighet/vekt.

⁷ Skår benyttes i beregningene, men gjøres om til et resiliensnivå, bl.a. fordi det er stor usikkerhet i beregningene.

2.2 Metodedrinn

Metoden består av 10 trinn som vist i tabell 2.2. De seks første trinnene er direkte relatert til de seks nivåene vist i figur 2.1. I de tre neste trinnene (7-9) forberedes og utføres målingene og beregningene. Til slutt presenteres resultatene i form av status, trender, osv. (trinn 10).

Tabell 2.2 Metodedrinn

Trinn	Kort beskrivelse	Nivå i modellen
Definer omfanget av vurderingen		
1	Velg område	Nivå 1
2	Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)	Nivå 2
3	Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene	Nivå 3
Etabler forhold og indikatorer for alle faser		
4	Vurder hver fase for hver fare/trussel/hendelse	Nivå 4
5	Velg forhold for hver fase	Nivå 5
6	Velg indikatorer for hvert forhold	Nivå 6
Forbered og utfør målingene og beregningene		
7	Fastsett grenseverdiene for hver indikator og angi vektorer	6
8	Angi måleverdier for indikatorene (utfør målingen)	6
9	Gjennomfør beregningene (skår og resiliensnivå)	1-6
Presenter resultatene		
10	Vis status, trender, styrker og svakheter, forbedringsbehov, osv.	1-6

Trinn 1: Velg område

Velg et definert område. Dette kan være alt fra lokalt til nasjonalt nivå. Typisk kan det være kommune, by, fylke, region, eller hele landet. Dersom man kun ser på én enkelt kritisk infrastruktur, starter man på trinn 2.

Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)

Velg en eller flere kritiske infrastrukturer innenfor det valgte området. Det kan eksempelvis være én enkelt kritisk infrastruktur, som en infrastruktureier har ansvaret for, alle kritiske infrastrukturene i en kommune som kommuneledelsen ønsker å følge opp, eller det kan være helsetjenesten i hele landet under en gitt hendelse (som en pandemi), som Helse- og omsorgsdepartementet eller Helsedirektoratet ønsker en vurdering av. Se ellers kap. 1.2 og vedlegg C med hensyn til identifisering av kritisk infrastruktur.

Det er en nær kopling mellom kritiske samfunnsfunksjoner og kritiske infrastrukturer, og i noen tilfeller kan det være at man ser på en kritisk samfunnsfunksjon, eller delfunksjon, med tilhørende kritiske infrastrukturer (anlegg og systemer), spesielt dersom man vurderer resiliens på nasjonalt nivå.

Et eksempel kan være helsetjenesten (eller helsevesenet), som inngår i den kritiske samfunnsfunksjonen "helse og omsorg" (DSB, 2016), med tilhørende sykehus (kritisk infrastruktur) og deres kapasiteter som intensivsengposter, respiratorkapasitet, testkapasitet, osv. Koronapandemien er et eksempel på en hendelse

på nasjonalt nivå, men som også må håndteres lokalt. Det vil derfor være relevant å vurdere helsevesenets resiliens både nasjonalt og lokalt i et slikt tilfelle.

Et annet eksempel er "vann og avløp" som utgjør en kritisk samfunnsfunksjon og som er avhengig av kritiske infrastrukturer som vannverk, renseanlegg, pumper, høydebasseng, ledninger og rør.

Et tredje eksempel er "forsyning av elektrisk energi", som er en kritisk samfunnsdelfunksjon (del av den kritiske samfunnsfunksjonen "kraftforsyning") og som er avhengig av kritiske infrastrukturer som kraftverk, transformatorer, kraftnett, osv.

I noen tilfeller, spesielt på et nasjonalt nivå, kan det være aktuelt å se på den kritiske samfunnsfunksjonen (eller delfunksjonen) fremfor kun de kritiske infrastrukturene. Det må også klargjøres hvilke kritiske infrastrukturer som skal inngå i vurderingen, dvs. om alle anlegg og systemer skal inngå, eller kun noen av disse.

Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene

Velg én eller flere farer/trusler/hendelser for de valgte kritiske infrastrukturene. Dette kan eksempelvis være terrorangrep, nettangrep eller ekstremvær (som ekstrem nedbør eller storm).

Et naturlig utgangspunkt kan være "analyser av krisescenarioer" (AKS), utarbeidet av DSB (2019a), fordi Meld. St. 10 (2016-2017) peker på at *"DSBs krisescenarioer er et godt utgangspunkt for kommunenes arbeid med risiko- og sårbarhetsanalyser"*. De kan også være et godt utgangspunkt for vurdering av resiliens, selv om det kan være helt andre hendelser som rammer oss, jf. DSB (2019a): *"Faren er stor for at vi kan komme til å oppleve hendelser som overrasker oss fordi vi ikke fullt ut forstår de truslene og farene vi står overfor, eller har oversikt over avhengigheter og mulige følgehendelser"*. *"Mange av de krisene vi har opplevd de siste tiårene har kommet overraskende på de aller fleste. Dette gjelder 11. september-angrepene i USA i 2001, tsunamien som rammet Sør-Asia i 2004, askeskykrisen i 2010 og 22. juli-hendelsene i 2011"*.

DSB (2019a) skiller mellom risikoområder, hendelser og scenarioer. Eksempelvis *ekstremvær og flom* risikoområde), *storm* (hendelse), og *storm i indre Oslofjord* (scenario). Konkrete scenarioer, med angivelse av blant annet tid og sted, er nødvendig for en risikoanalyse (bl.a. for vurdering av sannsynlighet og konsekvens). For vurdering av resiliens med bruk av CIRAM er det tilstrekkelig å angi en hendelse, fordi vi ikke skal analysere sannsynlighet og konsekvens. Dessuten vil sted angis gjennom valg av område og kritiske infrastrukturer (trinn 1 og 2).

Valg av hendelser må tilpasses valg av kritiske infrastrukturer. Mange av hendelsene/scenarioene i AKS er på et nasjonalt nivå, mens andre er på et veldig lokalt nivå. Kun noen av disse er relevante for en bestemt kritisk infrastruktur.

Eksempel på hendelse for helsevesenet er *pandemi*, mens *regnflom* er aktuelt for vann og avløp (og forsyning av elektrisk energi, jf. oversvømmelse av transformatorer), og *langvarig strømrasjonering* er aktuelt for forsyning av elektrisk energi. I tillegg vil tilsiktede hendelser som *digitale angrep* og *terrorangrep* være relevant for alle de nevnte kritiske infrastrukturene/samfunnsfunksjonene.

Man kan velge én eller flere hendelser, gjerne de man er mest bekymret for om man klarer å håndtere. Det er ikke nødvendig å dekke alle relevante hendelser fra AKS. Dersom man håndterer noen, er man også godt rustet til å håndtere andre hendelser. Dette er etter samme tankegang som DSB (2019a): *"Gjennom risiko- og sårbarhetsanalyser, beredskapsplanlegging og øvelser styrker vi våre forutsetninger for å mestre krevende utfordringer, selv om de måtte bli annerledes enn de vi har analysert og øvd på"*.

Andre aktuelle kilder for hendelser/scenarioer er, som nevnt innledningsvis, trussel- og risikovurderingene presentert årlig av NSM, PST og E-tjenesten (NSM, 2020a; PST, 2020; E-tjenesten, 2020).

Dersom man vurderer resiliens knyttet til mer enn én hendelse, så vil disse vurderingene bli vektet i forhold til hverandre.

Trinn 4: Vurder hver fase for hver fare/trussel/hendelse

Hver fare/trussel/hendelse vurderes i hver av de fem fasene vist i figur 1.1. Fasene er beskrevet i tabell 2.3.

Tabell 2.3 Kort beskrivelse av fasene

Fase	Beskrivelse
1	Forstå risikoene
2	Forberede/forutse
3	Absorbere/motstå
4	Respondere/gjenvinne
5	Tilpasse/lære

Det som vurderes i hver av de fem fasene er hvilke forhold som er viktig for å håndtere faren/trusselen/hendelsen (trinn 5) og deretter hvordan disse forholdene kan måles med indikatorer (trinn 6).

Trinn 5: Velg forhold for hver fase

Hvilke forhold er viktig for den kritiske infrastrukturen som vurderes for å verne seg mot og håndtere den aktuelle faren/trusselen/hendelsen? Hva er viktig for å forstå risikoene knyttet til faren/trusselen/hendelsen? Hva er viktig for å være godt forberedt og forutseende med hensyn til den aktuelle faren/trusselen? Hva er viktig for å absorbere og motstå hendelsen? Hva er viktig for rask respons og gjenvinning av kritiske funksjoner etter hendelsen? Hva er viktig for å lære av faren/trusselen/hendelsen og tilpasse seg til håndtering av fremtidige farer, trusler og hendelser?

Den/de som gjennomfører resiliensvurderingen må benytte seg av nødvendig ekspertise med relevant kompetanse og fagkunnskap for å svare på disse spørsmålene, og derigjennom identifisere viktige forhold. Et *forhold* kan være funksjoner, oppgaver, faktorer, evner, egenskaper, ressurser, adferd, osv. som er viktig for å verne seg mot og håndtere farer/trusler/hendelser, dvs. "forhold" er løst definert og favner veldig vidt. Det dekker både hva som må gjøres i de ulike fasene (funksjoner og oppgaver) og hva som kreves (ressurser, evner, egenskaper, osv.). Eksempler på forhold er vist i tabell 2.4.

Tabell 2.4 Eksempler på forhold

Fase	Forhold
1 Forstå risikoene <i>Gjør virksomheten nok for å forstå risikoen?</i>	Kunnskap om avhengigheter Inngående systemkunnskap Informasjon om kvaliteten på sikkerhetsbarrierene
2 Forberede/forutse <i>Forutser virksomheten godt nok hva som kan inntreffe, og forbereder den seg godt nok på trusler og andre uønskede hendelser?</i>	Systemer for tidlig varsling Redundans Budsjett for beredskaps- og responsressurser Trening- og øvelsesplaner
3 Absorbere/motstå <i>Har virksomheten gjennom aktive grep økt sin evne til å stå imot og håndtere kjente og ukjente ekstreme påkjenninger?</i>	Varsling og kommunikasjon Tidlig situasjonsforståelse Beslutningsstøtte Koordinering

Fase		Forhold
4	Respondere/gjenvinne <i>Har virksomheten kapasitet og evne til rask respons og evnen til å komme seg raskt på fote igjen etter ekstremhendelsen?</i>	Beredskapsressurser Organisatorisk robusthet Improvisering/tilpasning Utholdenhet av beredskapsrespons
5	Tilpasse/lære <i>Evner virksomheten å lære i etterkant?</i>	Debriefing av hendelser og respons Gransking og rapportering Kontinuerlig (resiliens-) forbedring

I vedlegg F er det en tabell med forslag (kandidater) til forhold som kan gjennomgås med eksperter. De kan brukes slik de er, de kan tilpasses, eller de kan gi ideer til andre forhold som bør inkluderes dersom de anses som viktige. Forhold kan også avledes fra eventuelt eksisterende indikatorer, ved å stille spørsmål om *"hvorfor bruker vi denne indikatoren – hva er de vi ønsker å måle?"* Det er til syvende og sist alltid den enkelte brukeren som er ansvarlig for å finne et relevant og tilstrekkelig komplett sett av forhold (og indikatorer) for sitt eget tilfelle. Metoden er i høyeste grad medvirkningsbasert.

Det er altså opp til brukeren av metoden å bestemme hvor omfattende vurderingen skal være, men det bør være et minimum av forhold for at vurderingen skal være noenlunde dekkende. Anslagsvis bør det være minst 7-8 forhold i hver fase, altså minimum 35-40 forhold totalt. Relevansen vurderes ut fra om forholdet er viktig for å verne seg mot og håndtere faren/trusselen/hendelsen, uavhengig av om forholdet håndteres godt eller dårlig. Forholdene velges også uavhengig av om man vet eller tror det er vanskelig å måle forholdet. Da blir det fort at man "leter der det er lyst" (kun tar med det som er lett å måle). Først må man konsentrere seg om å få med alt som er viktig. Hvordan man skal måle disse viktige forholdene er neste trinn i metoden (trinn 6).

Hvilken fase man skal plassere et gitt forhold i er ikke alltid åpenbart, men det er ikke veldig kritisk om det plasseres "feil", fordi det kan korrigeres med bruk av vektorer. Forholdene plasseres i den fasen hvor man mener de hører best hjemme. Forholdene bør imidlertid spesifiseres slik at de ikke dekker flere faser. Eksempelvis vil "kommunikasjon" være relevant i flere faser, men det vil være svært ulike former for kommunikasjon. Dette kan derfor spesifiseres som for eksempel *"kommunikasjon om tidligere farer/trusler/hendelser"* i fase 1 (kunnskapsdeling) og *"kommunikasjon med eksterne aktører"* i fase 4 (f.eks. via nødnett).

Hvordan skal avhengigheter mellom kritiske infrastrukturer og interoperabilitet håndteres? Dersom den/de kritiske infrastrukturene som vurderes er avhengig av andre kritiske infrastrukturer (eller andre ressurser/forsyninger), så inkluderes dette som separate forhold i vurderingen, eksempelvis redundans i strøm-forsyning. Analyser av gjensidige avhengigheter mellom flere kritiske infrastrukturer i et område (f.eks. kommune, fylke, landsdekkende) er ansvaret til kommunen, fylkeskommunen, departementer, osv., ikke den enkelte infrastruktureier. Dette er tilleggsanalyser som går ut over den vurdering som gjøres med CIRAM. Intern interoperabilitet, for eksempel av ulike kommunikasjonssystemer, kan inkluderes som forhold dersom dette er viktig. Ekstern interoperabilitet i form av ekstern redundans/erstatning, ta "buss for tog" som et eksempel, kan inkluderes som et forhold, for eksempel samarbeidsavtale (for å opprettholde den kritiske funksjonen).

Trinn 6: Velg indikatorer for hvert forhold

Mens *forhold* er HVA som er viktig for å være resilient mot alvorlige farer/trusler/hendelser, så er *indikatorer* HVORDAN vi måler disse forholdene. Alle typer indikatorer kan benyttes, det vil si ja/nei spørsmål, antall, andeler, frekvenser, osv.

Et forhold kan måles med én eller flere indikatorer. Én enkelt indikator vil som oftest ikke gi en dekkende representasjon av et forhold. Dette gjelder spesielt for ja/nei spørsmål.

Det kan stilles en rekke kvalitetskrav til indikatorer, som påvirker valg av indikatorer. Noen av disse er:

1. Målbar
2. Følsom for endringer
3. Mulig å fremskaffe tilstrekkelige data for
4. Kontrollerbar
5. Individuelt valid (relevant for det aktuelle forholdet)
6. Kollektivt dekkende
7. Enkel å forstå og utvetydig
8. Benytter eksisterende data

En indikator må være *målbar*. Hvis ikke er det ikke en indikator. Den må også være *følsom for endringer*, altså at dersom forholdet endrer seg må dette reflekteres gjennom en endring i indikatorverdien. Hvis ikke er det ikke nødvendig å foreta gjentakende målinger. Dette er også relatert til *tilstrekkelige data* for å vite om endringen er statistisk signifikant eller kun tilfeldig. Indikatoren (eller egentlig forholdet den måler) bør også være *kontrollerbar*. Med andre ord, at det er mulig å påvirke og endre måleverdien. Indikatorene bør være *enkeltvis valide*, det vil si at de måler viktige aspekter ved et forhold, men enda viktigere er det at de *samlet gir tilstrekkelig dekning* – altså at de samlet sett måler de viktigste aspektene ved et forhold. Indikatorene bør også være *enkle å forstå og være utvetydige* i betydningen av at det bør være åpenbart og akseptert av "enhver" at de sier noe om kritiske infrastrukturers evne til å håndtere ekstreme hendelser. Til slutt, så er det også viktig å vurdere tilgjengeligheten av data. Ganske ofte vil brukere insistere på å *benytte kun eksisterende informasjonssystemer* for å unngå å belaste driftsorganisasjonen ekstra med å kreve innsamling av nye data. De kan også insistere på å kun benytte automatisk datainnsamling, spesielt hvis innsamlingen må gjennomføres ofte.⁸

Andre kandidater for kvalitetskriterier er reliabilitet, det vil si at ulike personer bør komme frem til samme måleresultat, og at indikatorene ikke bør være lett å manipulere. Listen over mulige kvalitetskriterier er imidlertid lang. Ingen indikatorer oppfyller alle krav. Det vil være en avveining hvilke kvalitetskrav man ønsker å vektlegge, noe som er opp til den enkelte brukeren å ta stilling til.

Identifisering av indikatorer kan gjøres av de samme ekspertene som benyttes for å identifisere viktige forhold (i trinn 5). For et gitt forhold stiller man spørsmålet: *Hva vil fortelle oss at vi håndterer dette forholdet godt?* En annen kilde til indikatorer er allerede eksisterende indikatorer som brukes av den aktuelle kritiske infrastrukturen. Indikatorer (og forhold) innsamlet i Øien m.fl. (2017b) kan også brukes som utgangspunkt. Eksempler på indikatorer er vist i tabell 2.5.

Tabell 2.5 Eksempler på indikatorer

Fase	Forhold	Indikatorer
1	Forstå risikoene	Kunnskap om avhengigheter • Er det gjennomført systematisk kartlegging av avhengigheter? • Er det foretatt en uavhengig verifikasjon?
2	Forberede/forutse	Systemer for tidlig varsling • Antall systemer for tidlig varsling • Endring i antall systemer for tidlig varsling
3	Absorbere/motstå	Varsling og kommunikasjon • Er det bemanning 24/7 for varsling og kommunikasjon?

⁸ Dette er normalt ikke tilfellet for CIRAM, som typisk gjennomføres årlig.

Fase		Forhold	Indikatorer
4	Respondere/gjenvinne	Beredskapsressurser	• Antall uavhengige varslingsveier • Prosentvis endring i personellressurser • Prosentvis endring i utstyrsressurser
5	Tilpasse/lære	Debriefing av hendelser og respons	• Gjennomsnittlig andel involverte debriefet om hendelser og respons

Det vil som oftest være behov for å spesifisere indikatorene ytterligere ved implementering.

Trinn 7: Fastsett grenseverdiene for hver indikator og angi vektor

Vi benytter en skår-skala fra 0-5, hvor 0 er verst og 5 er best, som angitt i tabell 2.6.

Tabell 2.6 Skår-skala

Skår	Resiliensnivå	Betegnelse
4-5	A	Svært bra
3-4	B	Bra
2-3	C	Middels
1-2	D	Dårlig
0-1	E	Kritisk

Hvert hele trinn i skårskalaen tilsvarer et resiliensnivå angitt med en karakter E-A, hvor E er verst (kritisk) og A er best (svært bra). Eksempelvis vil en skår mellom 3 og 4 tilsvare et resiliensnivå B (bra).

Hver enkelt indikator har sin måleskala som må tilpasses skårskalaen, altså det må angis grenseverdier for hver indikator. Det kan være en nedre grense som tilsvarer skår 0 og en øvre grense som tilsvarer skår 5 (og en antatt lineær sammenheng mellom 0-5), eller det kan angis nedre og øvre grenser innen hvert skårintervall/resiliensnivå, hvor det ikke behøver å være en lineær sammenheng mellom 0-5 (kun for hvert trinn).

For indikatorskalaen bruker vi generelt notasjonen LL (Lav-Lav), L (Lav), M (Middels), H (Høy) og HH (Høy-Høy), og angir nedre (N) og øvre (Ø) grense med senket skrift. Eksempelvis LL_N-LL_Ø som generell notasjon for å angi grenseverdiene for skår 0-1. Dette er vist i tabell 2.7.

Tabell 2.7 Grenseverdier for indikatorene og sammenheng med skårverdier

Indikatorskala, skårskala og resiliensnivå med tilhørende betegnelser og verdier					
Indikatorverdier					
Indikatorskala-betegnelse:	LL	L	M	H	HH
Indikatorskala:	LL _N -LL _Ø	L _N -L _Ø	M _N -M _Ø	H _N -H _Ø	HH _N -HH _Ø
Skårverdier					
Skårbetegnelse:	Kritisk	Dårlig	Middels	Bra	Svært bra
Skårskala*:	0-1	1-2	2-3	3-4	4-5
Skårverdier (standard):	0,5	1,5	2,5	3,5	4,5
Skårverdier for J/N spørsmål (standard):	N=0				J=5
Resiliensnivå					
Resiliensnivå-betegnelse:	E	D	C	B	A

* Forenklet er områdene angitt som 0-1, 1-2, osv. De er egentlig ikke-overlappende, dvs. [0≤Kritisk<1], [1≤Dårlig<2], osv.

Det er indikert med hvit bakgrunn at det kun er indikatorskalaen som må fastsettes av den enkelte bruker for hver av indikatorene, mens de øvrige verdiene er forhåndsdefinert (gul bakgrunn).

For å forenkle er det angitt at standard ("default") skårverdier er middelverdier på hvert nivå (0,5, 1,5, osv.) når indikatorverdien faller innenfor dette området. Et eksempel kan være *antall tilgjengelige brannmenn* hvor indikatorskalaen er satt til ([0-3>, [3-7>, [7-11>, [11-15>, [15-20]) og man måler/teller at man faktisk har 8 brannmenn tilgjengelig. Skårverdien blir da (forenklet) 2,5. Man kan velge å gjøre dette mer nøyaktig gjennom interpolasjon innenfor grenseverdiene. I eksempelet her vil skårverdien da bli 2,25.

Standard skårverdier (middelverdier på hvert nivå) benyttes også for kvalitative indikatorer hvor man bruker en fem-delt skala. For ja/nei-spørsmål er standard skårverdi 0 for "nei" og 5 for "ja".

Fastsettelse av grenseverdier er erfaringsmessige krevende. Det tar tid å fastsette disse første gang, og det er ofte behov for justering etter at man får erfaring gjennom målinger.

Et betydelig enklere alternativ, men også mindre pålitelig, er direkte skårangivelse uten grenseverdier. Det kan man gjøre ved å stille spørsmålet: "På en skala fra 0-5, hvilken skår vil du gi denne indikatoren?" Pga. subjektivitet bør mer enn én person inngå i en slik vurdering/måling.

Vekting

På alle nivå (unntatt øverste nivå – nivå 1) er det behov for å angi vekter, altså bestemme hvorvidt en indikator er viktigere enn en annen indikator (og hvor mye viktigere), hvorvidt et forhold er viktigere enn andre forhold osv., eller om de anses som like viktig og vektet likt (eller det ikke er grunnlag for å vekte de ulikt).

Ved lik vekt blir vekten av hver enhet (indikator, forhold, osv.) $1/n$, hvor n er antall enheter. Summen av vekter skal alltid være lik 1,0, enten det benyttes like eller ulike vekter.

Fastsettelse av vekter kan gjøres komplisert med bruk av egne metoder (jf. Øien m.fl., 2019a), men her beskrives en enkel fremgangsmåte. I utgangspunktet anses de fem fasene (nivå 4) å være like viktige, det vil si at de har en vekt på 0,2 (eller 20%) hver. Deretter vektet forholdene (nivå 5) innenfor hver fase. Disse kan også, som et utgangspunkt, ha lik vekt (dvs. $1/n$), men man kan velge å fordele totalvekten 1,0 (100%) ulikt mellom forholdene. På tilsvarende måte vektet indikatorene (nivå 6) innenfor hvert forhold. Er det kun én indikator for et gitt forhold er vekten 1,0 (100%).

Dersom vurderingen dekker mer enn én fare/trussel/hendelse (nivå 3), kan disse vektet likt, eller ulikt dersom man har grunnlag for det. Tilsvarende gjelder for kritiske infrastrukturer (nivå 2), dersom det inngår mer enn én i vurderingen.

Under trinn 5 var det angitt at det ikke er kritisk om et forhold plasseres i "feil" fase, fordi det kan korrigeres med bruk av vekter. Dersom man er usikker på plasseringen og samtidig ikke har noe godt grunnlag for å si at et forhold er viktigere enn et annet, så kan alle forhold *vektet likt* uavhengig av hvilken fase de er plassert i. Det innebærer at antallet forhold i hver fase påvirker vekten for hele fasen, og dermed får ikke fasene samme vekt (20%), med mindre det er akkurat samme antall forhold i hver fase. Man kan gjøre tilsvarende for *ulik vekting* av forholdene, men dette kan bli krevende når det er mange forhold totalt sett (alle vurderes mot alle; eksempelvis 35-40 forhold totalt, mot 7-8 for hver enkelt fase).

Grunnlaget/argumentasjonen for valg av eventuelle ulike vekter bør dokumenteres, og det samme gjelder valg av grenseverdier for indikatorene, slik at dette er sporbart for senere revurderinger.

Trinn 8: Angi måleverdier for indikatorene (utfør målingen)

I dette trinnet samles data inn for indikatorene, det vil si at de faktiske indikatorverdiene måles/fastsettes/beregnes. Verdiene kan komme fra ulike informasjonssystemer (automatisk eller manuelt), basere seg på dataanalyse (stordata/big data), angis av eksperter, osv.

Måleverdiene på indikatornivå benyttes for å beregne/bestemme indikatorskår, og sammen med vektorer beregnes skår og resiliensnivå på aggregerte nivå i trinn 9.

Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)

Måleverdien til en indikator (indikatorverdien) gir en skår i henhold til tabell 2.7. Skårverdien har også et tilhørende resiliensnivå (E-A), som angitt nederst i tabell 2.7.

Skårverdier for forhold (nivå 5) beregnes som summen av vektete skårverdier for de underliggende indikatorene, skårverdier for faser (nivå 4) beregnes som summen av vektete skårverdier for de underliggende forholdene, osv. inntil man har den totale skårverdien for området (nivå 1). På hvert nivå tilsvarer skårverdien et resiliensnivå.

Eksempel: Indikator 1 har skår 3,5 og vekt 0,7, mens indikator 2 har skår 1,5 og vekt 0,3. Forhold A måles kun med disse to indikatorene. Skårverdien til forhold A blir da $(3,5 \cdot 0,7) + (1,5 \cdot 0,3) = 2,9$, som ligger mellom 2 og 3, og dermed tilsvarer resiliensnivå C (middels).

Generelle formler for beregning av skårverdier på alle nivå er beskrevet i vedlegg G.

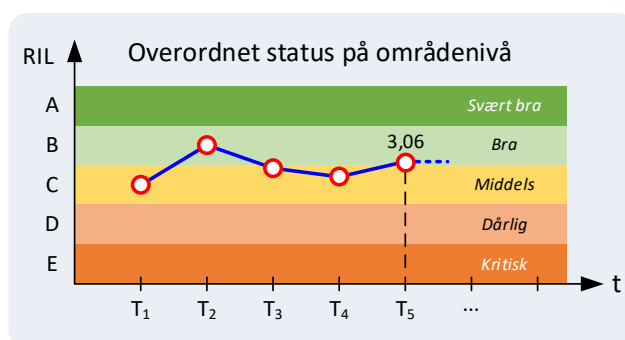
Beregningene er enkle og oversiktlige, og de kan gjøres for hånd. Det er imidlertid mer hensiktsmessig å benytte et Excel-regneark eller et annet verktøy, spesielt når det er mange indikatorer og målingene gjentas regelmessig. Det er også nyttig med et verktøy for presentasjon av resultatene (jf. trinn 10).

Et verktøy for beregninger og visualisering av resultater er beskrevet i vedlegg H.

Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.

Resiliensvurderingen gir en overordnet status for hele området som er vurdert, men også detaljert status på alle underliggende nivå. Den detaljerte statusen avdekker styrker og svakheter, og hvor forbedringsbehovet er mest prekært. Brukt over tid, med gjentakende målinger, vil man avdekke egen utvikling (trend) over tid.

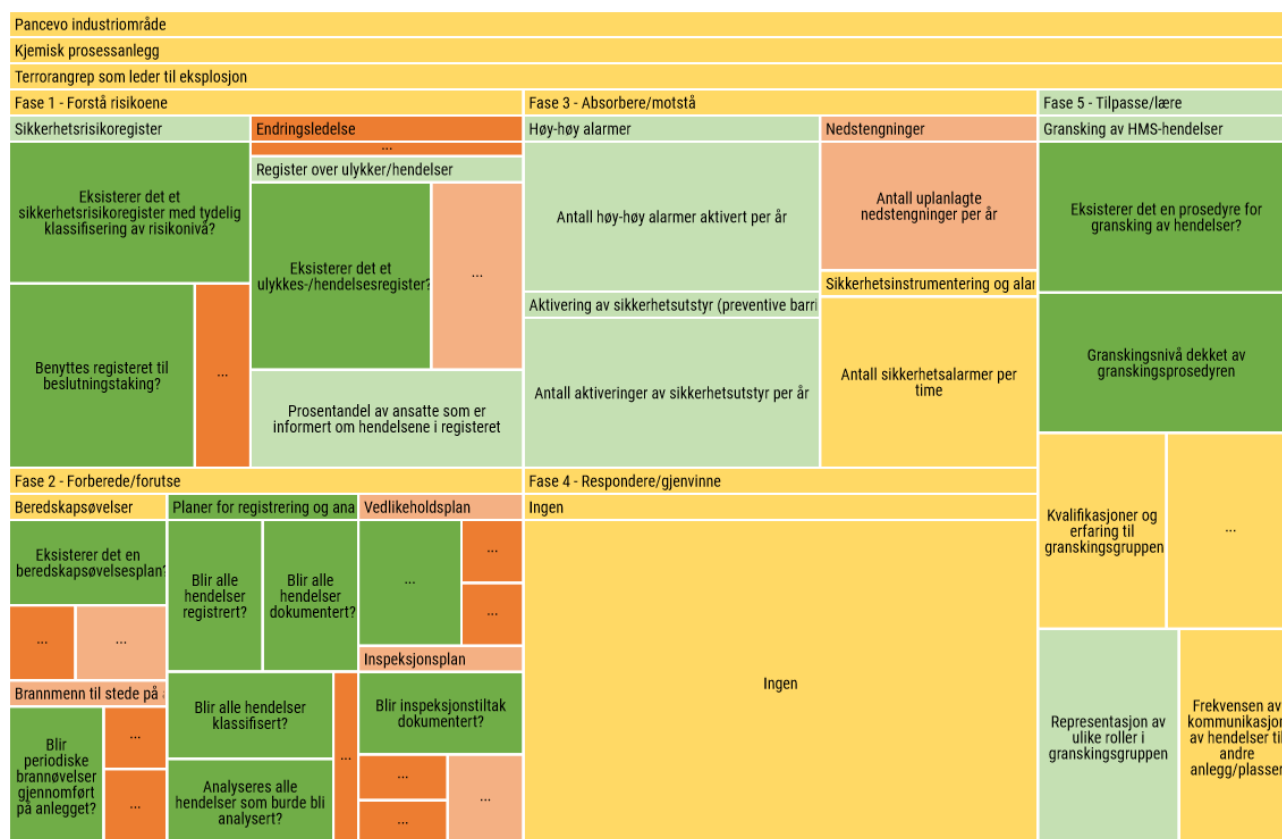
Overordnet status og trend er vist i figur 2.2.



Figur 2.2 Overordnet status og trend

Figur 2.2 viser en regelmessig måling, for eksempel årlig, hvor den overordnede statusen ved siste måling (ved tidspunkt T₅) er beregnet til en skår 3,06. Denne er akkurat innenfor intervallet 3-4 og dermed er resiliensnivået (RIL) lik B (bra). Trenden viser en forbedring siden forrige måling (T₄), men at statusen har vært bedre tidligere (T₂). Det vil være naturlig at kontinuerlig forbedring er en målsetting. Trend kan også vises på alle underliggende nivå.

Detaljert status på underliggende nivå kan presenteres med bruk av et trestruktur-diagram (TreeMap) som vist i figur 2.3.



Figur 2.3 Tre-struktur for visualisering av resiliens på alle nivå

Bakerst/ytterst i figuren vises område (nivå 1), dernest kritisk infrastruktur (nivå 2) og trussel (nivå 3). Siden det i eksempelet her er kun én kritisk infrastruktur og én trussel, så er disse nivåene representert med kun ett rektangel hver. Alle har RIL=C (middels). Fasene vises alltid som fem rektangler, og innenfor disse vises henholdsvis forhold og indikatorer.

Viktigheten (vekten) angis av størrelsen på rektanglene. Grønne rektangler angir styrker, mens røde angir svakheter. Store grønne rektangler (høy skår på viktige forhold/indikatorer) synliggjør hvor resiliensen er bra eller svært bra. Store røde rektangler (lav skår på viktige forhold/indikatorer) synliggjør hvor det er størst behov for forbedring. Se også figur 4.13, hvor samme trestrukturdiagram inngår.⁹

Man kan i tillegg etablere "10-på-topp-lister" over forhold eller indikatorer sortert etter skår og/eller RIL, for å vise styrker og svakheter, og dermed behov for forbedring.

⁹ Detaljer rundt trestruktur-diagram kan man finne blant annet i Barzelay m.fl. (2018).

Statusinformasjonen kan benyttes til å gi svar på spørsmål som:

- Hvilken kritisk infrastruktur er minst resilient (lavest skår / dårligst RIL)?
- Hvilken fare/trussel/hendelse er mest utfordrende (lavest skår / dårligst RIL)?
- Hvilken fase er "svakest" (lavest skår / dårligst RIL)?
- Hvilke forhold bidrar mest til lav skår / dårlig RIL i den "svakeste" fasen?
- Hvilke forhold bidrar mest til lav skår / dårlig RIL totalt sett?

Det er også mulig å tilpasse vurderingen slik at den kan benyttes til sammenlikning med andre. Da er man i utgangspunktet avhengig av at man for samme infrastruktur og fare/trussel/hendelse benytter de samme forholdene og indikatorene. Dette brukes typisk for ekstern evaluering og sammenlikning. Alternativt kan noen av forholdene og indikatorene være de samme, og sammenlikningen avgrenses til disse.

3 ANVENDELSESOMRÅDER, TILPASNINGER OG BEGRENSNINGER

Her ser vi på de mest aktuelle anvendelsesområdene (kritiske samfunnsfunksjoner) og sammenhengen mellom resiliensvurderinger og allerede eksisterende påkrevde analyser og planer, blant annet for å utdype merverdien med resiliensvurderinger. Også tilpasninger og begrensninger er beskrevet.

Aktuelle anvendelsesområder og eksisterende krav til analyser og planer

Regjeringen har det øverste ansvaret for den nasjonale beredskapen og håndteringen av hendelser som rammer samfunnet. Ansvar for å forberede og iverksette tiltak som er nødvendige for å håndtere uønskede hendelser, er tillagt det enkelte departement og underlagte etater. Regionalt ligger ansvaret hos fylkesmenn og kommuner. Politiet leder redningssentralene og er i henhold til politiloven § 27 normalt ansvarlig for å iverksette og organisere redningsinnsats der menneskers liv eller helse er truet. Justis- og beredskapsdepartementet er ut over sitt sektoransvar tillagt en samordningsrolle for å sikre en helhetlig og koordinert beredskap i sivil sektor (DSB, 2016, s. 34-35).

Ansvar og oppgaver ved sivil krisehåndtering er i noen grad lov- og instruksfestet. Det samme gjelder militær krisehåndtering, hvor også internasjonal rett (folkeretten) har stor betydning.

En tabell (se vedlegg I) er satt sammen på bakgrunn av informasjon i DSBs KIKS-II-rapport om samfunnets kritiske funksjoner (DSB, 2016). Lover og forskrifter er gjennomgått for å kartlegge hvilke analyser og planer som er påkrevde og hvilke aktører som er ansvarlige for disse. Denne kartleggingen er svært omfattende, og er kun påbegynt for noen samfunnsfunksjoner. Kartleggingen vil kompletteres i nye versjoner av denne veilederen etter hvert som metoden anvendes på flere områder. Foreløpig status for kartleggingen er vist i vedlegg I.

Sammenhengen mellom resiliensvurderinger og eksisterende påkrevde analyser og planer, som risiko- og beredskapsanalyser, ROS-analyser, kontinuitetsvurderinger og beredskaps- og kontinuitetsplaner, er beskrevet generelt under kap. 1.3 om nytteverdien ved resiliensvurderinger. Den konkrete sammenhengen, og dermed merverdien i forhold til andre analyser og planer, avhenger imidlertid av hvilke analyser og planer som er påkrevd innenfor det enkelte anvendelsesområdet, og hvordan disse i praksis gjennomføres og utformes. Dette krever en nærmere vurdering av analyser og planer innenfor hvert område, og som vil være en forberedelse til en resiliensvurdering. Dette vil inngå som del av nye eksempler på gjennomføring av resiliensvurderinger med bruk av denne veilederen.

Generelle merverdier inkluderer blant annet a) oversikt over og status på resiliensnivået b) håndtering av det uventede og overraskelser, c) en samlet vurdering, d) "stress-testing" og e) bevisstgjøring. Først og fremst gir CIRAM en *oversikt over forhold som bidrar til resiliens og status på resiliensnivået*. Dette inkluderer håndtering av *det uventede og overraskelser* (som ikke dekkes av risikovurderinger, jf. kap. 1.3). En resiliensvurdering utgjør *en samlet vurdering* av forhold som inngår i en rekke ulike analyser og planer (risiko, beredskap, virksomhetskontinuitet, m.m.), og den utgjør en form for *"stress-testing"* når ekstreme hendelser legges til grunn. Resiliensvurderingen bidrar også til en (påtvunget) *bevisstgjøring* av hva som er viktig for å opprettholde kritisk funksjon og håndtere ekstreme hendelser, på tvers av alle aktører som bidrar til dette gjennom ulike analyser enten under design eller drift.

Alternative anvendelser og tilpasninger

Metoden kan anvendes på ulike nivå fra lokalt til nasjonalt nivå og kan også tilpasses behovene. På nasjonalt nivå kan en alternativ anvendelse være å gi oversikt for regjering, departementer, etater, direktorater og tilsynsorganer i forhold til deres oppfølgings- og tilsynsplikt, eksempelvis DSBs og fylkesmennenes

oppfølging av kommunene i forhold til kommunal beredskapsplikt, NSMs (og NVEs¹⁰) oppfølging av bruken av deres grunnprinsipper, osv. På lokalt nivå vil kommuner og infrastructureiere kunne gjennomføre konkrete resiliensvurderinger.

Begrensninger

Selv om en resiliensvurdering kan gi generelle merverdier som nevnt ovenfor, så kan det være krevende å påvise spesifikke merverdier i forhold til eksisterende (og ofte påkrevde) analyser og planer innenfor et bestemt anvendelsesområde, herunder pedagogiske utfordringer med "resiliens" som begrep.¹¹

Grunntanken er at en resiliensvurdering kommer i tillegg til andre sikkerhets- og risikovurderinger. Det er ingen erstatning for disse.¹²

Resiliensvurdering med bruk av CIRAM er i stor grad medvirkningsbasert og resultatet blir ikke bedre enn innsatsen som legges ned i vurderingen. Det er som tidligere nevnt brukeren som til syvende og sist avgjør omfanget av vurderingen, herunder antall forhold og tilhørende indikatorer som inkluderes.

I prinsippet kan alle typer forhold inkluderes (tekniske, menneskelige, organisatoriske, sosiale, osv.), men det vil selvsagt være enkelte forhold som er vanskeligere å måle enn andre.

CIRAM representerer en strukturert tilnærming og det vil høyst sannsynlig være behov for tilpasninger i de enkelte tilfellene. Én slik tilpasning – som utgjør et spesialtilfelle – er å inkludere en direktevurdering av omfanget av tap av kritisk funksjon, eksempelvis gjennom grad av funksjonstap og varighet.¹³

Eksempler

Eksempler er gitt i neste kapittel, og nye eksempler vil legges til etter hvert som metoden anvendes i Norge.

¹⁰ NVE – Norges vassdrags- og energidirektorat.

¹¹ Se vedlegg A.

¹² Se vedlegg B for en diskusjon rundt den såkalte "Safety II"-tilnærmingen som *erstatning* for den påståtte (dagens og tidligere) "Safety I"-tilnærming. Dette er en farlig vei å gå og har blitt kraftig imøtegått og kritisert (Leveson, 2020).

¹³ Dette er i utgangspunktet en alternativ fremgangsmåte sammenliknet med CIRAM, siden CIRAM baserer seg på en indirekte vurdering av resiliens.

4 EKSEMPLER

Fire eksempler er tatt med i denne versjonen av veilederen. Det første eksempelet er "eksplosjon i kjemisk industri" fra uttestingen under utviklingen av metoden i EU-prosjektet SmartResilience. Det andre eksempelet er "pandemi i Norge (covid-19)". Det tredje eksempelet er "nettangrep", og det fjerde eksempelet er knyttet til "ekstremvær" som følge av klimaendringer. Flere eksempler vil legges til etter hvert som metoden blir benyttet innenfor kritisk infrastruktur i Norge.

4.1 Eksplosjon i kjemisk anlegg

Eksempelet dekker kjemisk industri og er hentet fra Øien m.fl. (2019b). Det er ikke et komplett eksempel og det er gjort en del forenklinger og antakelser, men det illustrerer bruken av metoden.

Figur 4.2-4.9 er utdrag fra et Excel-regneark som ble benyttet for beregningene.

Pančevo er en by (ca. 90.000 innbyggere) og kommune (ca. 130.000 innbyggere) utenfor Beograd i Serbia. Den har det såkalte sørlige industriområdet lokalisert ved den sørøstlige utkanten av byen, rett ved siden av boligområdet i byen, ca. 4 km fra sentrum. Området er forbundet med vei, jernbane og en havn ved elva Donau. I dette industriområdet produseres det petroleumsprodukter, kjemiske produkter, polyetylen, mineralgjødsel, osv. Anleggene/infrastrukturene i industriområdet er sammenhengende og gjensidig avhengige. Hele industriområdet betraktes som en stor kritisk infrastruktur.

Eksplosjon – BLEVE (kokende væskeekspanderende dampeksplasjon) – er av eierne (NIS – Petroleum Industry of Serbia) identifisert som den største ulykken med de alvorligste konsekvensene basert på beregning og modellering gjort og presentert i sikkerhetsrapporten.

En av hovedårsakene er lekkasje av flytende petroleumsgass (LPG) i en ventilflens plassert ved siden av LPG-fartøyet, med påfølgende antennelse av LPG. Forbrenning av LPG som strømmer ut av ventilflensen vil ha direkte kontakt med fartøyet og vil føre til oppvarming av LPG inne i fartøyet. Dette vil resultere i rask fordampning og økt trykk som vil føre til eksplosjon. Konsekvensene av en slik eksplosjon kan hypotetisk omfatte en domino-effekt på grunn av termisk stråling og flyvende vrakrester. Hendelsen kan også utløses av terrorangrep eller sabotasje. Hypotetisk er det også mulig å bli påvirket via nettangrep på IKT-systemer.



Figur 4.1 Bilder fra i) deler av hovedanlegget, ii) kritisk ventil, iii) testing av vannkanoner ved havneanlegget (Foto: Knut Øien, februar 2018)

Eksempelet er beskrevet trinn for trinn i henhold til tabell 2.2 (metodetrinn).

Trinn 1: Velg område

Området er det sørlige industriområdet til byen Pančevo utenfor Beograd i Serbia.

Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)

Industriområdet produserer blant annet petroleumsprodukter og bidrar dermed til den kritiske samfunnsfunksjonen (delfunksjonen) drivstofforsyning, som består av kritisk infrastruktur som raffinerier, havneanlegg, tankanlegg, og bensinstasjoner.

I EU betraktes *kjemisk industri* som en kritisk infrastruktur-sektor, og kritiske infrastruktur-produkter eller -tjenester innbefatter *produksjon og lagring/prosessering av kjemiske og nukleære stoffer*.

Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene

Tre aktuelle farer/trusler/hendelser som ble valgt av selskapet ansvarlig for anleggene (NIS) var:

1. Terrorangrep (som igjen kan utløse BLEVE-eksplosjon og eskalering/dominoeffekter)
2. Naturlige farer (flom i elva Donau)
3. Farer relatert til ny teknologi (BLEVE-eksplosjon i LPG-anlegget/LPG-fartøy)

Trinn 4: Vurder hver fase for hver fare/trussel/hendelse

Her er hver av farene/truslene/hendelsene vurdert for hver av de fem fasene (jf. figur 1.1 og tabell 2.3).

Trinn 5: Velg forhold for hver fase

Hvilke forhold er viktig for det kjemiske anlegget for å håndtere – være resilient mot – terrorangrep (eller flom eller eksplosjon)? HVA er viktig?

HVA er viktig for å forstå risikoene (fase 1), forberede/forutse (fase 2), absorbere/motstå (fase 3), respondere/gjenvinne (fase 4) og tilpasse/lære (fase 5) av disse farene/truslene/hendelsene?

Viktige forhold, slik NIS vurderte det under uttestingen av metoden, er vist i tabell 4.1.

Tabell 4.1 Viktige forhold identifisert for hver fase

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Forstå risikoene	Forberede/forutse	Absorbere/motstå	Respondere/gjenvinne	Tilpasse/lære
Sikkerhetsrisikoregister	Beredskapsøvelser	Høy-høy alarmer	(Ingen)	Gransking av hendelser
Endringsledelse	Brannmenn til stede på anlegget	Aktivering av sikkerhetsutstyr		
Hendelsesregister	Plan for registrering og analyse av hendelser	Nedstengninger		
	Vedlikeholdsplan	Sikkerhetsinstrumentering og alarmer		
	Inspeksjonsplan			

Identifiseringen er ikke fullstendig. Blant annet mangler det forhold i fase 4, og plasseringen av enkelte forhold kan diskuteres. "Brannmenn ved anlegget" er en respons-ressurs som kunne vært plassert under fase

4. Dessuten bør det være flere forhold enn disse som er viktige. Vi har antydnet at det bør være minst 7-8 forhold i hver fase for å gi en noenlunde representativ vurdering av resiliens.

Trinn 6: Velg indikatorer for hvert forhold

HVORDAN måler vi disse viktige forholdene, ved hjelp av indikatorer (ja/nei spørsmål, antall, andeler, frekvenser, osv.)? Hvilke indikatorer er relevante for de ulike forholdene (én eller flere per forhold)?

Eksempler på indikatorer av ulike typer er vist for de tre forholdene i fase 1 fra trinn 5:

- Sikkerhetsrisikoregister
 - Eksisterer det et sikkerhetsrisikoregister med tydelig klassifisering av risikonivå?
 - Benyttes registeret til beslutningstaking?
 - Er det definert en frekvens for oppdatering av registeret?
- Endringsledelse
 - Er det etablert en prosedyre for endringsledelse?
- Register over ulykker/hendelser
 - Eksisterer det et ulykkes-/hendelsesregister?
 - Frekvensen av kommunikasjon til operatørene om hendelser
 - Prosentandel av ansatte som er informert om hendelsene i registeret

Her har NIS valgt tre indikatorer for første og siste forhold og én indikator for det andre forholdet, med en blanding av ja/nei-spørsmål, frekvenser og prosenter.

Når det blir mange indikatorer kan det være hensiktsmessig å nummerere dem kronologisk for fase, forhold og indikator. Vi har valgt å bruke romertall for fasene, slik at forholdene listet ovenfor blir I.1, I.2 og I.3. Indikatorene for sistnevnte blir da I.3.1, I.3.2 og I.3.3.

Trinn 7: Fastsett grenseverdiene for hver indikator og angi vektor

Eksempel på fastsettelse av grenseverdier for indikatorene I.3.1, I.3.2 og I.3.3 er vist i tabell 4.2.

Tabell 4.2 Fastsettelse av grenseverdier for indikatorene

Grenseverdier for indikatorene (indikator-skalaer)					
Indikatorskala-betegnelse:	LL	L	M	H	HH
I.3.1 Eksisterer det et ulykkes-/hendelsesregister?	Nei				Ja
I.3.2 Frekvensen av kommunikasjon til operatørene om hendelser [per måned]	< 1/6	1/6	1/3	1	Alltid
<i>I.3.2 Frekvensen av kommunikasjon til operatørene om hendelser [per måned]</i>	<i>< 1/6</i>	<i>1/6-1/4</i>	<i>1/4-1/2</i>	<i>1/2-1</i>	<i>> 1</i>
I.3.3 Prosentandel av ansatte som er informert om hendelsene i registeret	0-30	30-50	50-70	70-90	90-100

Her har NIS gjort en vurdering av hva som skal gi laveste skår og høyeste skår. Første indikator er et ja/nei spørsmål hvor nei gir absolutt laveste skår (0) og ja gir absolutt høyeste skår (5,0). Andre indikator (I.3.2) er først vist slik NIS opprinnelig definerte grenseverdiene, deretter korrigerte grenseverdier. Problemet med de første grenseverdiene var at de ikke anga intervall, og dermed uklart hvilken verdi f.eks. 1/5 eller 1/4 skulle gi, samt at "alltid" eller "hver gang" kunne være sjeldnere enn 1 per måned (men allikevel gi bedre skår).

Med de korrigerte grenseverdiene blir I.3.2 på samme form som I.3.3. I utgangspunktet vil middelverdiene for skårverdiene benyttes (dvs. 0,5, 1,5, 2,5, 3,5 eller 4,5) uavhengig av hvor i de enkelte intervallene indikatorverdiene ligger. Hvis man ønsker å gjøre det mer nøyaktig kan man interpolere innenfor hvert intervall. F.eks. hvis I.3.3 er 25 %, så kan man benytte skår 0,83 i stedet for middelverdien 0,5.

I denne uttestingen av metoden dokumenterte ikke NIS valgene av grenseverdier, noe som normalt bør gjøres, fordi det ofte vil bli behov for å revurdere grenseverdiene etter at man har tatt metoden/verktøyet i bruk.

Tilsvarende ble det under uttestingen gjort forenklinger med hensyn til vekting, hvor kun lik vekting ble benyttet. Det vil si at indikatorene I.3.1, I.3.2 og I.3.3 alle ble gitt vekt 1/3 (33 %). Det samme ble de tre forholdene I.1, I.2 og I.3, samt de tre indikatorene for forhold I.1. Indikator I.2.1, som er eneste indikator for forhold I.2 har naturligvis vekt 100 %.

Figur 4.2 viser flere grenseverdier angitt av NIS for indikatorene i fase 1 og 5. (Fase 2-4 er ikke vist her).

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia			Resiliensnivå, skår-skala og skår-verdier				
			Kritisk	Dårlig	Middels	Bra	Svært bra
			E	D	C	B	A
			0-1	1-2	2-3	3-4	4-5
			0,5	1,5	2,5	3,5	4,5
Område: Det sørlige industriområdet i byen Pančevo			Indikator-skala (grenseverdier) for hver indikator (J/N: J=5 and N=0)				
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer							
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)							
Fase I - Forstå risikoene							
Nr.	Forhold	Indikatorer					
I.1	Sikkerhetsrisikoregister						
I.1.1		Eksisterer det et sikkerhetsrisikoregister med tydelig klassifisering av risikonivå?	0				5
I.1.2		Benyttes registeret til beslutningstaking?	0				5
I.1.3		Er det definert en frekvens for oppdatering av registeret?	0				5
I.2	Endringsledelse						
I.2.1		Er det etablert en prosedyre for endringsledelse?	0				5
I.3	Register over ulykker/hendelser						
I.3.1		Eksisterer det et ulykkes-/hendelsesregister?	0				5
I.3.2		Frekvensen av kommunikasjon til operatørene om hendelser [per mnd]	< 1/6	1/6	1/3	1	Alltid
I.3.3		Prosentandel av ansatte som er informert om hendelsene i registeret	0-30%	30-50%	50-70%	70-90%	90-100%
Fase V - Tilpasse/lære							
Nr.	Forhold	Indikatorer					
V.1	Gransking av HMS-hendelser						
V.1.1		Eksisterer det en prosedyre for gransking av hendelser?	0				5
V.1.2		Granskingsnivå dekket av granskingsprosedyren	Ingen	P&D	Alle-2	Alle-1	Alle
V.1.3		Kvalifikasjoner og erfaring til granskingsgruppen	Ingen	> 1 år	> 2 år	> 3-4 år	> 5 år
V.1.4		Prosentandel anvendelse av granskingsprosedyren	< 19%	20-39%	40-59%	60-79%	80-100%
V.1.5		Representasjon av ulike roller i granskingsgruppen	Ingen	1 rolle	2 roller	3 roller	4 roller
V.1.6		Frekvensen av kommunikasjon av hendelser til andre anlegg/plasser	Aldri	1/s.ulykke	1/år	1/6 mnd	1/3 mnd

Figur 4.2 Fastsettelse av grenseverdier for indikatorene

Alle de øvrige indikatorene i fase 1, som ikke allerede er omtalt, er av typen ja/nei-spørsmål, som gir enten skår 0 (nei) eller skår 5 (ja).

I fase 5 fastsettes skårverdi til indikator V.1.2 og V.1.5 ut fra kvalitative beskrivelser. Indikator V.1.6 kunne, tilsvarende som indikator I.3.2, benyttet intervall, i alle fall for de tre kategoriene med høyest skår. "Aldri" og hver gang det skjer en stor ulykke ("1/s.ulykke") kan beholdes slik de er.

Trinn 8: Angi måleverdier for indikatorene (utfør målingen)

Indikatorenes virkelige verdier registreres/måles i henhold til type indikator-skala (ja/nei, prosent, frekvens, kvalitativt utsagn, osv.) på et gitt tidspunkt. Det kan typisk være en årlig gjentatt måling for sammenlikning med tidligere års resultater og utvikling.

Indikatorverdiene/måleverdiene er vist i siste kolonne i figur 4.3.

Her er det seks ja/nei-spørsmål som er besvart, to prosentandeler og to frekvenser som er registrert og tre kvalitative målinger som er utført. Måleverdiene bør være de samme uavhengig av hvem som gjennomfører målingen.

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia			Resiliensnivå, skår-skala og skår-verdier					Indikator virkelig verdi	
			Kritisk	Dårlig	Middels	Bra	Svært bra		
			E	D	C	B	A		
			0-1 0,5	1-2 1,5	2-3 2,5	3-4 3,5	4-5 4,5		
Område: Det sørlige industriområdet i byen Pančevo			Indikator-skala (grenseverdier) for hver indikator (J/N: J=5 and N=0)						
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer									
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)									
Fase I - Forstå risikoene									
	Nr.	Forhold	Indikatorer						
	I.1		Sikkerhetsrisikoregister						
	I.1.1		Eksisterer det et sikkerhetsrisikoregister med tydelig klassifisering av risikonivå?	0				5	J
	I.1.2		Benyttes registeret til beslutningstaking?	0				5	J
	I.1.3		Er det definert en frekvens for oppdatering av registeret?	0				5	N
	I.2		Endringsledelse						
	I.2.1		Er det etablert en prosedyre for endringsledelse?	0				5	N
	I.3		Register over ulykker/hendelser						
	I.3.1		Eksisterer det et ulykkes-/hendelsesregister?	0				5	J
	I.3.2		Frekvensen av kommunikasjon til operatørene om hendelser [per mnd]	< 1/6	1/6	1/3	1	Alltid	1/6
	I.3.3		Prosentandel av ansatte som er informert om hendelsene i registeret	0-30%	30-50%	50-70%	70-90%	90-100%	80 %
Fase V - Tilpasse/lære									
	Nr.	Forhold	Indikatorer						
	V.1		Gransking av HMS-hendelser						
	V.1.1		Eksisterer det en prosedyre for gransking av hendelser?	0				5	J
	V.1.2		Granskingsnivå dekket av granskingsprosedyren	Ingen	P&D	Alle-2	Alle-1	Alle	Alle
	V.1.3		Kvalifikasjoner og erfaring til granskingsgruppen	Ingen	> 1 år	> 2 år	> 3-4 år	> 5 år	> 2 år
	V.1.4		Prosentandel anvendelse av granskingsprosedyren	< 19%	20-39%	40-59%	60-79%	80-100%	50 %
	V.1.5		Representasjon av ulike roller i granskingsgruppen	Ingen	1 rolle	2 roller	3 roller	4 roller	3 roller
	V.1.6		Frekvensen av kommunikasjon av hendelser til andre anlegg/plasser	Aldri	1/s.ulykke	1/år	1/6 mnd	1/3 mnd	1/år

Figur 4.3 Registrering av indikatorenes virkelige verdier - måleverdiene

Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)

Beregningene gjennomføres på alle seks nivå. Figur 4.4 viser beregningene på indikator-nivå (nivå 6).

Indikatorenes skårverdier fastsettes ved å sammenlikne måleverdien med indikatorskalaen. Ja/nei-spørsmål gir enten 0 eller 5, mens de øvrige her er gitt middelverdien i tilhørende skår-intervall (0,5, 1,5, 2,5, 3,5, eller 4,5). Skårintervallet gir også direkte et gitt resiliensnivå (RIL) for indikatorene (0-1 gir E, 1-2 gir D, 2-3 gir C, 3-4 gir B, og 4-5 gir A).

Skårverdien multiplisert med vekten gir indikatorens vektete skår (siste kolonne i figur 4.4). Denne verdien tas videre til beregninger på neste nivå.

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia			Indikator: skår, vektor og RIL				
			Indikator virkelig verdi	Indikator skår verdi	Indikator resiliens nivå	Indikator vekt	Indikator vektet skår
Område: Det sørlige industriområdet i byen Pančevo							
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer							
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)							
Fase I - Forstå risikoene							
Nr.	Forhold	Indikatorer					
I.1	Sikkerhetsrisikoregister						
I.1.1		Eksisterer det et sikkerhetsrisikoregister med tydelig klassifisering av risikonivå?	J	5	A	0,33	1,67
I.1.2		Benyttes registeret til beslutningstaking?	J	5	A	0,33	1,67
I.1.3		Er det definert en frekvens for oppdatering av registeret?	N	0	E	0,33	0,00
I.2	Endringsledelse						
I.2.1		Er det etablert en prosedyre for endringsledelse?	N	0	E	1,00	0,00
I.3	Register over ulykker/hendelser						
I.3.1		Eksisterer det et ulykkes-/hendelsesregister?	J	5	A	0,33	1,67
I.3.2		Frekvensen av kommunikasjon til operatørene om hendelser [per mnd]	1/6	1,5	D	0,33	0,50
I.3.3		Prosentandel av ansatte som er informert om hendelsene i registeret	80 %	3,5	B	0,33	1,17
Fase V - Tilpasse/lære							
Nr.	Forhold	Indikatorer					
V.1	Gransking av HMS-hendelser						
V.1.1		Eksisterer det en prosedyre for gransking av hendelser?	J	5	A	0,17	0,83
V.1.2		Granskingsnivå dekket av granskingsprosedyren	Alle	4,5	A	0,17	0,75
V.1.3		Kvalifikasjoner og erfaring til granskingsgruppen	> 2 år	2,5	C	0,17	0,42
V.1.4		Prosentandel anvendelse av granskingsprosedyren	50 %	2,5	C	0,17	0,42
V.1.5		Representasjon av ulike roller i granskingsgruppen	3 roller	3,5	B	0,17	0,58
V.1.6		Frekvensen av kommunikasjon av hendelser til andre anlegg/plasser	1/år	2,5	C	0,17	0,42

Figur 4.4 Beregninger på indikator-nivå (nivå 6)

Figur 4.5 viser beregningene på forhold-nivå (nivå 5).

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia			Forhold: skår, vektor og RIL				
			Indikator vektet skår	Forhold skår	Forhold resiliens nivå	Forhold vekt	Forhold vektet skår
Område: Det sørlige industriområdet i byen Pančevo							
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer							
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)							
Fase I - Forstå risikoene							
Nr.	Forhold	Indikatorer					
I.1	Sikkerhetsrisikoregister			3,33	B	0,33	1,11
I.1.1		Eksisterer det et sikkerhetsrisikoregister med tydelig klassifisering av risikonivå?	1,67				
I.1.2		Benyttes registeret til beslutningstaking?	1,67				
I.1.3		Er det definert en frekvens for oppdatering av registeret?	0,00				
I.2	Endringsledelse			0,00	E	0,33	0,00
I.2.1		Er det etablert en prosedyre for endringsledelse?	0,00				
I.3	Register over ulykker/hendelser			3,33	B	0,33	1,11
I.3.1		Eksisterer det et ulykkes-/hendelsesregister?	1,67				
I.3.2		Frekvensen av kommunikasjon til operatørene om hendelser [per mnd]	0,50				
I.3.3		Prosentandel av ansatte som er informert om hendelsene i registeret	1,17				
Fase V - Tilpasse/lære							
Nr.	Forhold	Indikatorer					
V.1	Gransking av HMS-hendelser			3,42	B	1,00	3,42
V.1.1		Eksisterer det en prosedyre for gransking av hendelser?	0,83				
V.1.2		Granskingsnivå dekket av granskingsprosedyren	0,75				
V.1.3		Kvalifikasjoner og erfaring til granskingsgruppen	0,42				
V.1.4		Prosentandel anvendelse av granskingsprosedyren	0,42				
V.1.5		Representasjon av ulike roller i granskingsgruppen	0,58				
V.1.6		Frekvensen av kommunikasjon av hendelser til andre anlegg/plasser	0,42				

Figur 4.5 Beregninger på forhold-nivå (nivå 5)

Et forhold sitt skår (skårverdi) fås ved å summere vektet skår for de indikatorene som inngår i (benyttes for å måle) forholdet. For forhold I.1 blir dette $1,67 + 1,67 + 0 = 3,33$.

Dette tilsvarer resiliensnivå B siden skår 3,33 ligger mellom 3-4 (jf. fig. 4.2 og 4.3).

Forhold I.1 er vektet likt med øvrige forhold i fase 1, dvs. $1/3 = 0,33$.

Vektet skår (skår multiplisert med vekt) blir for forhold I.1 $3,33 \cdot 0,33 = 1,11$. Denne verdien tas videre til beregninger på neste nivå.

Figur 4.6 viser beregningene på fase-nivå (nivå 4).

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia			Fase: skår, vektor og RIL			
			Forhold vektet skår	Fase skår	Fase resiliens nivå	Fase vektet skår
Område: Det sørlige industriområdet i byen Pancevo						
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer						
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)						
Fase I - Forstå risikoene				2,22	C	0,44
Nr.	Forhold	Indikatorer				
I.1	Sikkerhetsrisikoregister		1,11			
I.2	Endringsledelse		0,00			
I.3	Register over ulykker/hendelser		1,11			
Fase II - Forberede/forutse				2,29	C	0,46
Nr.	Forhold	Indikatorer				
II.1	Beredskapsøvelser		0,47			
II.2	Brannmenn til stede på anlegget		0,37			
II.3	Planer for registrering og analyse av hendelser på anlegget		0,80			
II.4	Vedlikeholdsplan		0,33			
II.5	Inspeksjonsplan		0,33			
Fase III - Absorbere/motstå				2,75	C	0,55
Nr.	Forhold	Indikatorer				
III.1	Høy-høy alarmer		0,88			
III.2	Aktivering av sikkerhetsutstyr (preventive barrierer)		0,88			
III.3	Nedstengninger		0,38			
III.4	Sikkerhetsinstrumentering og alarmer		0,63			
Fase IV - Respondere/gjenvinne				2,50	C	0,50
Nr.	Forhold	Indikatorer				
IV.1						
Fase V - Tilpasse/lære				3,42	B	0,68
Nr.	Forhold	Indikatorer				
V.1	Gransking av HMS-hendelser		3,42			

Figur 4.6 Beregninger på fase-nivå (nivå 4)

Skårverdier for faser fås ved å summere vektet skår for forholdene som inngår i fasen. For fase 1 blir dette $1,11 + 0 + 1,11 = 2,22$. Dette tilsvarer resiliensnivå C siden skår 2,22 ligger mellom 2-3. For fase 4, hvor det ikke er identifisert forhold, og vi dermed ikke kjenner statusen, er det gitt en middels skårverdi (2,5).

Fase 1 er vektet likt med øvrige faser, dvs. $1/5 = 0,20$. Vektet skår (skår multiplisert med vekt) blir for fase 1 $2,22 \cdot 0,2 = 0,44$. Denne verdien tas videre til beregninger på neste nivå.

Figur 4.7 viser beregningene på trussel-nivå (nivå 3).

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia	Fase vektet skår	Trussel: skår, vektor og RIL			
		Trussel skår	Trussel resiliens nivå	Trussel vekt	Trussel vektet skår
Område: Det sørlige industriområdet i byen Pančevo					
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer					
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)		2,64	C	0,33	0,88
Fase I - Forstå risikoene	0,44				
Fase II - Forberede/forutse	0,46				
Fase III - Absorbere/motstå	0,55				
Fase IV - Respondere/gjenvinne	0,50				
Fase V - Tilpasse/lære	0,68				
Trussel 2: Naturlige farer (flom i elva Donau)		2,64	C	0,33	0,88
Trussel 3: Farer relatert til ny teknologi (BLEVE-eksplosjon)		3,90	B	0,33	1,30

Figur 4.7 Beregninger på trussel-nivå (nivå 3)

Skårverdier for trusler fås ved å summere vektet skår for de fem fasene. For trussel 1 blir dette $0,44 + 0,46 + 0,55 + 0,50 + 0,68 = 2,64$. Dette tilsvarer resiliensnivå C siden skår 2,64 ligger mellom 2-3.

Trussel 1 er vektet likt med øvrige trusler, dvs. $1/3 = 0,33$. Vektet skår (skår multiplisert med vekt) blir for trussel 1 $2,64 \cdot 0,33 = 0,88$. Denne verdien tas videre til beregninger på neste nivå.

Figur 4.8 viser beregningene på kritisk infrastruktur-nivå (nivå 2).

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia	Trussel vektet skår	Kritisk infrastruktur: skår, vektor og RIL			
		KI skår	KI resiliens nivå	KI vekt	KI vektet skår
Område: Det sørlige industriområdet i byen Pančevo					
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer		3,06	B	1,00	3,06
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)	0,88				
Fase I - Forstå risikoene					
Fase II - Forberede/forutse					
Fase III - Absorbere/motstå					
Fase IV - Respondere/gjenvinne					
Fase V - Tilpasse/lære					
Trussel 2: Naturlige farer (flom i elva Donau)	0,88				
Trussel 3: Farer relatert til ny teknologi (BLEVE-eksplosjon)	1,30				

Figur 4.8 Beregninger på kritisk infrastruktur-nivå (nivå 2)

Skårverdier for kritisk infrastruktur fås ved å summere vektet skår for de tre truslene. For den kritiske infrastrukturen blir dette $0,88 + 0,88 + 1,30 = 3,06$. Dette tilsvarer resiliensnivå B siden skår 3,06 ligger mellom 3-4.

I dette eksempelet er det kun én kritisk infrastruktur i området, slik at vekten blir 1,0 (100 %). Vektet skår (skår multiplisert med vekt) blir dermed $3,06 \cdot 1,0 = 3,06$. Denne inngår i beregningene på område-nivå (nivå 1).

Figur 4.9 viser beregningene på område-nivå (nivå 1).

Eksempel fra kjemisk industri i Pancevo utenfor Beograd i Serbia	KI: skår, vekt og RIL			Område: skår og RIL	
	KI resiliens nivå	KI vekt	KI vektet skår	Område skår	Område resiliens nivå
Område: Det sørlige industriområdet i byen Pančevo				3,06	B
Kritisk infrastruktur: Kjemisk industri – Produksjon and lagring/prosessering av kjemiske stoffer	B	1,00	3,06		
Trussel 1: Terrorangrep (som leder til BLEVE-eksplosjon)					
Fase I - Forstå risikoene					
Fase II - Forberede/forutse					
Fase III - Absorbere/motstå					
Fase IV - Respondere/gjenvinne					
Fase V - Tilpasse/lære					
Trussel 2: Naturlige farer (flom i elva Donau)					
Trussel 3: Farer relatert til ny teknologi (BLEVE-eksplosjon)					

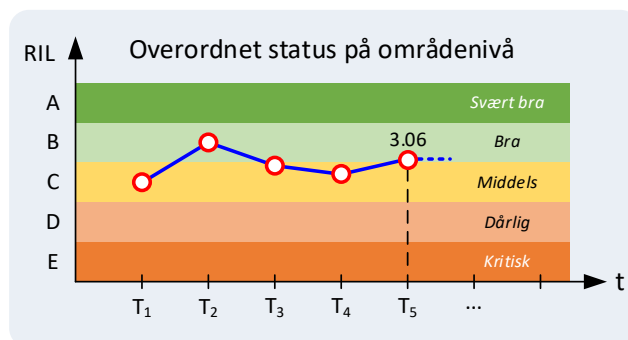
Figur 4.9 Beregninger på område-nivå (nivå 1)

I og med at det er kun én kritisk infrastruktur som inngår i området, blir skårverdien for område lik skårverdien for den kritiske infrastrukturen, dvs. 3,06, og resiliensnivået blir også det samme, det vil si RIL=B.

Dersom flere kritiske infrastrukturer hadde vært inkludert ville skårverdiene fra disse blitt vektet sammen for å gi skår (og RIL) på områdenivå. Man kunne da velge å vektlegge enkelte kritiske infrastrukturer mer enn andre, eller vekte dem helt likt.

Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.

Den overordnede statusen for området (som er identisk med den kritiske infrastrukturen) og utviklingen i forhold til tidligere år (trenden) er vist i figur 4.10.



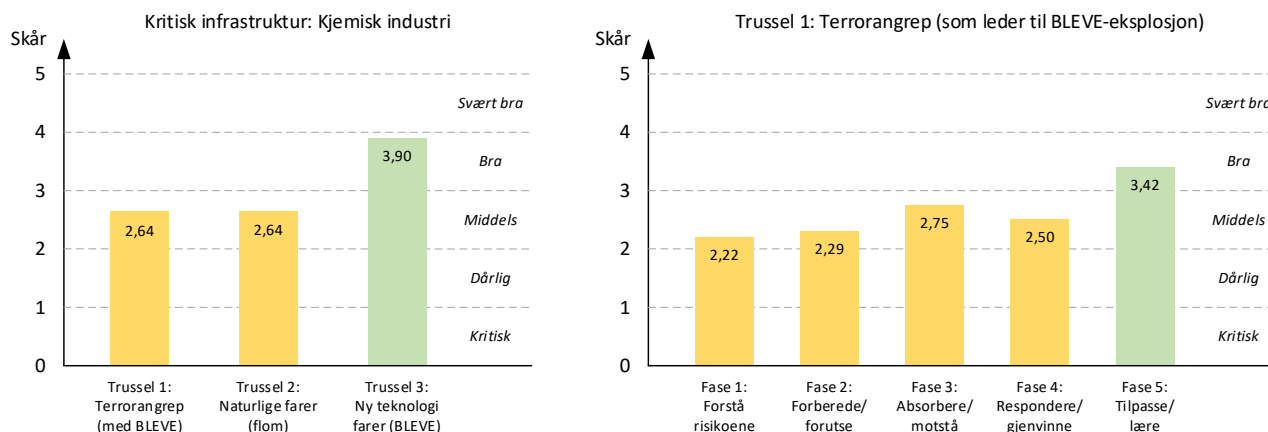
Figur 4.10 Status på område-nivå (nivå 1) – RIL og skår

Statusen er RIL = B ("bra"), med skår 3,06. Dette er bedre enn for de to foregående målingene (RIL=C), men noe lavere skår enn for tidspunkt T₂.

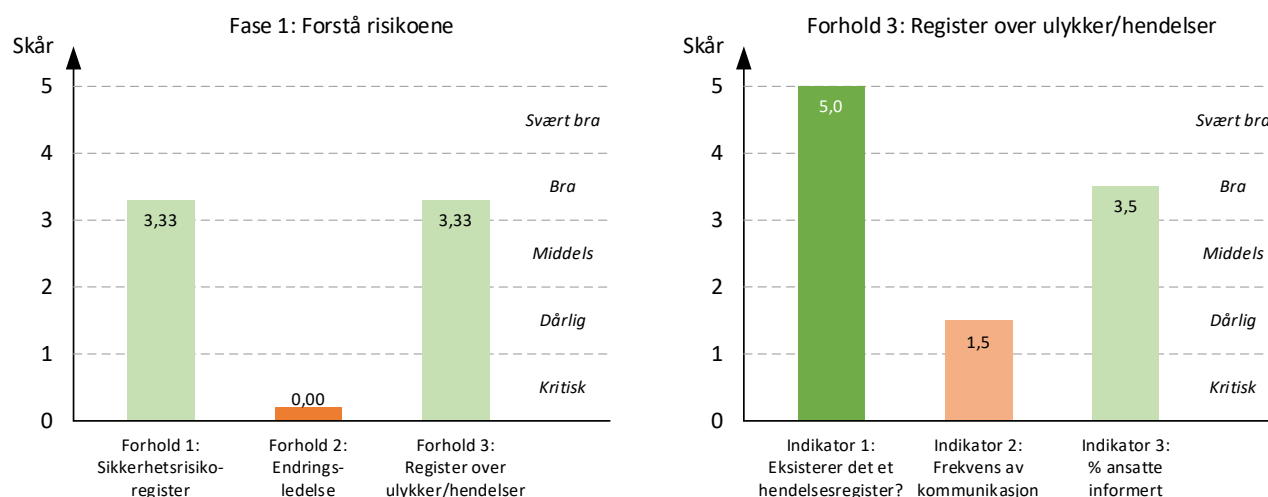
Dersom man vil se på underliggende resultater, kan man "bore seg nedover" nivå for nivå.

Figur 4.11 viser resultatene på trussel-nivå (nivå 3) – venstre side, og på fase-nivå (nivå 4) for trussel 1 – høyre side.

Figur 4.12 viser resultatene på forhold-nivå (nivå 5) for fase 1 for trussel 1 – venstre side, og på indikator-nivå (nivå 6) for forhold 3 for fase 1 for trussel 1 – høyre side.



Figur 4.11 Status på trussel-nivå (nivå 3) og fase-nivå (nivå 4)



Figur 4.12 Status på forhold-nivå (nivå 5) og indikator-nivå (nivå 6)

Tabell 4.3 viser resultater i form av en topp-fem og bunn-fem liste over forhold. Sistnevnte viser hvor forbedringsbehovet er mest prekært.

Tabell 4.3 "Topp-fem" og "bunn-fem" forhold

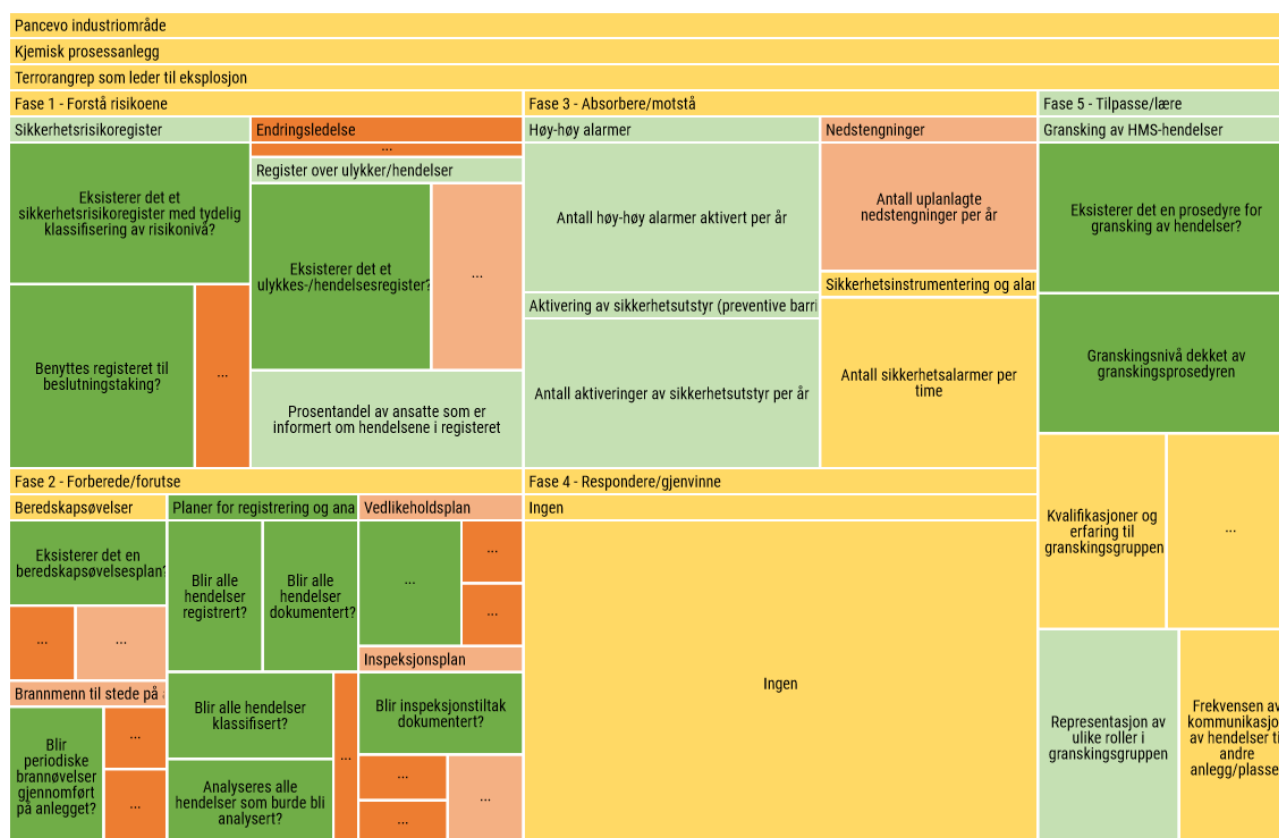
Topp-fem forhold	Skår	RIL	Bunn-fem forhold	Skår	RIL
1. Hendelsesanalyseplan	4,00	A	1. Endringsledelse	0,00	E
2. Høy-høy alarm	3,50	B	2. Nedstengninger	1,50	D
2. Aktivering av sikkerhetssystemer	3,50	B	3. Inspeksjonsplan	1,63	D
4. Gransking av hendelser	3,42	B	4. Vedlikeholdsplan	1,67	D
5. Sikkerhetsrisikoregister	3,33	B	5. Brannmenn ved anlegget	1,83	D

Tabell 4.4 viser en alternativ måte å presentere resultater for alle forholdene samlet på (for trussel 1).

Tabell 4.4 Status for alle forhold (for trussel 1)

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Forstå risikoene	Forberede/forutse	Absorbere/motstå	Respondere/gjenvinne	Tilpasse/lære
Sikkerhetsrisikoregister	Beredskapsøvelser	Høy-høy alarmer	(Ingen – medium skår)	Gransking av hendelser
Endringsledelse	Brannmenn til stede på anlegget	Aktivering av sikkerhetssystemer		
Hendelsesregister	Plan for registrering og analyse av hendelser	Nedstengninger		
	Vedlikeholdsplan	Sikkerhetsinstrumentering og alarmer		
	Inspeksjonsplan			

Ved bruk av trestruktur-diagrammet (TreeMap) i figur 2.3 kan man få frem et tilsvarende "varmekart" som dekker alle nivå samtidig (inkludert indikatorene). Dette er vist i figur 4.13. Dette er laget med bruk av web-verktøyet ResiliN ("Resiliensvurdering i Norge") for beregninger og visualisering beskrevet i vedlegg H.


Figur 4.13 Trestrukturdiagram laget med web-verktøyet ResiliN (se vedlegg H)

Tekst som mangler for noen indikatorer i figur 4.13 (...) fremkommer ved å holde musa over prikkene i web-verktøyet.

De største rektangelene har størst innvirkning på totalresultatet. (Fase 4 er fiktivt satt til medium, siden det her ikke var definert forhold eller indikatorer – "ingen").

4.2 Pandemi i Norge (covid-19)

Dette eksempelet bygger blant annet på Jovanović m.fl. (2020), hvor håndteringen av pandemien i 10 land ble vurdert og sammenliknet. Vurderingen av håndteringen i Norge ble gjennomført 5. april 2020. Eksempelet er spesielt ved at det ikke er en vurdering av en mulig fremtidig hendelse, slik som eksempelet i kapittel 4.1. Det er heller ikke en vurdering etter en hendelse, men en "underveis-vurdering".¹⁴

Kort om covid-19

Utbruddet av koronavirussykdom 2019 (covid-19) startet som en økning i antall personer med alvorlig lungebetennelse av ukjent årsak i storbyen Wuhan i Hubei-provinsen i Kina i desember 2019. Et nytt koronavirus, kalt SARS-CoV-2, ble identifisert av kinesiske helsemyndigheter 7. januar 2020 som årsak til utbruddet. Det ble starten på først en alvorlig lokal epidemi i Wuhan og siden en pandemi som har nådd Norge, Europa og alle kontinenter (FHI, 2020a).

Folkehelseinstituttet startet å teste for covid-19 23. januar 2020, og det første laboratoriebekreftede tilfellet i Norge ble påvist 26. februar 2020. De første sykdomstilfellene i Norge ble knyttet til smitte i utlandet. Det første tilfellet av innenlandssmitte uten kontakt med et bekreftet tilfelle ble identifisert 9. mars 2020. Første dødsfall i Norge ble rapportert 12. mars 2020 (FHI, 2020a). Per 5. april 2020 var det registrert 59 dødsfall i Norge og 68 976 dødsfall globalt (FHI, 2020b). Per 10. november 2020 er det registrert 285 dødsfall i Norge og 1,3 million dødsfall globalt (FHI, 2020c).

Hva visste vi på forhånd?

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal ha oversikt over risiko og sårbarhet i samfunnet (i Norge). I DSBs Analyser av Krisescenarioer (AKS) fra 2019 er det gjennomført risikoanalyser og sammenlikninger av 25 krisescenarioer. Scenarioet med størst risiko (relatert til sannsynlighet og konsekvens) er pandemi! Her står det blant annet *"Pandemi-scenarioet tar i grove trekk utgangspunkt i den verste influensapandemien vi kjenner, nemlig spanskesyken i 1918–19, men vi kan ikke se bort fra at den neste pandemien kan ha enda mer alvorlig karakter enn denne."* (DSB, 2019).

DSB var i sin analyse av pandemi (sist oppdatert i 2018) både optimistisk og pessimistisk. De har blant annet anslått en varighet på fire måneder (optimistisk) og 8 000 dødsfall (pessimistisk slik det nå ser ut).

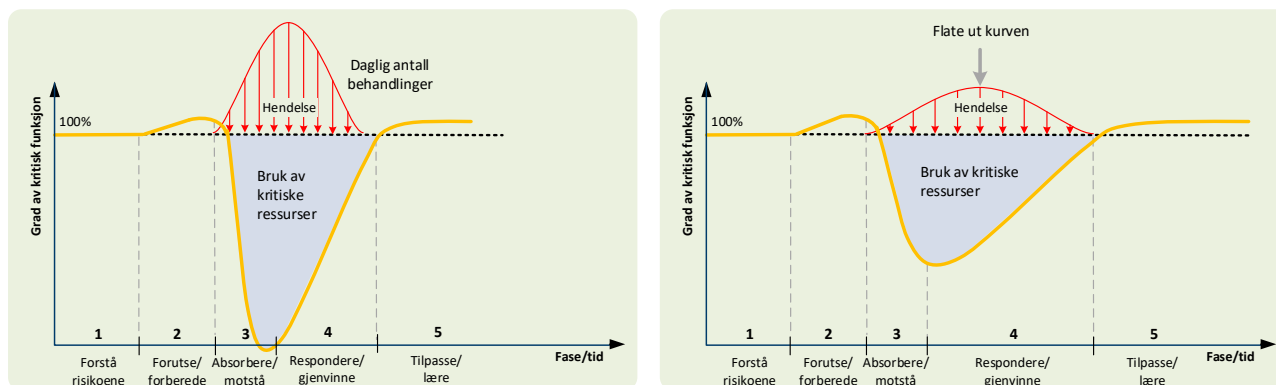
DSB benyttet i denne analysen en "pandemikalkulator" utviklet av FHI med utspring i data fra WHO (World Health Organization), som beregnet ca. 6 000 døde. Men, dette forutsetter at alle som trenger intensivbehandling, får det. *"Det er ikke mulig i dagens situasjon, da det vil bli mangel både på utstyr og behandlingspersonell. Også de som er syke og trenger intensivbehandling av andre årsaker, vil lide under samme kapasitetsmangel de fire månedene pandemien varer. Basert på dette oppjusteres antall døde fra rundt 6 000 til rundt 8 000 personer."* (DSB, 2019).

Et mål for håndteringen av pandemien, både i Norge og andre land, har nettopp vært å unngå å overbelaste helsevesenet, ved å "flate ut kurven" over antall daglige behandlinger (sykehusinnleggelser, intensivbehandling og respiratorbehandling) av covid-19-pasienter, som illustrert i figur 4.14.

En underliggende utfordring knyttet til mangel på utstyr og behandlingsskapasitet som gjelder så å si alle land i Europa er at helsevesenet ikke er bærekraftig. Det vil si at helsekostnader vokser vanligvis raskere enn nasjonale inntekter, noe som betyr at det på lang sikt bare er et begrenset sett med alternativer: man reduserer

¹⁴ Det kan senere være aktuelt å utvide eksempelet med flere forhold relevant for Norge, dekke hele 2020 og/eller gjøre vurderingen etter at pandemien er over.

enten medisinske tjenester som tilbys til befolkning eller kutter ned i andre sektorer, med mindre teknologisk utvikling reduserer fremtidig etterspørsel etter helsetjenester (Jovanovic m.fl., 2020).



Figur 4.14 Unngå overbelastning av helsevesenet ved å "flate ut kurven"

Som en konsekvens av dette blir helsetjenestesystemene stadig presset til å operere på maksimal kapasitet, for eksempel når det gjelder antall pasienter behandlet på sykehus og belegg av sykehussenger. Dersom helsevesenet allerede er nær sin maksimale kapasitet under en normalsituasjon, hvordan vil det kunne håndtere kriser som en pandemi? Hvilken grad av beredskap ønsker vi å ha mot ekstreme hendelser som en pandemi? Hvilken beredskap hadde vi mot pandemi? Hvor godt forberedt var vi? Hvor godt har vi håndtert pandemien? Hvor resiliente er vi?

Figur 4.14 viser også (en mulighet for) å øke kapasiteten på kritiske ressurser før viruset kom til Norge ("humpen" på kurven i fase 2), siden vi kjente til utbruddet i Kina. Det samme gjelder underveis i en langvarig hendelse som denne pandemien, samt etterpå (økning i kritiske ressurser etter hendelsen i fase 5). Utnyttet vi tiden godt nok fra utbruddet ble kjent og til vi ble rammet i Norge?

Avgrensning/begrensning

Her ser vi kun på de 18 forholdene og 40 indikatorene som de ansvarlige for studien hadde definert, og som hvert land ble bedt om å bedømme, i tillegg ble det benyttet 17 indikatorer som ble bedømt av de ansvarlige for studien (Jovanovic m.fl., 2020).

Noen av indikatorene vet vi nå bedre status på, også hvordan dette var før 5. april, og disse har blitt justert. Det er derfor flere grunner til at de tallene vi viser nå (for Norge) ikke samsvarer med de tallene som ble lagt til grunn i sammenlikningen mellom de 10 landene.

Trinn 1: Velg område

Området er hele Norge.

Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)

Det som her er valgt er helsetjenesten/helsevesenet som inngår i den kritiske samfunnsfunksjonen "helse og omsorg" (DSB, 2016), med tilhørende kritisk infrastruktur som sykehus og deres kapasiteter som intensiv-sengeposter, respiratorkapasitet, testkapasitet, osv.

Helse- og omsorgsdepartementet (HOD) er ansvarlig for den kritiske samfunnsfunksjonen "helse og omsorg" og har det overordnede ansvaret for å håndtere en pandemi i samarbeid med underliggende etater og den utøvende helse- og omsorgstjenesten. Denne rollen vil normalt delegeres til Helsedirektoratet fra krisen oppstår. Dette skjedde den 31. januar 2020. Dersom en pandemi skulle kreve tverrsektoriell innsats, vil HOD som fag-/lederdepartement få ansvar for krisehåndteringen på departementsnivå. Dette betyr at HOD blir ansvarlig for å koordinere arbeidet med andre departementer og sektorer. Helsedirektoratet og FHI har viktige roller som myndighets- og fagorganer på sentralt nivå (Helsedirektoratet, 2020).

HOD har løpende og tett kontakt med WHO og samarbeider også med andre europeiske land, blant annet gjennom EUs helse-sikkerhetskomite (HSC).

Justis- og beredskapsdepartementet er ut over sitt sektoransvar tillagt en samordningsrolle for å sikre en helhetlig og koordinert beredskap i sivil sektor, og regjeringen som kollegium har det øverste ansvaret for den nasjonale beredskapen og håndteringen av hendelser som rammer samfunnet.

Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene

Koronapandemien.

Trinn 4: Vurder hver fase for hver fare/trussel/hendelse

Her er koronapandemien vurdert for hver av fasene. Det som vurderes i hver av fasene er hvilke forhold som er viktig for å håndtere koronapandemien (trinn 5) og deretter hvordan disse forholdene kan måles med indikatorer (trinn 6).

Trinn 5: Velg forhold for hver fase

Hvilke forhold er viktig for å håndtere koronapandemien? HVA er viktig? HVA er viktig for å forstå risikoene (fase 1), forberede/forutse (fase 2), absorbere/motstå (fase 3), respondere/gjenvinne (fase 4) og tilpasse/lære (fase 5) av koronapandemien?

Tabell 4.5 viser de forhold som ble valgt i månedsskiftet mars-april 2020 i studien som sammenliknet 10 land (Frankrike, Israel, Italia, Kina, Norge, Sveits, Sør-Afrika, Sør-Korea, Tyskland og Østerrike). USA var også med i studien, men er ikke tatt med i sammenlikningen.

Tabell 4.5 Valgte forhold for de ulike fasene

Fase		Forhold
1	Forstå risikoene <i>Gjør virksomheten* nok for å forstå risikoen?</i>	Studier Erfaring
2	Forberede/forutse <i>Forutser virksomheten godt nok hva som kan inntreffe, og forbereder den seg godt nok på trusler og andre uønskede hendelser?</i>	Intensivutstyr Reiseanbefalinger Relevante lover og forskrifter Grenser/flyplasser Økonomiske program
3	Absorbere/motstå <i>Har virksomheten gjennom aktive grep økt sin evne til å stå imot og håndtere kjente og ukjente ekstreme påkjenninger?</i>	Grenser/transport Økonomiske tiltak/program Fjernarbeid Produksjonstilpasning av industri til medisinsk utstyr Utdanning Medisinske ressurser Prioritering ("triage") Sporing med app Sosial distansering Begrensning av reiser og karantene Intensivutstyr
4	Respondere/gjenvinne <i>Har virksomheten kapasitet og evne til rask respons og evnen til å komme seg raskt på fote igjen etter ekstremhendelsen?</i>	Fjerning av sosial distansering Økonomisk gjenoppretting Økonomisk stimulering Grenseåpning
5	Tilpasse/lære <i>Evner virksomheten å lære i etterkant?</i>	Pandemiplaner Økonomiske læringspunkter Evaluerings av sosiale tiltak

* Virksomheten – myndighetene/helsemyndighetene/helsevesenet

Man valgte å begrense seg til de tre første fasene, selv om det er glidende overgang mellom å motstå i fase 3 og respondere i fase 4.

Det ble valgt ut 18 forhold av de ansvarlige for studien for bedømmelse av det enkelte land (i tillegg ble noen forhold bedømt av de ansvarlige for studien for alle landene). Dette utvalget av forhold kan selvsagt diskuteres. Det gjelder både representativitet for Norge (hvorvidt andre forhold burde vært valgt i stedet for eller i tillegg til disse) og innplassering i fase.

Trinn 6: Velg indikatorer for hvert forhold

HVORDAN måler vi disse viktige forholdene, ved hjelp av indikatorer (ja/nei spørsmål, antall, andeler, frekvenser, osv.)? Hvilke indikatorer er relevante for de ulike forholdene (én eller flere per forhold)?

I likhet med forholdene, så ble indikatorene definert av de ansvarlige for studien. Av disse ble 40 bedømt av det enkelte land. Disse er vist i tabell 4.6. I tillegg ble 17 indikatorer bedømt av de ansvarlige for studien, for alle landene. Dessuten var det tatt med noen indikatorer i starten, men som det var ikke mulig å skaffe data for eksempelvis antall leger og medisinsk personell som ble smittet eller døde.

I likhet med utvelgelsen av forhold kan også utvelgelsen av indikatorer selvsagt diskuteres.

Tabell 4.6 Valgte indikatorer for hvert forhold

Fase	Forhold	Indikatorer
1	Forstå risikoene	Studier
		Er det noen studier/undersøkelser om temaet pandemier og deres innvirkninger gjort av eller brakt til myndighetenes oppmerksomhet? Hvor mange studier/forskning ble inkludert i den statlige risikoanalysen? (<i>I prosent av totale studier tilgjengelig for undersøkelse av det relevante nasjonale ansvarlige organet (f.eks. nasjonal sikkerhetskomité, etc.)</i>)
	Erfaring	Har landet tidligere erfart lignende situasjoner/hendelser, og ble nødvendige tiltak iverksatt for å være bedre forberedt på fremtidige hendelser?
2	Forberede/forutse	Intensivutstyr
		Ble det tatt hensyn til en pandemi ved kjøp av sykehus-/intensivutstyr og materiell? (<i>For et tilfelle av pandemi på nasjonalt nivå, hvor balansering mellom sykehus er nødvendig.</i>)
		Tar de tilgjengelige mengdene med medisinsk personlig utstyr i betraktning ekstraordinær arbeidsmengde? (<i>Dekning av tilgjengelig medisinsk personlig utstyr, inkludert masker og annet beskyttelsesutstyr for alt utsatt personell, beregnet som prosent av personell med nevnt utstyr av det totale utsatte personellet.</i>)
		Reiseanbefalinger
		Er det prosedyrer på plass for å gi reiseanbefalinger/begrensninger?
		Relevante lover og forskrifter
		Finnes det en lov/forskrift i landet som styrer pandemier og tilhørende risikoer? (<i>Pandemispesifikke lover eller forskrifter eller andre gjeldende lover.</i>)
		Støtter forordningen tiltak som reisebegrensninger, stenging av grenser og personlig karantene?
3	Absorbere/motstå	Er det mekanismer på plass for raskt å vedta lover som gir myndighetene muligheten til å treffe tiltak for best å redusere hendelsen? (<i>F.eks. erklære krigsrett, unntakstilstand eller andre alternativer.</i>)
		Grenser/flyplasser
		Er det en prosedyre på plass for å håndtere karantene langs grensepassasjene?
		Er grensekontrollpersonell utstyrt for å håndtere smittetilfeller ved grensen? (<i>Eller annen ansvarlig myndighet?</i>)
		Økonomiske program
		Er det en statlig økonomisk støtteordning på plass? (<i>Godkjent med klare betingelser for aktivisering.</i>)
		Grenser/transport
		Hvor effektivt kan grensene stenges? (<i>Inkluderer land, sjø og flyreiser gjennom både anerkjente og andre passasjer. Mål på tid for beslutning og tid til å utføre.</i>)
		Er det tilført tilstrekkelig personell for å opprettholde den lukkede grensen? (<i>Grensekontrollpersonell utsettes for pandemien, vurder om mengden tilgjengelig personell er tilstrekkelig gitt sannsynligheten for smitte.</i>)
		I hvilken grad er det kuttet i offentlig transport for å støtte reisebegrensningene? (<i>Utvidelse av bevegelsesbegrensning. Flyreiser, tog, offentlig transport.</i>)
		Økonomiske tiltak/program
		Hvor lang tid tar det å vedta det statlige programmet for økonomisk støtte?
		Hva er omfanget av det statlige støtteprogrammet? (<i>Hvor stort budsjett tildeles i forhold til forventet økonomisk tap?</i>)
		Fjernarbeid
		I hvilken grad er støtteinfrastruktur tilgjengelig for fjernarbeid?
		Støttes fjernarbeid generelt av myndighetene?

Fase	Forhold	Indikatorer
	Produksjons-tilpasning av industri til medisinsk utstyr	Hvor lett imøtekommer de nasjonale industrilederne de nye produksjonskravene? (<i>Kreves det statlig inngripen i markedet (motstand) eller mobiliserer industrien seg selv (initiativ)?</i>)
		Endrer industrien produksjonen for å møte dagens utstyrskrav?
		I hvilken grad tilbyr industrien frivillig egen serverkapasitet for å sørge for sikre nettverk osv.?
	Utdanning	I hvilken grad er landet forberedt på nettkurs/hjemmeskole (infrastruktur, utstyr, etc.)?
		I hvilken grad brukes alternative utdanningsmodeller?
	Medisinske ressurser	Hvor mange ekstra medisinske støtteressurser forventes å bli mobilisert under hendelsen? (<i>I hvilken grad pensjonister, medisinstudenter eller sosialarbeidere vil benyttes for å understøtte helsesystemet.</i>)
		Hvor lang tid tar det å mobilisere ytterligere medisinske ressurser, og er det veiledende prosedyrer på plass?
		Hvor lang tid tar det å etablere flere første-responssentre/sykehus, og er det støttetiltak/prosedyrer på plass?
		I hvilken grad oppfyller den tilgjengelige "virustestings-kapasiteten" kravene?
	Prioritering ("triage")	Hvor ofte og i hvilken grad kreves prioritering/sortering under operasjon? (<i>Er det allerede satt opp triage-kategorier (f.eks. aldersgrupper)? Hvor mange daglige tilfeller er rapportert å ha vært utsatt for triage?</i>)
	Sporing med app	Er apper tilgjengelige for å spore bevegelse/kontakt mellom innbyggere? (<i>Sporing kan enten gjøres gjennom spesielle apper eller lokalisering av mobil. Er det obligatorisk å tillate sporing, eller brukes den på frivillig basis, eller er den ikke tilgjengelig i det hele tatt?</i>)
		Er samarbeid med mobilnettleverandører på plass for å samle inn og analysere stedsdata?
		Hvor mye av befolkningen dekkes av appsporing?
	Sosial distansering	I hvilken grad kreves det portforbud for å begrense pandemien? (<i>Begrensning av offentlige tjenester og offentlig liv (enhver aktivitet i grupper).</i>)
		Hvor mye forventes samfunnet å rette seg etter portforbud og/eller påkrevd sosial distansering?
	Begrensning av reiser og karantene	Hvor raskt og effektivt kan reisebegrensninger iverksettes? (<i>Hvor rask er beslutningen om å begrense reiser og hvor streng kan håndhevelsen være?</i>)
		Hvor raskt og omfattende blir karanteneinstrukser brukt og håndhevet på reisende fra risikoområder? (<i>Hvor rask er beslutningen om å sette returnerende statsborgere fra risikoregioner i karantene?</i>)
		Hvor raskt og omfattende blir karanteneinstruksjoner brukt og håndhevet for smittetilfeller i lokalsamfunnet?
		I hvilken grad er bevegelsen til enkeltpersoner begrenset innen deres egen by? (<i>Er det mulig å bevege seg fritt hvis man respekterer de sosiale distanseringsreglene?</i>)
	Intensivutstyr	Er det en prosess på plass for å muliggjøre oppskalering av tilgjengeligheten av utstyr? (<i>Er det avtaler med leverandørene om å levere ekstra utstyr innen foreskrevet tid? Var budsjett bevilget for dette?</i>)

Fase	Forhold	Indikatorer
		Hvor pålitelig er levering av nødvendig medisinsk utstyr til den angitte mottakeren? (<i>Evaluer presisjonen og leveringstid ved levering av nødvendig utstyr.</i>)
4	Respondere/ gjenvinne	
5	Tilpasse/lære	

Trinn 7: Fastsett grenseverdiene for hver indikator og angi vekt

I likhet med valg av forhold og definering av indikatorer ble grenseverdiene for hver indikator fastsatt av den ansvarlige for studien. Grenseverdiene er vist i tabell 4.7. Det ble benyttet lik vekt på alle nivå.

(Valgt måleverdi, som utgjør trinn 8, er lagt inn som blått tall ytterst i siste kolonne, for å slippe gjentak av tabellen under trinn 8).

Tabell 4.7 Grenseverdier for indikatorene

Fase	Forhold	Indikatorer	Grenseverdier og skår
1	Forstå risikoene	Studier	Er det noen studier/undersøkelser om temaet pandemier og deres innvirkninger gjort av eller brakt til myndighetenes oppmerksomhet?
			Ja/Nei (5/0)
			5
		Hvor mange studier/forskning ble inkludert i den statlige risikoanalysen? (<i>I prosent av totale studier tilgjengelig for undersøkelse av det relevante nasjonale ansvarlige organet (f.eks. nasjonal sikkerhetskomité, etc.)</i>)	0 – NA 1 – 0% 3 – 1% 5 – 5%
			4
		Erfaring	Har landet tidligere erfart lignende situasjoner/hendelser, og ble nødvendige tiltak iverksatt for å være bedre forberedt på fremtidige hendelser?
2	Forberede/forutse		Ja/Nei (5/0)
			5
		Intensivutstyr	Ble det tatt hensyn til en pandemi ved kjøp av sykehus-/intensivutstyr og materiell? (<i>For et tilfelle av pandemi på nasjonalt nivå, hvor balansering mellom sykehus er nødvendig.</i>)
			Ja/Nei (5/0)
			5
		Tar de tilgjengelige mengdene med medisinsk personlig utstyr i betraktning ekstraordinær arbeidsmengde? (<i>Dekning av tilgjengelig medisinsk personlig utstyr, inkludert masker og annet beskyttelsesutstyr for alt utsatt personell, beregnet som prosent av personell med nevnt utstyr av det totale utsatte personellet.</i>)	1 – mindre enn 50% 3 – mindre enn 90% 5 – 100%
			5
		Reise-anbefalinger	Er det prosedyrer på plass for å gi reiseanbefalinger/begrensninger?
			Ja/Nei (5/0)
			5
		Relevante lover og forskrifter	Finnes det en lov/forskrift i landet som styrer pandemier og tilhørende risikoer? (<i>Pandemispesifikke lover eller forskrifter eller andre gjeldende lover.</i>)
			Ja/Nei (5/0)
			5
		Støtter forordningen tiltak som reisebegrensninger, stenging av grenser og personlig karantene?	Ja/Nei (5/0)
			5
		Er det mekanismer på plass for raskt å vedta lover som gir myndighetene muligheten til å treffe tiltak for best å redusere hendelsen? (<i>F.eks. erklære krigsrett, unntaks-tilstand eller andre alternativer.</i>)	Ja/Nei (5/0)
			5
		Grenser/flyplasser	Er det en prosedyre på plass for å håndtere karantene langs grensepassasjene?
			Ja/Nei (5/0)
			5
		Er grensekontrollpersonell utstyrt for å håndtere smittetilfeller ved grensen? (<i>Eller annen ansvarlig myndighet?</i>)	0 – ikke noe utstyr 1 – basisutstyr 3 – basisutstyr + mulighet for spesialutstyr 5 – fullt utstyrt
			0

Fase		Forhold	Indikatorer	Grenseverdier og skår
		Økonomiske program	Er det en statlig økonomisk støtteordning på plass? <i>(Godkjent med klare betingelser for aktivering.)</i>	0 – ingen program 1 – basisstøtteprogram 3 – ... 5 – fullt program tilgjengelig og klart til bruk på kort varsel 5
3	Absorbere/ motstå	Grenser/ transport	Hvor effektivt kan grensene stenges? <i>(Inkluderer land, sjø og flyreiser gjennom både anerkjente og andre passasjer. Mål på tid for beslutning og tid til å utføre.)</i>	1 – lang prosess og beslutning nødvendig 3 – beslutning tar lang tid, men implementering er rask 5 – raskt og effektivt 5
			Er det tilført tilstrekkelig personell for å opprettholde den lukkede grensen? <i>(Grensekontrollpersonell utsettes for pandemien, vurder om mengden tilgjengelig personell er tilstrekkelig gitt sannsynligheten for smitte.)</i>	Ja/Nei (5/0) 5
			I hvilken grad er det kuttet i offentlig transport for å støtte reisebegrensningene? <i>(Utvidelse av bevegelsesbegrensning. Flyreiser, tog, offentlig transport.)</i>	1 – redusert frekvens, men ellers ingen store kutt 3 – fly og langdistanse transport er drastisk redusert 5 – all offentlig transport er drastisk redusert 3
		Økonomiske tiltak/program	Hvor lang tid tar det å vedta det statlige programmet for økonomisk støtte?	1 – lang prosess og sen implementering 3 – beslutningsprosess rask, implementering forsinket 5 – program aktiveres automatisk i stor skala raskt 4
			Hva er omfanget av det statlige støtteprogrammet? <i>(Hvor stort budsjett tildeles i forhold til forventet økonomisk tap?)</i>	% av forventet tap 4
			Fjernarbeid	I hvilken grad er støtteinfrastruktur tilgjengelig for fjernarbeid?
		Støttes fjernarbeid generelt av myndighetene?		Ja/Nei (5/0) 5
		Produksjons-tilpasning av industri til medisinsk utstyr	Hvor lett imøtekommer de nasjonale industrilederne de nye produksjonskravene? <i>(Kreves det statlig inngripen i markedet (motstand) eller mobiliserer industrien seg selv (initiativ)?)</i>	1 – full motstand 3 – ingen motstand, men heller ingen initiativ 5 – fullt samarbeid 4
			Endrer industrien produksjonen for å møte dagens utstyrskrav?	Ja/Nei (5/0) 5
			I hvilken grad tilbyr industrien frivillig egen serverkapasitet for å sørge for sikre nettverk osv.?	1 – full motstand 3 – ingen motstand, men heller ingen initiativ 5 – fullt samarbeid 3
		Utdanning	I hvilken grad er landet forberedt på nettkurs/hjemmeskole (infrastruktur, utstyr, etc.)?	1 – veldig lite nettbasert skolegang tilgjengelig, hjemmeskole med foreldre 3 – nettbasert skolegang delvis tilgjengelig, eller blir utvidet 5 – nettbasert skolegang fullt tilgjengelig 4
			I hvilken grad brukes alternative utdanningsmodeller?	1 – bare for høyere nivå (f.eks. videregående skole)

Fase	Forhold	Indikatorer	Grenseverdier og skår
			3 – for alle skoler, men ikke barnehager 5 – all barneomsorg/utdanning gjøres eksternt 3
	Medisinske ressurser	Hvor mange ekstra medisinske støtteressurser forventes å bli mobilisert under hendelsen? (<i>I hvilken grad pensjonister, medisinstudenter eller sosioarbeidere vil benyttes for å understøtte helsesystemet.</i>)	0 – ikke mobilisert 1 – noe er mobilisert på spesielle områder 3 – frivillige mobilisert på noen områder 5 – obligatoriske tjenester er planlagt for medisinsk støtte 4
		Hvor lang tid tar det å mobilisere ytterligere medisinske ressurser, og er det veiledende prosedyrer på plass?	1 – ingen prosedyrer, lang mobiliseringstid 3 – delvis kort mobiliserings- tid og støttende prosedyrer 5 – kort mobiliseringstid og støttende prosedyrer 4
		Hvor lang tid tar det å etablere flere første-respons-sentre/sykehus, og er det støttetiltak/prosedyrer på plass?	1 – ingen prosedyrer/planer tilgjengelig 3 – planer tilgjengelig, lang implementeringstid 5 – planer tilgjengelig og rask implementering 4
		I hvilken grad oppfyller den tilgjengelige "virustestings-kapasiteten" kravene?	1 – ikke tilstrekkelig test-kapasitet (kun spesielt personell kan testes) 3 – testkapasitet til å teste alle personer med symptomer 5 – full nasjonal dekning av testing tilgjengelig 2
	Prioritering ("triage")	Hvor ofte og i hvilken grad kreves prioritering/sortering under operasjon? (<i>Er det allerede satt opp triage-kategorier (f.eks. aldersgrupper)? Hvor mange daglige tilfeller er rapportert å ha vært utsatt for triage?</i>)	0 – ingen kategorier tilgjengelig 1 – nødvendig på daglig basis 3 – sjeldent nødvendig 5 – tilgjengelig men ikke nødvendig 5
	Sporing med app	Er apper tilgjengelige for å spore bevegelse/kontakt mellom innbyggere? (<i>Sporing kan enten gjøres gjennom spesielle apper eller lokalisering av mobil. Er det obligatorisk å tillate sporing, eller brukes den på frivillig basis, eller er den ikke tilgjengelig i det hele tatt?</i>)	0 – ikke tilgjengelig 1 – tilgjengelig, men på frivillig basis 3 – tilgjengelig og obligatorisk for smittede 5 – obligatorisk for alle 0
		Er samarbeid med mobilnettleverandører på plass for å samle inn og analysere stedsdata?	Ja/Nei (5/0) 0
		Hvor mye av befolkningen dekkes av appsporing?	0 – ingen appsporing tilgjengelig 1 – 20% av befolkningen 3 – 60 % av befolkningen 5 – hele befolkningen 0
	Sosial distansering	I hvilken grad kreves det portforbud for å begrense pandemien? (<i>Begrensning av offentlige tjenester og offentlig liv (enhver aktivitet i grupper).</i>)	0 – ingen begrensning 1 – restriksjoner for store arrangementer 3 – begrensning av det offentlige liv (stengte restauranter, osv.) 5 – fullt portforbud 3

Fase	Forhold	Indikatorer	Grenseverdier og skår
		Hvor mye forventes samfunnet å rette seg etter portforbud og/eller påkrevd sosial distansering?	0 – ikke i det hele tatt 1 – kun smittede personer 3 – risikogrupper 5 – fullstendig 4
	Begrensning av reiser og karantene	Hvor raskt og effektivt kan reisebegrensninger iverksettes? (<i>Hvor rask er beslutningen om å begrense reiser og hvor streng kan håndhevelsen være?</i>)	1 – lang prosess fra anbefaling til begrensning 3 – kort prosess, men lang implementeringstid 5 – raskt og effektivt 5
		Hvor raskt og omfattende blir karanteneinstrukser brukt og håndhevet på reisende fra risikoområder? (<i>Hvor rask er beslutningen om å sette returnerende statsborgere fra risikoregioner i karantene?</i>)	1 – frivillig hjemmekarantene 3 – hjemmekarantene uten kontroll 5 – karantene og regelmessig kontroll og bøter 3
		Hvor raskt og omfattende blir karanteneinstruksjoner brukt og håndhevet for smittetilfeller i lokalsamfunnet?	1 – hjemmekarantene uten kontroll 3 – hjemmekarantene med regelmessig kontroll 5 – hjemmekarantene med regelmessig helsesjekk + kontroll + bøter 4
		I hvilken grad er bevegelsen til enkeltpersoner begrenset innen deres egen by? (<i>Er det mulig å bevege seg fritt hvis man respekterer de sosiale distanseringsreglene?</i>)	1 – ingen restriksjoner hvis sosial distansering benyttes 3 – bevegelse tillatt kun til bestemte steder (apotek, matvarebutikker) 5 – ingen bevegelse tillatt uten spesialtillatelse 1
	Intensivutstyr	Er det en prosess på plass for å muliggjøre oppskalering av tilgjengeligheten av utstyr? (<i>Er det avtaler med leverandørene om å levere ekstra utstyr innen foreskrevet tid? Var budsjett bevilget for dette?</i>)	Ja/Nei (5/0) 5
		Hvor pålitelig er levering av nødvendig medisinsk utstyr til den angitte mottakeren? (<i>Evaluer presisjonen og leveringstid ved levering av nødvendig utstyr.</i>)	1 – fullstendig upålitelig 3 – noe pålitelig 5 – pålitelig 4
4	Respondere/ gjenvinne		
5	Tilpasse/lære		

Det er noen (13) ja/nei-spørsmål, men mest brukt er en kvalitativt indikert skala, enten fra 0-5 eller 1-5. Selv om skår 2 og 4 ikke er kvalitativt beskrevet kan også disse benyttes.

Preferansen for enkelte av tiltakene vil naturligvis variere fra land til land på grunn av for eksempel politisk, kulturell, sosial, økonomisk og andre forskjeller. Valg av grenseverdier og tilhørende skår kan derfor diskuteres. Effekt på smittespredning er i mange tilfeller satt over personvern og demokratiske verdier. Dette er selvsagt ikke like akseptabelt og dermed gjennomførbart i alle land.

Trinn 8: Angi måleverdier for indikatorene (utfør målingen)

Selve målingen og angivelse av skår er lagt inn i tabell 4.8, ytterst i siste kolonne (blå tall), for å unngå å gjenta hele tabellen.

Selve målingen (for Norge) ble gjennomført av én person, og med begrenset tid til rådighet (3.-5. april 2020). Vurderingen baserte seg blant annet på de 90 tiltakene som regjeringen hadde iverksatt frem til 5. april, slik

det fremgår av tabell 4.8. Dette er hentet fra tidslinjen over myndighetenes håndtering av koronasituasjonen presentert på Regjeringen.no (Regjeringen, 2020b).

Tabell 4.8 Tiltak iverksatt av regjeringen frem til 5. april 2020

Dato	Tiltak
30.01	Koronaviruset og norske myndigheters arbeid
31.01	Delegert myndighet i forbindelse med koronavirus-utbruddet Koronavirus blir meldepliktig sykdom og defineres som allmennfarlig smittsom sykdom
14.02	Norge bidrar i arbeidet med å bekjempe koronaviruset covid-19
28.02	Vedtar hjemmel for å sikre tilgang til nødvendige legemidler og utstyr
04.03	Fraværsgrensen endres som følge av koronaviruset
06.03	Helsedirektoratet får fullmakt til å sikre helsehjelp
10.03	Strakstiltak for å bøte på de økonomiske konsekvensene av korona
11.03	Norske borgere kan møte nye innreisetiltak i andre land Dekning av tap og utgifter som følge av koronautbruddet
12.03	Omfattende tiltak for å bekjempe koronaviruset Nok mat til alle Rettigheter ved stengte skoler og barnehager
13.03	Motsyklisk kapitalbuffer settes ned Utsatt betaling av forskuddsskatt Pressekonferanse om økonomiske tiltak Bedre tilgang til smittevernutstyr Regjeringens strakstiltak for å dempe de økonomiske virkningene av koronaviruset Helsepersonell som driver pasientbehandling forbys midlertidig å reise utenlands Matproduksjonen går som normalt Utgifter knyttet til koronavirusutbruddet Foreslår endringer i permitteringsregelverket Krevende for norske kommuner Reiseråd for USA og Frankrike
14.03	Fraråder reiser som ikke er strengt nødvendige til alle land Regjeringen stanser ankomster av nye overføringsflyktninger Ny forskrift om karantene etter reiser utenfor Norden Frivilligheten beholder statlige tilskudd Innfører strengere grensekontroll Presisering fra norske myndigheter: Norske flyplasser stenger ikke
15.03	Flere tiltak for å sikre at jordbruksproduksjon går som normalt All godstrafikk kan gå som normalt Regjeringen kan forby opphold på fritidseiendommer og fastsetter tydelige regler for karantene og isolasjon 100 milliarder i garantier og lån for å hjelpe kriserammede bedrifter
16.03	COVID-19 utbruddet og anskaffelsesregelverket Mulighet for større fleksibilitet i arbeidstid Liste over kritiske samfunnsfunksjoner fastsatt Trapper opp legemiddelberedskapen i Norge
17.03	Lokale regler må ikke hindre samfunnsfunksjoner Foreldre slepp å betale for barnehage og SFO Nordisk samarbeid for å hjelpe nordiske statsborgere Nye nasjonale retningslinjer for dagligvarebransjen Regjeringen samarbeider med flyselskapene om å bistå nordmenn på reise med å komme hjem Oppfordrer helsetjenesten til å bruke videokonsultasjon Utenlandske borgere som ikke har symptomer på koronasmitte kan forlate Norge
18.03	Stor kompensasjonsordning til kultur, frivillighet og idrett Lettere for pensjonert personell i helsesektoren å jobbe

Dato	Tiltak
	Ny koronalov Norge mobiliserer til vaksinedugnad Varsler ekstraordinære koronatiltak for sjømatnæringen
19.03	250 millioner kroner ekstra til kommunene i 2020 Innfører hytteforbud Omfattende tiltakspakke for norsk luftfart: 6 milliarder i lånegaranti
20.03	Foreldres rett til omsorgspenger doubles Slik blir endringene i permitterings- og dagpengeregelverket Nye regler om koronarelatert sykefravær og egenmelding Garanti- og låneordninger for bedre likviditet i bedriftene Betydelig fall i aktiviteten og kraftfulle økonomiske grep Regjeringen foreslår flere tiltak for å trygge arbeidsplassene Regjeringen vil sikre kapasitet i NAV
22.03	Fjerner egenandel for hjelpeorganisasjoner
23.03	Norge tar initiativ til nytt koronafond i FN Nye koronatiltak for å bedre likviditeten til norske bedrifter Midlertidig økt fleksibilitet i boliglånforskriften
24.03	Tiltakene mot koronavirus videreføres
25.03	Koronapandemien: Regjeringen styrker den humanitære innsatsen Lettere å få smittevernutstyr til Norge Nedsettelse av en ekspertgruppe for samfunnsøkonomisk vurdering av smitteverntiltak m.v – Covid-19
26.03	Noreg bidreg med over 14 millioner kroner til Malawis respons på covid-19 50 millioner kroner til kompetanseutvikling for å hindre permitteringer og oppsigelser
27.03	Vil dekke faste kostnader for å redde arbeidsplasser Oppdaterte regler om koronarelatert sykefravær og egenmelding Nye tiltak for å dempe de økonomiske virkningene av koronavirusutbruddet Helsefritak under koronapandemien Ny tiltakspakke for næringslivet: Skal hjelpe landets gründere og vekstbedrifter gjennom krisen Norge øker bistanden til vaksineutvikling med 2,2 milliarder kroner
28.03	Regjeringen viderefører tiltakene som er iverksatt for å bekjempe utbruddet av koronavirus
29.03	Regjeringen legger frem veileder om bruk av kommunale karantene- og innreiseregler
30.03	Innreisemuligheter for EØS-borgere
31.03	Garantiordningen for norsk luftfart er operativ Forlenger samarbeidet med flyselskapene og reiseselskapene for å få nordmenn hjem Norsk pandemiregister er opprettet og i drift i rekordfart Norge bidrar til FNs nye koronafond for global innsats
01.04	Intens innsats for å hjelpe nordmenn på reise hjem til Norge
02.04	Rekordstor avtale med Kirkens Nødhjelp for kampen mot fattigdom Garantiordningen åpnes for større bedrifter Utenriksdepartementet trapper opp støtten til internasjonal koronaforskning Foretak med minst 30 % omsetningsfall kan få kompensasjon
03.04	Utenriksdepartementet opprettholder reiserådet fra 14. mars Koronatiltak for fiskerieringen

Videre ble ukesrapportene til FHI frem til 5. april 2020 gjennomgått (dette gjaldt uke 11, 12 og 13 i 2020), og alle pressekonferanser holdt av medlemmer av regjeringen samt helsedirektoratet og FHI. I tillegg ble hjemmesidene til regjeringen, helsedirektoratet og FHI benyttet, samt nasjonal beredskapsplan for pandemisk influensa. Kildehenvisning ble gitt til hver indikatorskår, hvor relevante kilder fantes.

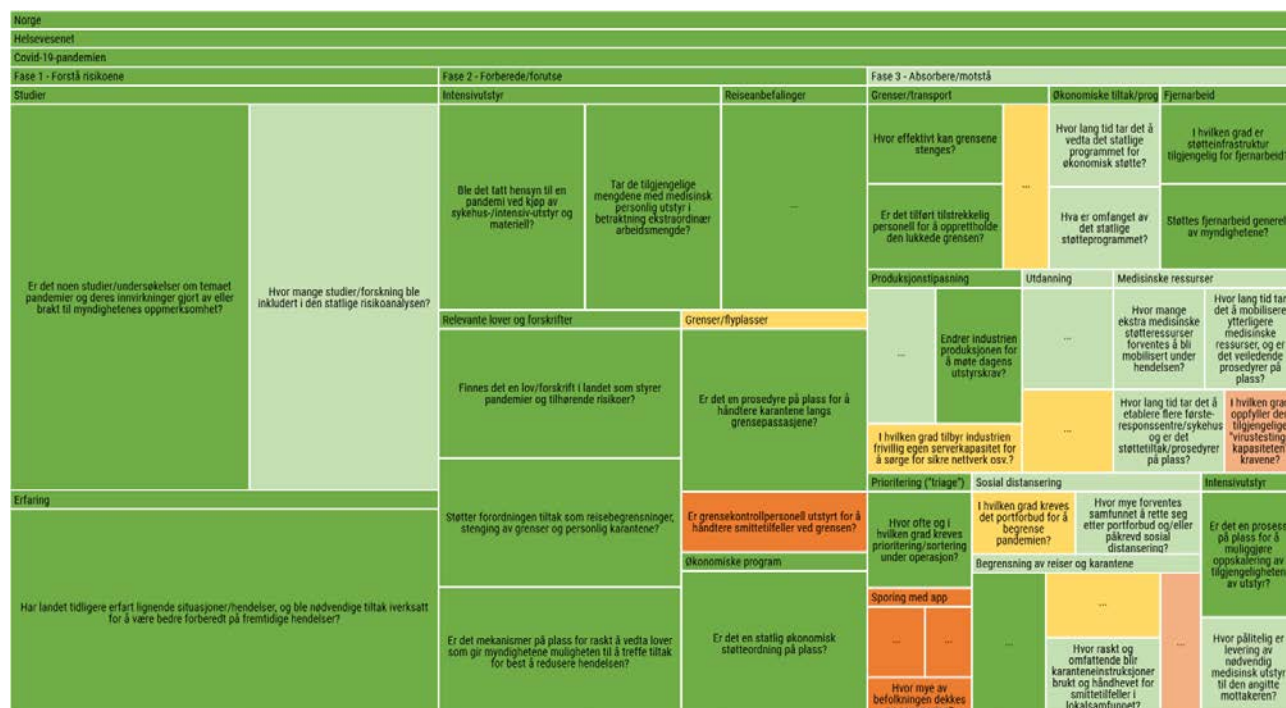
Det var ikke tid til å konsultere eksperter for å vurdere måleverdier, og mange måleverdier baserer seg derfor på antakelser som er forbundet med stor usikkerhet. Det er også mulig at enkelte vurderinger er feil.

Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)

Beregningene er gjennomført med bruk av web-verktøyet ResiliN beskrevet i vedlegg H. Resultatene er vist i neste trinn.

Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.

Statusen er vist visuelt med trestrukturdiagrammet i figur 4.15 (med bruk av web-verktøyet ResiliN).



Figur 4.15 Trestrukturdiagram for covid-19 laget med web-verktøyet ResiliN¹⁵

Øverst (ytterst) er området (Norge), deretter den kritiske infrastrukturen eller samfunnsfunksjonen (helsevesenet), og så hendelsen (covid-19-pandemien). Siden det kun er én av hver av disse, så dekker boksene/rektangelene for disse hele diagrammet, og resultatet er også likt for disse tre nivåene. De er alle mørkegrønn, så totalresultatet er svært bra (resiliensnivå A).

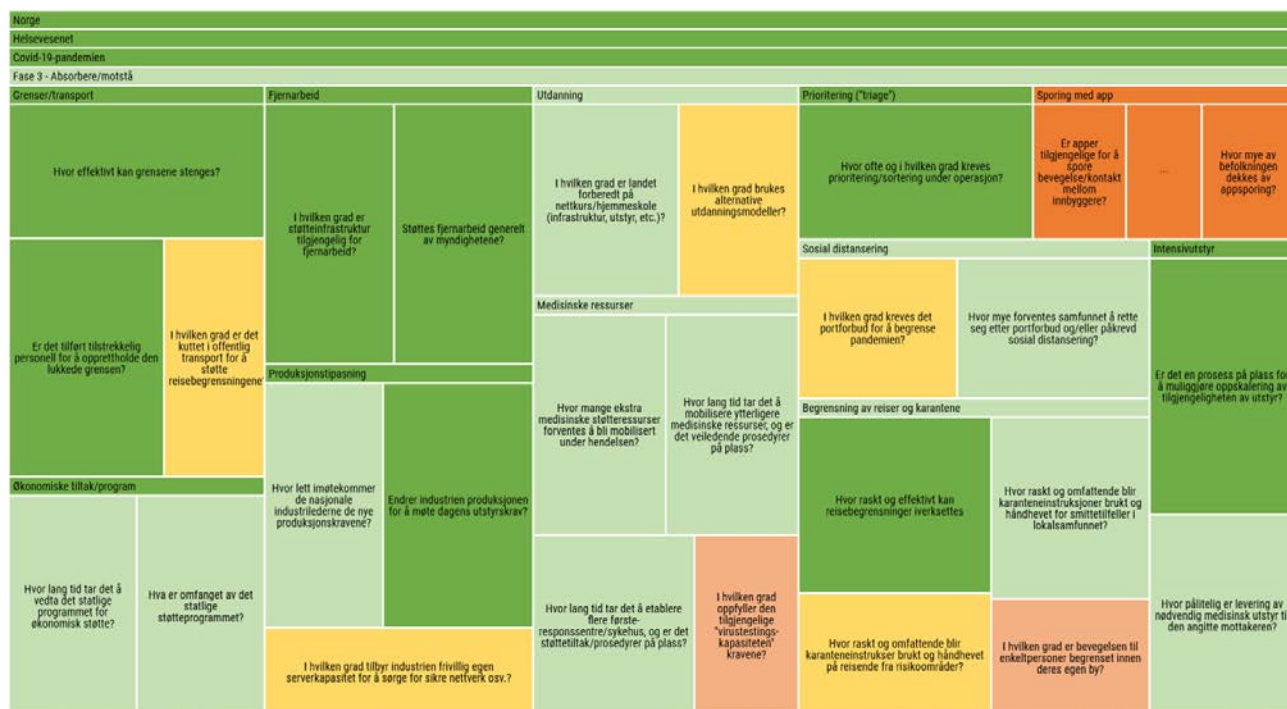
På nivå 4 har vi fasene, og siden vi kun dekker de tre første fasene, og disse er vektet likt, så utgjør de 1/3-del hver av diagrammet (fase 1 til venstre, fase 2 i midten, og fase 3 til høyre). Både fase 1 og 2 er mørkegrønn, dvs. resiliensnivå A, mens fase 3 er lysegrønn som tilsvarer resiliensnivå B.

Innenfor fasene har vi forholdene (nivå 5) og indikatorene (nivå 6). Størrelsen på boksene/rektangelene angir viktigheten/vekten. Forholdene og indikatorene i fase 1 er for det meste svært bra, mens det for fase 1 er ett forhold som er gult, dvs. resiliensnivå C, noe som skyldes at én av indikatorene er rød (resiliensnivå E). I fase 3 er det ett forhold som er rødt, og det er sporing med app, som ikke var kommet i gang i Norge 5. april 2020. Ellers er det noen indikatorer som skårer dårlig eller middels, men forholdene er allikevel samlet sett

¹⁵ Skriften er litt liten, men dere får zoome inn om nødvendig. Steder hvor det ikke er plass til hele teksten er angitt med "...". Teksten fremkommer i web-verktøyet ved å holde musepekeren over den aktuelle boksen.

enten bra (lysegrønn = resiliensnivå B) eller svært bra (mørkegrønn = resiliensnivå A), med unntak av sporing med app. Dette viser at mye ble håndtert bra i Norge i starten av pandemien.

I figur 4.16 har vi "zoomet inn" på fase 3, hvor mer av teksten til indikatorene fremkommer.



Figur 4.16 Trestrukturdiagram "zoomet inn" på fase 3

Figur 17 viser trestrukturdiagram hvor kun indikatorene som skårer dårlig eller svært dårlig er tatt med.



Figur 4.17 Trestrukturdiagram for utvalg av indikatorer som skårer dårlig eller svært dårlig

For å se de eksakte tallene (vektede skårverdier) på de ulike nivåene, må vi inn i redigeringsmodus i web-verktøyet. Dette er vist i figur 4.18.

Område:	Norge						+	
Kritisk infrastruktur:	Helsevesenet						+	
Trussel:	Covid-19-pandemien						+	
Fase:	Fase 1 - Forstå risikoene	Fase 2 - Forberede/forutse	Fase 3 - Absorbere/motstå	Fase 4 - Respondere/gjenvinne	Fase 5 - Tilpasse/lære			
Forhold:	Studier	Erfaring						+
Indikator:	Er det noen studier/undersøkelser om temaet pandemier og deres innvirkninger gjort av eller brakt til myndighetenes oppmerksomhet?						+	
Hvor mange studier/forskning ble inkludert i den statlige risikoanalysen?								

Område ✕	Kritisk infrastruktur ✕	Trussel ✕
Navn: Norge	Navn: Helsevesenet	Navn: Covid-19-pandemien
Vekt: 1	Vekt: 1	Vekt: 1
Resiliensnivå: Svært bra	Resiliensnivå: Svært bra	Resiliensnivå: Svært bra
Skår: 4.31	Skår: 4.31	Skår: 4.31

Fase ✕	Forhold ✕	Indikator ≡ ✕
Navn: Fase 1 - Forstå risikoene	Navn: Studier	Navn: Er det noen studier/under
Vekt: 1	Vekt: 1	Vekt: 1
Resiliensnivå: Svært bra	Resiliensnivå: Svært bra	Resiliensnivå: Ja
Skår: 4.75	Skår: 4.50	Skår: 5
Overskriv skår: ☐	Overskriv skår: ☐	Overskriv skår: ☐

Figur 4.18 Redigeringsmodus i web-verktøyet ResiliN

Boksene for område, kritisk infrastruktur og trussel viser skår 4,31, og fase 1 har skår 4,75. Første underliggende forhold og indikator vises også fordi disse er valgt (skyggelagt). For øvrige faser, forhold og indikatorer må disse velges for å se skårverdiene. Fase 2 har skår 4,50 og fase 3 har skår 3,69.

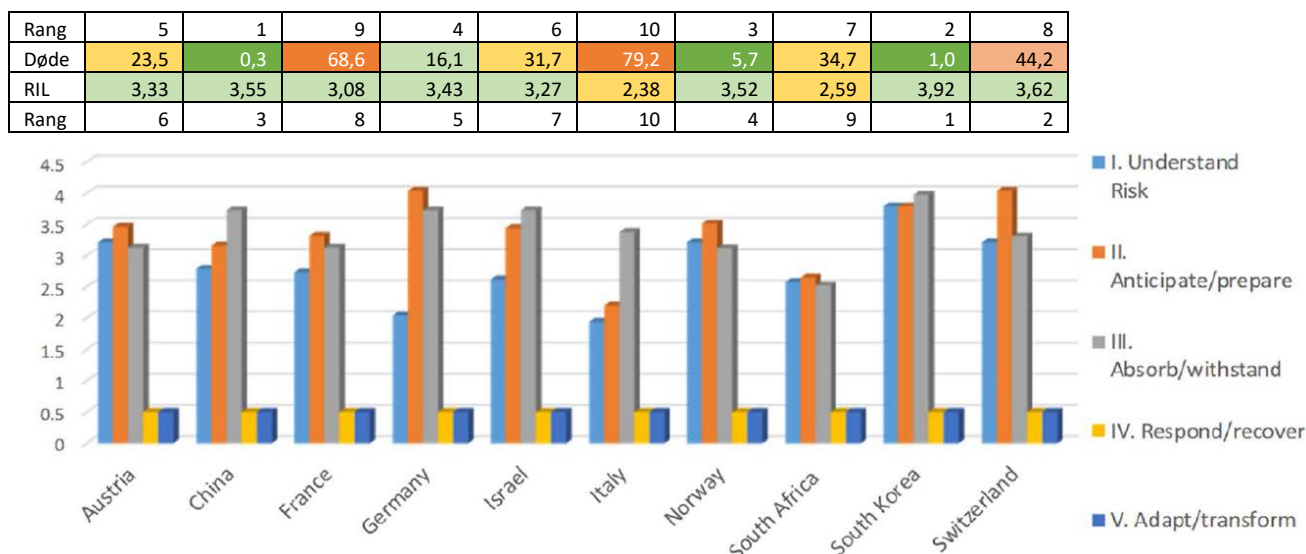
Trend er ikke relevant i dette eksempelet, siden det er en engangsvurdering av status. Styrker og svakheter er vist i form av en topp-fem og bunn-fem liste over forhold. Sistnevnte viser hvor forbedringsbehovet er mest prekært. Dette er vist i tabell 4.9.

Tabell 4.9 "Topp-fem" og "bunn-fem" forhold

Topp-fem forhold	Skår	RIL	Bunn-fem forhold	Skår	RIL
1. Erfaring	5,00	A	1. Sporing med app	0,00	E
1. Intensivutstyr	5,00	A	2. Grenser/flyplasser	2,50	C
1. Reiseanbefaling	5,00	A	3. Begrensning av reiser/karantene	3,25	B
1. Relevante lover og forskrifter	5,00	A	4. Sosial distansering	3,50	B
1. Økonomisk program	5,00	A	4. Medisinske ressurser	3,50	B

Forbedringsbehovet er størst i forhold til sporing med app, og dernest utstyr og personell for håndtering av smittetilfeller ved grensene/flyplassene.

Figur 4.19 viser sammenlikningen mellom 10 land (Jovanovic m.fl., 2020) som baserte seg på vurderinger per 5. april 2020, og hvor totalt resiliensnivå (RIL/skår) er vist i nest nederste linje i tabellen over figuren. Til sammenlikning er det vist i nest øverste linje antall døde per 100.000 innbyggere per 19. november 2020 (vg.no, 2020).



Figur 4.19 Sammenlikning av resiliensnivå mellom 10 land (Jovanovic m.fl., 2020)

Tallene er av mange grunner ikke sammenliknbare, men allikevel interessante. Resiliensvurderingen dekker mye mer enn bare det rent helsemessige, mens relativt antall døde sier noe om evnen til å stoppe smitten (og behandle de som blir smittet). Variasjonen i resiliensnivå og skår er liten: ingen er svært bra, de fleste er bra (lysegrønn) og to er middels (Italia og Sør-Afrika). Ingen er dårlig eller kritisk dårlig.¹⁶

Variasjonen i relativt antall døde er betydelig større, og litt avhengig av hvordan man setter grensene for ulike klassifiseringer¹⁷, så kan man trekke frem Kina, Sør-Korea og Norge på den positive siden, og Frankrike og Italia i andre ytterkant. USA ville også havnet i samme kategori (75,3), og det samme ville Sverige (62,8).

Ser vi på rangeringen (øverste og nederste linje i tabellen over figuren), så stemmer den rimelig godt overens, med et stort unntak og det er Sveits. Dette kan skyldes mange ting, hvorav en er ulik tolkning av indikatorene og grenseverdiene, ved at vurderingene er gjort av mange forskjellige personer. Den som gjorde vurderingen for Sveits, kan ha hatt en annen fortolkning enn mange av de andre. Det kan også skyldes at Sveits skåret bra på forhold som ikke direkte påvirker smittebegrensning eller andre helsemessige forhold.

¹⁶ Italia skårer imidlertid dårlig i fase 1, og nær dårlig i fase 2, men fase 3 er vurdert slik at de totalt sett havner på middels.

¹⁷ Her er det valgt 0-10 døde per 100.000 innbyggere for mørkegrønn, 10-20 lysegrønn, 20-40 gul, 40-60 lyserød, og 60-80 mørkerød.

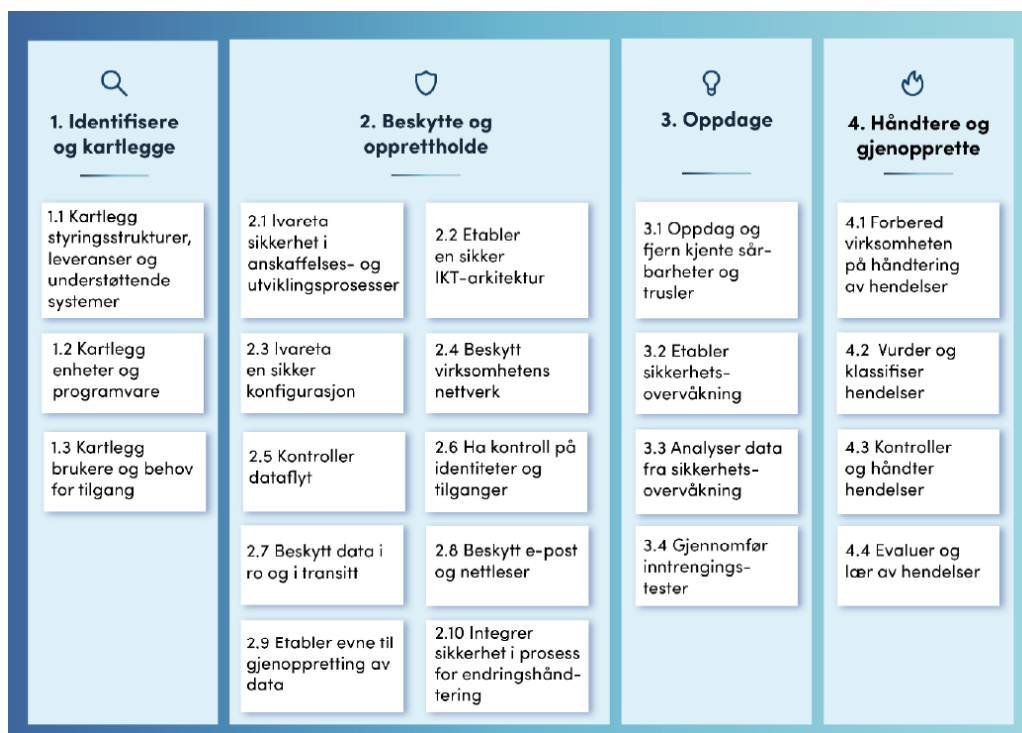
4.3 Nettangrep

Her vil vi se på alternative anvendelser av metoden. Som nevnt i kapittel 1.2, så kan det for nettangrep være aktuelt å inkludere NSMs grunnprinsipper for IKT-sikkerhet (NSM, 2020b), og i kapittel 3 er det nevnt at metoden kan benyttes for oppfølging av bruken av NSMs grunnprinsipper.

Dette kan gjøres på to måter. Den første er å inkludere tiltakene knyttet til NSMs grunnprinsipper som forhold (i trinn 5), og gjennomføre metoden som normalt. Den andre er å beholde strukturen som benyttes i NSMs grunnprinsipper, det vil si kategorier, grunnprinsipper og tiltak, men benytte beregningsmåten i CIRAM.

4.3.1 Inkludere NSMs grunnprinsipper for IKT-sikkerhet

En oversikt over NSMs grunnprinsipper for IKT-sikkerhet er vist i figur 4.20.



Figur 4.20 Oversikt over NSMs grunnprinsipper for IKT-sikkerhet (NSM, 2020b)

Totalt 21 grunnprinsipper er fordelt på fire kategorier. Hvert grunnprinsipp (GP) består av et antall anbefalte tiltak (mellom tre og ti tiltak), og totalt er det 118 tiltak.

Eksempel: Grunnprinsipp 1.2 Kartlegg enheter og programvare

- Tiltak:
- 1.2.1 Etabler en prosess for å kartlegge enheter og programvare som er i bruk i virksomheten
 - 1.2.2 Fastsett retningslinjer for godkjente enheter og programvare i virksomheten
 - 1.2.3 Kartlegg enheter i bruk i virksomheten
 - 1.2.4 Kartlegg programvare i bruk i virksomheten

Beskrivelse av tiltak – eksempel: 1.2.3 Kartlegg enheter i bruk i virksomheten

Kartlegg enheter i bruk i virksomheten iht. prosess i 1.2.1. **a)** Kartlegg informasjon etter en hensiktsmessig vurdering, for eksempel nettverksadresse, maskinvareadresse, enhetsnavn, avdelingstilknytning, samt om enhetene er forvaltet av virksomheten. Hver enhet som har en IP-adresse på nettverket bør være med i oversikten, inkludert stasjonære og bærbare datamaskiner, servere, nettverksutstyr (rutere, svitsjer, brannmurer, osv.), skrivere, lagringsnettverk, IP-telefoner, IoT-enheter, osv. **b)** Få oversikt over alle mobile enheter og lagringsmedier som benyttes utenfor virksomhetens nett som inneholder virksomhetsinformasjon. **c)** Lag en plan for håndtering av enheter som ikke er godkjent for bruk i virksomheten (se 1.2.2). For håndtering se 2.4.1.b. **d)** Virksomheten bør også ha oversikt over virtuelle enheter (enten de kjører hos virksomheten eller i en leverandørs «sky»). I mange tilfeller bør oversikten da være litt overordnet hvis «levetid» på virtuelle enheter er variabel/dynamisk, f.eks. «stateless» «Virtual Desktops». Oversikt over virtuelle enheter som kjører hos en leverandør er primært kun hensiktsmessig ifm. kjøp av «IaaS».

Hvert tiltak består av flere del-tiltak, som her for tiltak 1.2.3 er **a) - d)**, dvs. fire del-tiltak.

Anvendelsen av NSMs grunnprinsipper for IKT-sikkerhet må tilpasses metoden (CIRAM). Dette gjelder bl.a.:

- Tilpasning av omfang
- Tilpasning til faser, forhold og indikatorer
- Måling av status på enkelttiltak

Tilpasning av omfang

En inkludering av alle 118 tiltak vil være svært omfattende. I første omgang velger vi derfor ut de 15 tiltakene (tilhørende åtte ulike grunnprinsipper) som NSM har vurdert å ha 1. prioritet. Dette er ifølge NSM de sikkerhetstiltakene som haster mest. Mangelen på implementering av flere av disse tiltakene er som oftest "rot-årsaken" til vellykkede data-angrep.

Tilpasning til faser, forhold og indikatorer

Kategoriene tilpasses til fasene i CIRAM, men i noen tilfeller vil aktuell fase vurderes for det enkelte grunnprinsipp, dvs. grunnprinsipper innenfor samme kategori kan tilordnes ulike faser. Tilordningen er vurdert å være som følger: Kategori 1 inngår i fase 1, kategori 2, 3 og GP 4.1 inngår i fase 2, GP 4.2 inngår i fase 3, GP 4.3 inngår i fase 4, og GP 4.4 inngår i fase 5. (Kategori 3 kan inngå både i fase 2 og 3).

Grunnprinsippene vil tilsvare forhold, og enkelttiltakene vil være underlaget for indikatorene, dvs. i hvilken grad tiltakene er gjennomført.

Måling av status på enkelttiltak

Dette kunne vært splittet opp på et sett med ja/nei-spørsmål for hvert del-tiltak, eller etablert modenhetsmodeller for hvert tiltak, men kan også forenkles til en samlet vurdering av hvert tiltak.

Nedenfor er det beskrevet hvordan de prioriterte tiltakene i NSMs grunnprinsipper for IKT-sikkerhet kan inkluderes i CIRAM, men uten at øvrige forhold er tatt med. Det vil si at det er ingen komplett vurdering av et nettangrep. Videre er det antatt at dette gjelder for én enkelt virksomhet uten at denne er nærmere spesifisert.

Trinn 1: Velg område

(Gjelder for en gitt virksomhet innenfor en aktuell kritisk infrastruktur – ikke et område).

Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)

En gitt virksomhet innenfor en aktuell kritisk infrastruktur.

Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene

Nettangrep generelt (eller spesifisert).

Trinn 4: Vurder hver fase for hver fare/trussel/hendelse

Her skal nettangrep vurderes for hver av fasene. Det som vurderes i hver av fasene er hvilke forhold som er viktig for å håndtere nettangrep (trinn 5) og deretter hvordan disse forholdene kan måles med indikatorer (trinn 6).

Trinn 5: Velg forhold for hver fase

Hvilke forhold er viktig for å håndtere et nettangrep? HVA er viktig? HVA er viktig for å forstå risikoene (fase 1), forberede/forutse (fase 2), absorbere/motstå (fase 3), respondere/gjenvinne (fase 4) og tilpasse/lære (fase 5) av nettangrepet?

Tabell 4.10 viser de åtte grunnprinsippene som inneholder de 15 prioriterte tiltakene i NSMs grunnprinsipper for IKT-sikkerhet. Disse er omformulert fra aktiviteter til forhold og plassert under tilhørende fase.

Tabell 4.10 Forhold bestående av prioriterte GP-er tilordnet de ulike fasene

Fase	Forhold (GP nummer og navn)
1 Forstå risikoene <i>Gjør virksomheten nok for å forstå risikoen?</i>	1.2 Kartlegging av enheter og programvare
2 Forberede/forutse <i>Forutser virksomheten godt nok hva som kan inntreffe, og forbereder den seg godt nok på trusler og andre uønskede hendelser?</i>	2.1 Ivaretagelse av sikkerhet i anskaffelses- og utviklingsprosesser 2.2 Etablering av en sikker IKT-arkitektur 2.3 Ivaretagelse av en sikker konfigurasjon 2.6 Kontroll på identiteter og tilganger 2.9 Etablering av evne til gjenoppretting av data 3.2 Etablering av sikkerhetsovervåking 4.1 Forberedelse av virksomheten på håndtering av hendelser
3 Absorbere/motstå <i>Har virksomheten gjennom aktive grep økt sin evne til å stå imot og håndtere kjente og ukjente ekstreme påkjenninger?</i>	(4.2 Vurdering og klassifisering av hendelser)
4 Respondere/gjenvinne <i>Har virksomheten kapasitet og evne til rask respons og evnen til å komme seg raskt på fote igjen etter ekstremhendelsen?</i>	(4.3 Kontroll og håndtering av hendelser)
5 Tilpasse/lære <i>Evner virksomheten å lære i etterkant?</i>	(4.4 Evaluering og læring av hendelser)

Tabell 4.10 viser at de prioriterte forholdene kun dekker fase 1 og 2. GP 4.2 vil inngå i fase 3, GP 4.3 i fase 4, og GP 4.4 i fase 5, men det er ingen tiltak fra disse som er gitt 1. prioritet av NSM.

Den enkelte virksomhet/bruker av metoden kan vurdere å legge til forhold/grunnprinsipper (med utvalgte tiltak) i fase 3-5 fra NSMs grunnprinsipper, selv om disse er av prioritet 2 eller 3. (Lagt inn kun med GP nummer og navn i tabell 4.10).

Trinn 6: Velg indikatorer for hvert forhold

HVORDAN måler vi disse viktige forholdene, ved hjelp av indikatorer (ja/nei spørsmål, antall, andeler, frekvenser, osv.)? Hvilke indikatorer er relevante for de ulike forholdene (én eller flere per forhold)?

Hvert enkelt forhold – representert ved de åtte grunnprinsippene, jf. tabell 4.10 – består av et eller flere prioriterte tiltak, til sammen 15 tiltak. Disse består igjen av flere del-tiltak (se eksempelvis beskrivelse av tiltak 1.2.3 ovenfor). Definerings av hvordan dette skal måles, ved hjelp av indikatorer, kan gjøres komplisert, eksempelvis ved definering av modenhetsmodeller for hvert enkelt tiltak. Her er det imidlertid valgt en forenklet måte å måle på, hvor indikatorene angir *prosentvis grad av gjennomføring av tiltak* (basert på en helhetlig vurdering).

Tabell 4.11 viser de 15 prioriterte tiltakene, og hvor indikatorene er grad av gjennomføring av tiltak, eksempelvis *grad av gjennomføring av kartlegging av enheter i bruk i virksomheten*.

Tabell 4.11 Indikatorer som *grad av gjennomføring* av de 15 prioriterte tiltakene

Fase	Forhold (GP nummer/navn)	Indikatorer – grad av gjennomføring av tiltak [%]
1	Forstå risikoene	1.2 Kartlegging av enheter og programvare 1.2.3 Kartlegging av enheter i bruk i virksomheten 1.2.4 Kartlegging av programvare i bruk i virksomheten
2	Forberede/forutse	2.1 Ivaretagelse av sikkerhet i anskaffelses- og utviklingsprosesser 2.1.2 Kjøp av moderne og oppdatert maskin- og programvare 2.1.9 Ansvar for virksomhetens sikkerhet ved tjenesteutsetting
	2.2 Etablering av en sikker IKT-arkitektur	2.2.3 Oppdeling av virksomhetens nettverk etter risikoprofil
	2.3 Ivaretagelse av en sikker konfigurasjon	2.3.1 Sentralt styrt regime for sikkerhetsoppdatering 2.3.2 Konfigurerings av klienter slik at kun kjent programvare kjøres 2.3.3 Deaktivering av unødvendig funksjonalitet 2.3.7 Standardpassord endret før produksjonssetting
	2.6 Kontroll på identiteter og tilganger	2.6.4 Minimering av rettigheter til sluttbrukere og spesialbrukere 2.6.5 Minimering av rettigheter på drifts-kontoer
	2.9 Etablering av evne til gjenoppretting av data	2.9.1 Plan for regelmessig sikkerhetskopiering av virksomhetsdata
	3.2 Etablering av sikkerhetsovervåking	3.2.3 Valg av hvilke deler av IKT-systemet som skal overvåkes 3.2.4 Innsamling av sikkerhetsrelevante data
	4.1 Forberedelse av virksomheten på håndtering av hendelser	4.1.1 Planverk for hendelseshåndtering

Trinn 7: Fastsett grenseverdiene for hver indikator og angi vektorer

Vi benytter en skår-skala fra 0-5, hvor 0 er verst og 5 er best, og tilordnet grad av gjennomføring av tiltak, som angitt i tabell 4.12 (jfr. tabell 2.6).

Tabell 4.12 Skår-skala

Skår	Resiliensnivå	Betegnelse	Grad av gjennomføring
4-5	A	Svært bra	80-100 %
3-4	B	Bra	60-80 %
2-3	C	Middels	40-60 %
1-2	D	Dårlig	20-40 %
0-1	E	Kritisk	0-20 %

Dersom tiltaket er gjennomført fullt ut (100 %) blir skårverdien 5,0. Dersom ingenting er gjennomført blir skårverdien 0. Dersom man ikke angir en bestemt prosentandel, men kun intervallet, vil det være naturlig å benytte 0,5 – 1,5 – 2,5 – 3,5 eller 4,5. Angir man imidlertid 80 %, så blir skårverdien 4,0.

Der det er mer enn én indikator (tiltak) for hvert forhold (grunnprinsipp) kan disse vektes likt eller ulikt. Tilsvarende kan de ulike forholdene (grunnprinsippene) vektes ulikt, men dette må ses i sammenheng med øvrige forhold (ut over grunnprinsippene hentet fra NSMs grunnprinsipper).

Trinn 8: Angi måleverdier for indikatorene (utfør målingen)

Dette kan eksempelvis for tiltak 1.2.3 *Kartlegging av enheter i bruk i virksomheten* være 50 % som tilsvarer skårverdi 2,5 ut fra en vurdering av at del-tiltak a) og b) er gjennomført, men ikke c) og d).

Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)

Når alle forhold (de prioriterte grunnprinsippene fra NSMs grunnprinsipper, og øvrige forhold) er statusvurdert, dvs. skårverdier er fastsatt, gjennomføres beregningene med bruk av web-verktøyet beskrevet i vedlegg H.

Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.

Statusen vises visuelt med trestrukturdiagram (med bruk av ResiliN web-verktøyet).

4.3.2 Oppfølging av NSMs grunnprinsipper for IKT-sikkerhet

I kapittel 4.3.1 tilpasset vi NSMs grunnprinsipper for IKT-sikkerhet til CIRAM, mens vi her går motsatt vei og tilpasser CIRAM til rammeverket for NSMs grunnprinsipper. Vi beholder strukturen som benyttes i NSMs grunnprinsipper, det vil si kategorier, grunnprinsipper og tiltak, men benytter beregningsmåten i CIRAM. Vi benytter også oversiktsbildet for NSMs grunnprinsipper for visualisering av status, i stedet for trestruktur-diagram (TreeMap).

Trinn 1: Velg område

(Gjelder for en gitt virksomhet innenfor en aktuell kritisk infrastruktur – ikke et område).

Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)

En gitt virksomhet innenfor en aktuell kritisk infrastruktur.

Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene

Nettangrep generelt (eller spesifisert).

Trinn 4: Vurder hver fase for hver fare/trussel/hendelse

De fem fasene i CIRAM erstattes av de fire kategoriene i NSMs grunnprinsipper for IKT-sikkerhet. Eneste trussel som vurderes er nettangrep (generelt).

Trinn 5: Velg forhold for hver fase

Forholdene i CIRAM representeres av grunnprinsippene (21), som er predefinert av NSM og tilordnet de fire kategoriene (1. Identifisere og kartlegge, 2. Beskytte og opprettholde, 3. Oppdage, og 4. Håndtere og gjenopprette).

Trinn 6: Velg indikatorer for hvert forhold

Indikatorene måler *grad av gjennomføring av tiltak* (118). Tiltakene er predefinert av NSM.

Trinn 7: Fastsett grenseverdiene for hver indikator og angi vektor

Her benyttes samme tabell som ovenfor, altså tabell 4.12. Grad av gjennomføring av tiltak (0-100%) bedømmes ut fra en helhetlig vurdering. Grenseverdiene utgjøres dermed av henholdsvis 0% og 100%.

Vektor (like eller ulike) angis på alle nivå (indikatorer/tiltak, forhold/grunnprinsipper, og fase/kategori).

Trinn 8: Angi måleverdier for indikatorene (utfør målingen)

Her er graden av gjennomføring av de 118 tiltakene vurdert, som prosentandeler mellom 0-100%. Eksempler for tiltakene i grunnprinsipp 1.1 er vist i figur 4.21. Siste kolonne angir indikator-verdiene.

Nr.	Kategori	GP. ID	Grunnprinsipp	Tiltak ID	Tiltaksoverskrift	Tiltaksbeskrivelse	Grad av gjennomføring av tiltak [%]
1	Identifisere og kartlegge						
		1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer				
1	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.1	Identifiser virksomhetens strategi og prioriterte mål	Identifiser virksomhetens strategi og prioriterte mål, samt regelverk, bransjenormer og avtaler som kan ha innvirkning på sikring av informasjonssystemer.	100
2	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.2	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring. Dette inkluderer normalt a) policyer fra ledelsen, b) ledelsesstruktur med veldefinert ansvar og ansvarslinjer, c) prosesser for risikostyring (se 1.1.3) d) fastsatte toleransegrenser for risiko (se 1.1.4), e) tilføring av tilstrekkelige ressurser og fagkompetanse for å støtte ledelsen i arbeidet.	90
3	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.3	Identifiser virksomhetens prosesser for risikostyring knyttet til IKT	Identifiser virksomhetens prosesser for risikostyring knyttet til IKT. Dette inkluderer normalt a) verdilvurdering, b) trusselvurdering, c) kartlegge eksisterende sikkerhetstiltak, d) risikoidentifisering, e) risikovurdering, f) risikorapportering, g) risikohåndtering, h) etablere eller justere sikkerhetstiltak for å redusere risiko i) verifisere at sikkerhetstiltakene fungerer etter hensikt.	80
4	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.4	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT. Ledelsen må fastsette hvilke grenser for risiko virksomheten aksepterer og hva som er uakseptabel risiko. Dette må kommuniseres på tvers i organisasjonen. Det er vanlig å fastsette risikogrenser basert på konsekvens for virksomheten ved tap av konfidensialitet, integritet og tilgjengelighet for informasjon og informasjonssystemer. Se 4.1.1, 4.1.2 og «Utdypende informasjon» for ytterligere informasjon.	95
5	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.5	Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner	Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner. Kartlegg a) IKT-systemer, data og tjenester, inkludert eierskap, b) kritiske forretningsroller og c) interne og eksterne IKT-avhengigheter. d) Grupper i henhold til virksomhetens risikoaksept (1.1.4) og bruk resultatet som grunnlag for etablering av en sikker IKT-arkitektur, se prinsipp 2.2 - Etabler en sikker IKT-arkitektur.	75
6	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.6	Kartlegg informasjonsbehandling og dataflyt i virksomheten	Kartlegg informasjonsflyt mellom arbeidsprosesser, brukere, enheter og tjenester og bruk resultatet som grunnlag for etablering av en sikker IKT-arkitektur, se prinsipp 2.2 - Etabler en sikker IKT-arkitektur.	50

Figur 4.21 Vurdering (måling) og registrering av indikator-verdiene

Tabellen i figur 4.21 tar utgangspunkt i ei Excel-fil utarbeidet av NSM (NSM, 2020c).

Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)

Skårverdier fastsettes ved at indikatorverdiene på skalaen 0-100% transformeres til en skårskala 1-5. Skårverdier (s) fastsettes ut fra indikatorverdiene (X) som følger:

$$s = 5 \cdot \frac{X [\%]}{100}$$

Ut fra skårverdiene kan resiliensnivået (A-E) fastsettes, som vist i tabell 4.12.

Eksempel (jf. tiltak/indikator 1.1.5 i figur 4.22):

$$X = 75\% \rightarrow s = 5 \cdot 75/100 = 3,75 \text{ (som tilsvarer resiliensnivå B – bra)}$$

Skårverdiene og resiliensnivåene er vist for tiltakene i grunnprinsipp 1.1 i figur 4.22. (Alle kolonnene er ikke tatt med her, eksempelvis tiltaksbeskrivelsene).

Nr.	Kategori	GP. ID	Grunnprinsipp	Tiltak ID	Tiltaksoverskrift	Grad av gjennomføring av tiltak [%]	Tiltak skårverdi	Tiltak resiliensnivå
1	Identifisere og kartlegge						3,08	B
		1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer				4,08	A
1	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.1	Identifiser virksomhetens strategi og prioriterte mål	100	5	A
2	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.2	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.	90	4,5	A
3	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.3	Identifiser virksomhetens prosesser for risikostyring knyttet til IKT	80	4	A
4	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.4	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT	95	4,75	A
5	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.5	Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner	75	3,75	B
6	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.6	Kartlegg informasjonsbehandling og dataflyt i virksomheten	50	2,5	C

Figur 4.22 Beregning av skårverdier og resiliensnivå

Figur 4.22 viser også aggregerte verdier på grunnprinsipp-nivå (her: 4,08 for grunnprinsipp 1.1) og på kategori-nivå (her: 3,08 for kategori 1).

For disse beregningene trenger vi fastsettelse av vekter, for henholdsvis tiltak og grunnprinsipper, og dernest beregning av vektet skår, for tiltak og grunnprinsipper. Her er det benyttet lik vekting på alle nivå (tiltak, grunnprinsipp og kategori).

Skår for grunnprinsipp fremkommer som summen av vektete skår for tilhørende tiltak, og skår for kategori fremkommer som summen av vektete skår for tilhørende grunnprinsipper. Førstnevnte vektete skår, det vil si for tiltak, er vist i figur 4.23.

Skår for grunnprinsipp 1.1 fremkommer som summen av verdiene i siste kolonne (som blir 4,08). For fastsettelse av skårverdien for kategori 1 (her: 3,08) trenger vi også vektet skår for grunnprinsipp 1.2 og 1.3 (ikke vist i figur 4.23).

						Indikator:	Tiltak: skår, vektor og RIL			
Nr.	Kategori	GP. ID	Grunnprinsipp	Tiltak ID	Tiltaksoverskrift	Grad av gjennomføring av tiltak [%]	Tiltak skårverdi	Tiltak resiliensnivå	Tiltak vekt	Tiltak vektet skår
1	Identifisere og kartlegge						3,08	B		
		1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer				4,08	A		
1	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.1	Identifiser virksomhetens strategi og prioriterte mål	100	5	A	0,17	0,83
2	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.2	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.	90	4,5	A	0,17	0,75
3	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.3	Identifiser virksomhetens prosesser for risikostyring knyttet til IKT	80	4	A	0,17	0,67
4	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.4	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT	95	4,75	A	0,17	0,79
5	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.5	Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner	75	3,75	B	0,17	0,63
6	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer	1.1.6	Kartlegg informasjonsbehandling og dataflyt i virksomheten	50	2,5	C	0,17	0,42

Figur 4.23 Beregning av skårverdier som vektet sum av skårverdier på nivået under

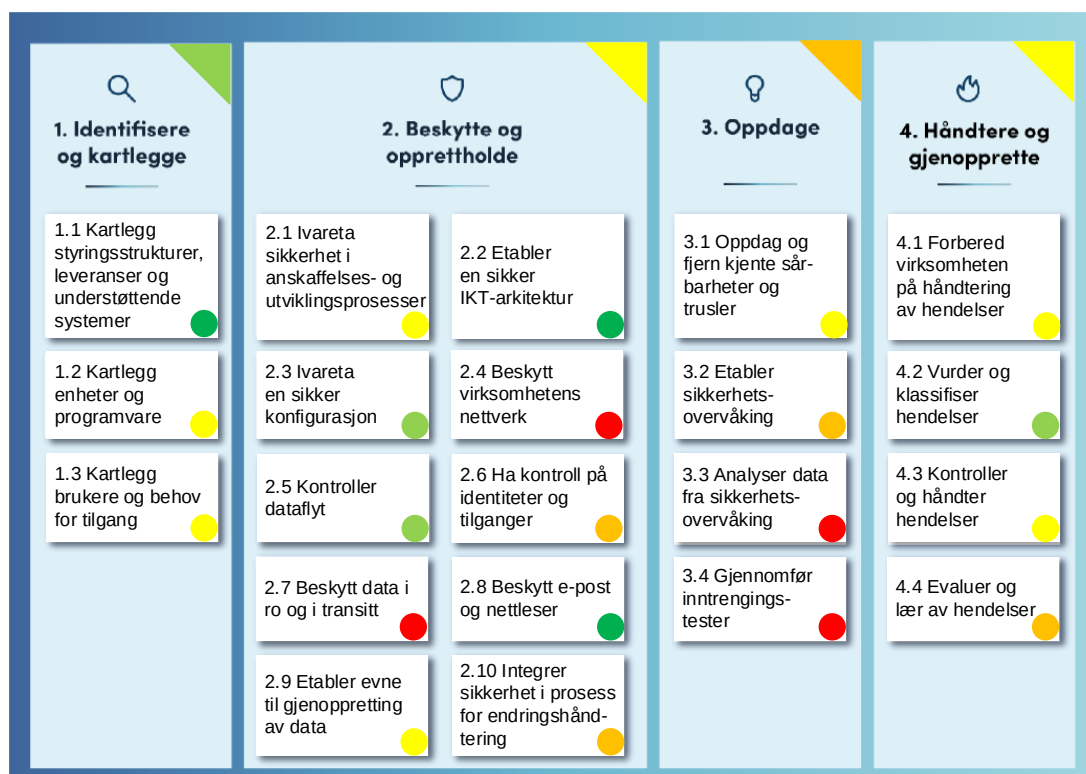
Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.

Figur 4.24 viser skårverdier og resiliensnivå for alle 21 grunnprinsipper, de fire kategoriene og totalt.

Nr.	Kategori	GP. ID	Grunnprinsipp	Tiltak ID	Tiltaksoverskrift	GP skår	GP resiliens-nivå	Kategori skår	Kategori resiliens-nivå	Kategori vekt	Kategori vektet skår	Total skår	Totalt resiliens-nivå
1	Identifisere og kartlegge							3,08	B	0,25	0,77	2,39	C
		1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer			4,08	A						
		1.2	Kartlegg enheter og programvare			2,31	C						
		1.3	Kartlegg brukere og behov for tilgang			2,83	C						
2	Beskytte og opprettholde							2,59	C	0,25	0,65		
		2.1	Ivareta sikkerhet i anskaffelses- og utviklingsprosesser			2,58	C						
		2.2	Etabler en sikker IKT-arkitektur			4,07	A						
		2.3	Ivareta en sikker konfigurasjon			3,95	B						
		2.4	Beskytt virksomhetens nettverk			0,69	E						
		2.5	Kontroller dataflyt			3,94	B						
		2.6	Ha kontroll på identiteter og tilganger			1,86	D						
		2.7	Beskytt data i ro og i transitt			0,55	E						
		2.8	Beskytt e-post og nettleser			4,38	A						
		2.9	Etabler evne til gjenoppretting av data			2,38	C						
		2.10	Integrer sikkerhet i prosess for endringshåndtering			1,50	D						
3	Oppdage							1,46	D	0,25	0,37		
		3.1	Oppdag og fjern kjente sårbarheter og trusler			2,67	C						
		3.2	Etabler sikkerhetsovervåking			1,79	D						
		3.3	Analyser data fra sikkerhetsovervåking			0,61	E						
		3.4	Gjennomfør inntrengningstester			0,79	E						
4	Håndtere og gjenopprette							2,43	C	0,25	0,61		
		4.1	Forbered virksomheten på håndtering av hendelser			2,38	C						
		4.2	Vurder og klassifiser hendelser			3,33	B						
		4.3	Kontroller og håndter hendelser			2,33	C						
		4.4	Evaluer og lær av hendelser			1,69	D						

Figur 4.24 Skårverdier og resiliensnivå for grunnprinsippene, kategoriene og totalt

Dette kan også visualiseres med bruk av oversiktsfiguren til NSM, jf. figur 4.25 nedenfor.



Figur 4.25 Status med hensyn til resiliensnivå for alle grunnprinsippene og kategoriene

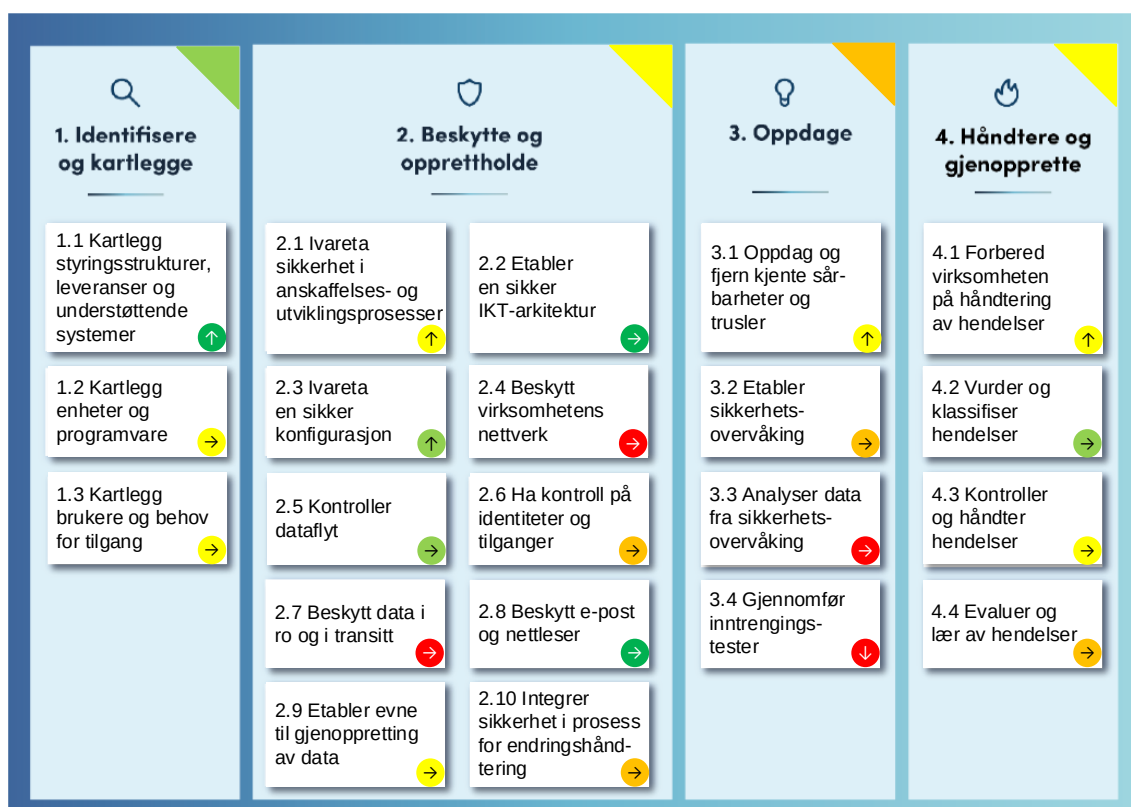
Statusvurderingen viser hvor det er størst behov for forbedring. Grunnprinsipp 2.4, 2.7, 3.3 og 3.4 er i dette eksempelet kritisk dårlig, mens statusen også er dårlig for grunnprinsipp 2.6, 2.10, 3.2 og 4.4. Tilsvarende kan man på nivået under (tiltak) se hvilke tiltak som har lavest skår og bidrar mest til en dårlig status for tilhørende grunnprinsipp. På kategori-nivå er det kategori 3 (oppdage) som kommer dårligst ut.

Statusen påvirkes av vektingen, som her er gjort likt på alle nivå. Det vil si at alle tiltak innenfor et grunnprinsipp teller like mye, at alle grunnprinsipp innenfor en kategori teller like mye, og at alle kategoriene teller like mye (25% hver). Dette kan endres på flere måter. Tiltak kan gis vekt avhengig av prioritet, og alle grunnprinsipp kan telle like mye totalt sett, det vil si at kategorier med mange grunnprinsipp har større vekt enn de med få grunnprinsipp. (Dette gir henholdsvis 14%, 48%, 19% og 19% vekt for kategori 1-4).

Man kan også tilpasse beregningen slik at tiltak eller grunnprinsipp som ikke er relevante for en gitt virksomhet ikke teller med i beregningene.

Ved gjentatte statusvurderinger kan man se på utviklingen over tid. Hva har blitt forbedret, eventuelt forverret siden forrige vurdering? Dette kan illustreres med piler i statussymbolene (som vist i figur 4.26), og/eller med egne grafer.

Figur 4.26 viser at man for fem grunnprinsipper (1.1, 2.1, 2.3, 3.1 og 4.1) har et forbedret resiliensnivå sammenliknet med forrige måling/vurdering. I ett tilfelle har status forverret seg (grunnprinsipp 3.4 pga. færre gjennomførte inntrengningstester). Alle øvrige grunnprinsipp har uforandret resiliensnivå (men skårverdiene kan allikevel ha endret seg innenfor samme resiliensnivå).



Figur 4.26 Status og utvikling i resiliensnivå for alle grunnprinsippene

En tydelig synliggjøring av status og utvikling kan motivere til kontinuerlig innsats og forbedring i forhold til gjennomføring av tiltakene som inngår i NSMs grunnprinsipper for IKT-sikkerhet.

Dette kan også gi en god oversikt og innsikt for NSM (og andre tilsynsmyndigheter slik som NVE) med hensyn til virksomhetenes implementering av grunnprinsippene. NSM (og andre) kan også peke på hvor de

er mest bekymret for at statusen er for dårlig, inkludert forhold de gjentatte ganger har sagt er viktig uten at virksomhetene i tilstrekkelig grad har grepet fatt i disse.

God implementering av NSMs grunnprinsipper for IKT-sikkerhet vil redusere risikoen og forbedre evnen til å håndtere hendelser (gi økt resiliens).

NVEs oppfølging av IKT-sikkerhet i kraftforsyningen

Eksempelet som er beskrevet her med oppfølging av NSMs grunnprinsipper for IKT-sikkerhet er relevant for blant annet Norges vassdrags- og energidirektorat (NVE) fordi det refereres til anvendelse av NSMs grunnprinsipper i veiledning til kraftberedskapsforskriften (NVE, 2021). Selve kraftberedskapsforskriften (2019) viser ikke direkte til NSMs grunnprinsipper, men viser til at *"virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer"*, og viser deretter kategoriene i NSMs grunnprinsipper for IKT-sikkerhet.

Riksrevisjonen (2021) har vurdert i hvilken grad NVEs virkemiddelbruk bidrar til å styrke IKT-sikkerheten i kraftforsyningen. Det konkluderes blant annet med at *"NVEs styring og oppfølging av arbeidet med IKT-sikkerhet i kraftforsyningen er svak"*.

NVE ba våren/forsommeren 2021 virksomhetene gjøre egevalueringer av status på implementeringen av NSMs grunnprinsipper for IKT-sikkerhet, som har store likhetstrekk med det vi har vist til her med en tilpasset bruk av CIRAM, blant annet ved at de anvender Excel-dokumentet utarbeidet av NSM (NSM, 2020c). Hovedforskjellene er at NVE benytter en tre-delning (rød, gul, grønn), mens CIRAM benytter en fem-delning, NVE inkluderer kun 1. og 2. prioritetsiltak (35 av 118 tiltak), mens vi også dekker 3. prioritetsiltak, og at NVE vurderer tiltakene enkeltvis, mens CIRAM også gir aggregerte beregninger av status. Med bruk av CIRAM legger vi dessuten opp til gjentakende evalueringer slik at utviklingen i implementeringen over tid kan synliggjøres.

Ulempen med tre-delningen er at mange av vurderingene lett kan havne i midterste kategori (gul), spesielt når det er benyttet kvalitative definisjoner av grad av implementering (grønn – høy grad, gul – moderat grad, rød – liten grad).

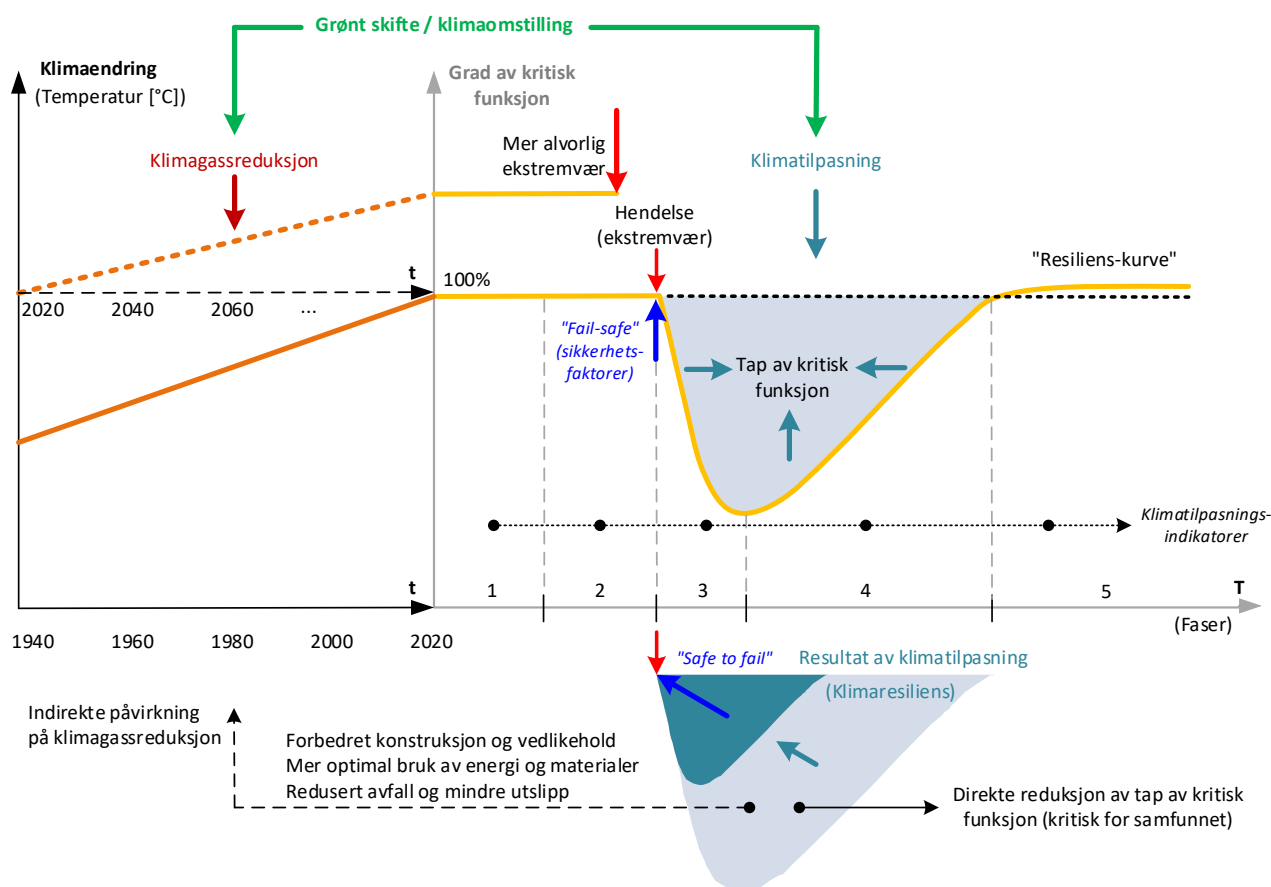
En aktuell tilpasning for bruk i kraftforsyningen er å skille mellom administrative IKT-systemer, driftskontrollsystemer og tjenesteutsetting.

4.4 Ekstremvær

Her er det beskrevet hvordan metoden for resiliensvurdering kan benyttes i arbeidet med klimaresiliens av kritisk infrastruktur, dvs. hvordan kritisk infrastruktur kan gjøres resiliert mot ekstremvær som forventes som følge av klimaendringer. Klimaendringene fører med seg temperaturendringer, økt nedbør, større regnflommer, flere skred, økt risiko for tørke, havnivåstigning (og dermed økt risiko for stormflo), med mere (NOU 2010: 10, Meld. St. 33 (2012-2013)).

Dette er basert på arbeid utført i prosjektet *Climate-RESilient infrastructure (CRES)* – "from fail-safe to safe-to-fail" (Depina og Øien, 2021), hvor målet var å "utvikle nye og praktiske resiliensindikatorer for å støtte grønt skifte av kritisk infrastruktur i et klima i endring". Grønt skifte og kampen mot klimaendringer gjennom klimaomstilling dekker både klimagassreduksjon og det å tilpasse seg klimaet – *klimatilpasning* – uansett hvordan klimaendringene blir (EC, 2019), og er "en kamp på to fronter".

Klimatilpasning defineres av IPCC (2014) som prosessen med å tilpasse seg faktisk eller forventet klima og dets effekter. Dette innebærer tilpasning for å moderere eller unngå skade, eller for å utnytte (positive) muligheter (Menon, 2018). Menon Economics har sammen med Sweco på oppdrag av Miljødepartementet etablert en metode for måling av klimatilpasning ved hjelp av indikatorer, men de har ikke benyttet en resiliensstilnærming. I beskyttelse mot og håndtering av ekstreme hendelser generelt, inklusive ekstremvær, er det imidlertid internasjonalt blitt vanlig å benytte en resiliensstilnærming, noe vi også benytter her. Figur 4.27 illustrerer resiliensstilnærmingen og også forholdet mellom klimatilpasning (høyre side i figuren) og klimagassreduksjon (venstre side i figuren) som til sammen utgjør det grønne skiftet / klimaomstillingen.



Figur 4.27 Resiliensstilnærming til klimatilpasning av kritisk infrastruktur

Høyre side av figuren viser resilienstilnærmingen, hvor en ekstremværhendelse kan redusere funksjonen til infrastrukturer som er kritisk for samfunnet fra nominelt 100 prosent, over kortere eller lengre tid. Dette er illustrert med "resiliens-kurven", som løper gjennom de fem fasene benyttet i CIRAM: 1) forstå risikoene, 2) forutse/forberede, 3) absorbere/motstå, 4) respondere/gjenvinne, og 5) tilpasse/lære.¹⁸ Arealet under kurven angir tap av kritisk funksjon, som kan reduseres gjennom økt resiliens mot ekstremværhendelser.

Det er også illustrert at man ved "normalt" ekstremvær kan benytte designkoder og sikkerhetsfaktorer for bygg og infrastrukturer (veier, rørledninger, osv.) som gjør at disse tåler en ekstremværhendelse, det vil si at de er designet *feil-sikker* ("fail-safe") – illustrert ved at blå pil (design-styrke) er større enn rød pil (belastningen fra ekstremværet).

Klimaendringene antas å gi mer ekstremt vær med mer alvorlige (og hyppigere) ekstremværhendelser, indikert med større rød pil som overskrider det som bygg og infrastruktur er designet for, og dermed økt risiko for tap av kritisk funksjon. Man må i større grad være innstilt på at feil-sikkert design ikke er tilstrekkelig under alle ekstremværhendelser, og ta høyde for dette ved å benytte en *sikkert-å-feile* ("safe-to-fail") strategi gjennom å redusere konsekvensene av en hendelse. Dette innebærer å tilpasse seg klimaendringene gjennom økt resiliens og derigjennom redusert "tap av kritisk funksjon",¹⁹ som illustrert nederst i figuren (og gjennom en større blå pil). Klimaresiliens bidrar til redusert sårbarhet for feil som følge av klimaendringer.

Dette vil i tillegg ha en indirekte påvirkning på det grønne skiftet / klimaomstillingen gjennom klimagass-reduksjon, som illustrert til venstre i figuren. Dette bidraget kommer fra redusert energiforbruk gjennom mer optimal bruk av energi og materialer, redusert avfall og mindre utslipp, og forbedret konstruksjon og vedlikehold. Klimaomstilling (og venstre side av figur 4.27) diskuteres ikke nærmere, men figuren illustrerer at temperaturen forventes å stige fremover i større eller mindre grad avhengig av hvordan vi lykkes i arbeidet med klimagassreduksjon.

Fokus her er *klimatilpasning* uansett hvor godt eller dårlig man lykkes i kampen mot klimaendringer!

Menon (2018) har foreslått en meny med indikatorforslag²⁰ for måling av kommunenes arbeid med klimatilpasning, som vi tar utgangspunkt i, i likhet med hva som er gjort i "indikatorprosjektet" til SINTEF Community (Sivertsen m.fl., 2021).²¹ I utgangspunktet har vi gjort tilsvarende avgrensing her hvor kommunene er i fokus (måling av kommunenes klimatilpasningsinnsats), og da særlig klimatilpasning av bebygde og regulerte arealer, bygninger/bygningsmassen, og kommunal infrastruktur begrenset til vei, vann og avløp (selv om ikke alt av dette er definert som kritisk infrastruktur). Underveis har vi utvidet omfanget noe ved å inkludere blant annet jernbane, strømforsyning og telekom.

Noen hovedforskjeller mellom arbeidet gjort av Menon (2018) og fremgangsmåten beskrevet her, i tillegg til at Menon ikke benytter en resilienstilnærming, er at Menon benytter en *kategorisering av indikatorer* etter type (ikke faser), de *identifiserer indikatorer direkte* uten først å identifisere forhold/faktorer/tema som er

¹⁸ Det finnes mange varianter av faser beskrevet i litteraturen, f.eks. forberede, absorbere, tilpasse og gjenvinne (prepare, absorb, adapt and recover), som delvis overlapper hverandre.

¹⁹ Dette kan også betegnes som redusert sårbarhet. NOU 2010: 10 *Tilpassing til eit klima i endring. Samfunnet si sårbarheit og behov for tilpassing til konsekvensar av klimaendringane* definerer sårbarhet for klimaendringer som "graden et system er mottakelig for eller er ute av stand til å håndtere negative effekter av klimaendringer".

²⁰ Menon (2018) baserer seg på bl.a. EEA 2015; Schönthaler & Andrian-Werburg 2015; Aall et al. 2009, 2012; Aall & Nordland 2003; Amundsen et al. 2010; Solecki et al. 2015, samt intervjuer med Oslo, Bergen og Kristiansand kommuner.

²¹ I "indikatorprosjektet" har indikatorene (inklusive Menons) blitt videreutviklet i samarbeid med tre kommuner.

viktig å måle på, det angis ikke hvordan resultatene av indikatormålingene *presenteres eller visualiseres*, og det inngår ingen *beregningsmetodikk eller aggregering* av indikatormålinger. Det er også forskjeller i *kriterier* brukt for å bedømme godheten av indikatorene.

Kategorisering av indikatorer

Menon (2018) baserer seg på en kategorisering fra EEA (2015), hvor de skiller mellom fire typer indikatorer: *statusindikatorer*, *prosessindikatorer*, *tiltaksindikatorer* og *resultatindikatorer*. Innenfor industriell sikkerhet er de tre første kategoriene normalt slått sammen og betegnet prosessindikatorer. Man skiller altså kun mellom *prosessindikatorer* og *resultatindikatorer*, eller *proaktive* og *reaktive* indikatorer, også betegnet på engelsk som "*leading*" og "*lagging*" indikatorer (Øien, 2011a). Det er også en glidende overgang mellom disse, og det er ikke nødvendigvis hensiktsmessig å operere med dette skillet (Hopkins, 2009). Menon (2018) opererer med svært få resultatindikatorer, og det kan diskuteres om eksempelvis resultatindikatoren "*Har klimatilpasningsarbeidet i kommunen blitt evaluert ila. de fire siste år?*" er en resultatindikator eller en prosessindikator.

Menon (2018) har innført statusindikatorer, som ikke benyttes av EEA (2015), pga. viktigheten av å skaffe seg oversikt over og status på klimautfordringene. Dette korresponderer med fase 1 – forstå risikoene – i CIRAM.

Videre så skilles det ikke mellom prosessindikatorer og resultatindikatorer i CIRAM (også her er det i all hovedsak prosessindikatorer), men det skilles mellom hvilken av de fem fasene de tilhører.

Identifisering av indikatorer

Menon (2018) identifiserer indikatorer direkte, enten fra litteraturen eller gjennom intervjuer med kommunene, uten først å vurdere hva som er viktig i arbeidet med klimatilpasning (forhold/faktorer/tema), og deretter vurdere hvordan dette kan måles (indikatorer). I CIRAM gjøres dette i to klart adskilte trinn, først identifiseres de forhold som er viktig innenfor hver fase, og dernest hvordan disse forholdene kan måles vha. indikatorer.²²

Presentering/visualisering av resultater

Menon-rapporten presenterer en meny med indikatorforslag, men sier ingenting om hvordan resultatene av indikatormålingene skal presenteres eller visualiseres. CIRAM viser hvordan indikatormålingene kan presenteres både enkeltvis og samlet/aggregert, med bruk av blant annet trestrukturdiagram (Tree Map).

Beregningsmetodikk og aggregering

Menon-rapporten inneholder ingen beregningsmetodikk eller aggregering av indikatorinformasjon. CIRAM benytter en beregningsmetodikk hvor enhver type indikator (ja/nei-spørsmål, andel, antall, osv.) gjøres om til en skår på en felles skala (0-5). Dernest kan disse aggregeres som sum av vektete skårverdier fra indikatornivå til – i dette tilfellet – kommunenivå (det vil si alle indikatorene en kommune benytter for å måle hvor klimatilpasset den er).

Kriterier

Menon (2018) bedømmer hver av indikatorene ut fra fire kriterier (*tolkbar*, *treffsikker*, *påvirkbar*, og *kostnadseffektiv*). I CIRAM diskuteres en lang rekke kriterier for indikatorer, men konklusjonen er, i likhet med Menon, at ingen indikator er perfekt, det vil si at ingen oppfyller alle kriterier. Et kriterium som savnes i

²² Her gjør vi ingen egen identifisering av indikatorer, men tar utgangspunkt i indikatorforslagene til Menon (2018). Vi identifiserer også forhold, men disse baserer seg på en vurdering av hva indikatorene egentlig måler. Kun unntaksvis går vi veien om forhold først. Dette gjelder faser hvor det mangler indikatorer fra Menon (2018), f.eks. for fase 5.

Menon-rapporten er *følsomheten* av indikatorene. Eksempelvis vil indikatoren "*Er det utpekt en ansvarlig for klimatilpasningsarbeidet i kommunen?*" være relativt statisk. Dersom svaret første gang er ja, er det lite trolig at denne indikatoren vil endre seg over tid, og det har liten verdi å foreta denne målingen.

Det er heller ingen vurdering i Menon-rapporten om hvor *dekkende* indikatorene er for viktige forhold for klimatilpasningen. Ja/nei-spørsmål gir enkeltvis veldig begrenset og lite dekkende informasjon. Vi har derfor samlet ja/nei-spørsmål som dekker samme forhold. Disse kan det så etableres en kombinert indikator for, dersom man går direkte på indikatorer uten å gå veien om forhold først.

Trinn 1: Velg område

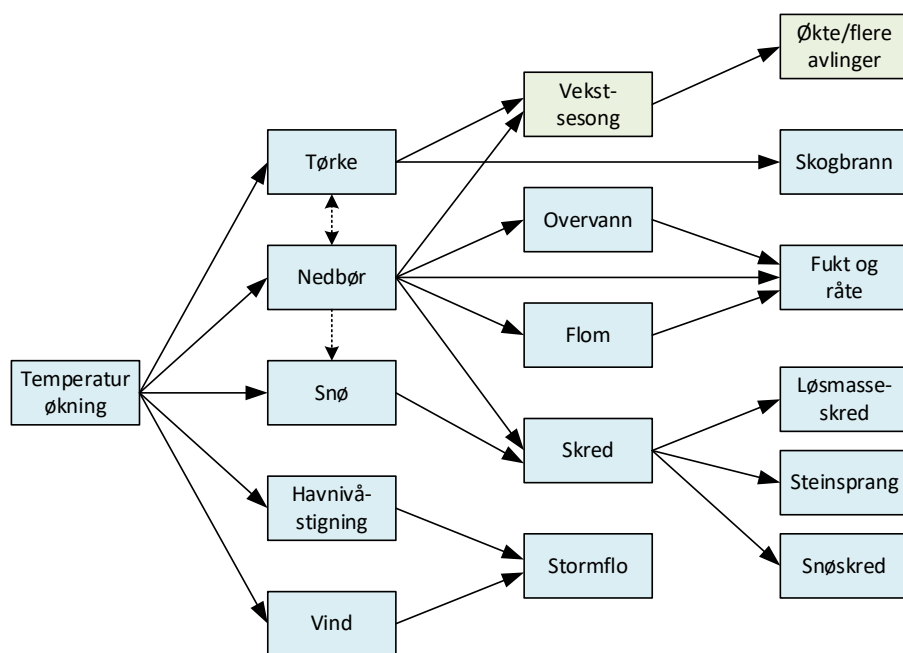
Området er i dette tilfellet en kommune.

Trinn 2: Velg kritiske infrastrukturer (eventuelt kritisk samfunnsfunksjon)

Kommunal infrastruktur begrenset til vei (del av samfunnsfunksjonen transport), og vann og avløp (samfunnsfunksjon). I tillegg inngår bebygde og regulerte arealer, og bygninger/bygningsmassen, selv om dette ikke defineres som kritisk infrastruktur av DSB (2016). I noen grad dekkes også jernbane, strømforsyning (del av samfunnsfunksjonen kraftforsyning) og telekom (del av samfunnsfunksjonen elektroniske kommunikasjonstjenester).

Trinn 3: Velg aktuelle farer/trusler/hendelser for de kritiske infrastrukturene

Ekstremvær, spesielt hyppigere og mer alvorlig ekstremvær som følge av klimaendringer. Dette kan gi en rekke klimautfordringer. Noen av disse og sammenhengen mellom dem er illustrert i figur 4.28. Det meste vil være negative effekter, men det kan være noen positive effekter, som økt vekstsesong og derigjennom økte eller flere avlinger. Aktuelle klimautfordringer må tilpasses den enkelte kommune.



Figur 4.28 Enkelte klimautfordringer og sammenhenger (basert på Menon, 2018)

Trinn 4: Vurder hver fase for hver fare/trussel/hendelse

Klimatilpasning for å kunne beskytte seg mot og håndtere ekstremvær vurderes for hver av fasene. Det som vurderes i hver av fasene er (normalt) hvilke forhold som er viktig for å beskytte seg mot og/eller håndtere ekstremvær (trinn 5), og hvordan disse forholdene kan måles med indikatorer (trinn 6). Her tar vi imidlertid hovedsakelig utgangspunkt i indikatorforslagene til Menon (2018) uten først å identifisere forhold. Dvs. at trinn 5 i liten grad blir benyttet.

Trinn 5: Velg forhold for hver fase

Hvilke forhold er viktig for å håndtere ekstremvær? HVA er viktig? HVA er viktig for å forstå risikoene/klimautfordringene (fase 1), forberede/forutse (fase 2), absorbere/motstå (fase 3), respondere/gjenvinne (fase 4) og tilpasse/lære (fase 5) av ekstremvær?

Tabell 4.13 viser aktuelle forhold for hver fase, hovedsakelig avledet fra utvalgte indikatorforslag fra Menon (2018).

Tabell 4.13 Forhold avledet fra utvalgte indikatorforslag fra Menon (2018)

Fase	Forhold
1 Forstå risikoene <i>Gjør virksomheten* nok for å forstå risikoen?</i>	1.1 Kunnskap om klimatilpasningsutfordringer
2 Forberede/forutse <i>Forutser virksomheten* godt nok hva som kan inntreffe, og forbereder den seg godt nok på trusler og andre uønskede hendelser?</i>	2.1 Ansvarliggjøring og involvering 2.2 Forankring i planverk og reguleringer 2.3 Inkludering av klimatilpasning i behandling og vurdering av plansaker og investeringsprosjekter 2.4 Overvåking
3 Absorbere/motstå <i>Har virksomheten* gjennom aktive grep økt sin evne til å stå imot og håndtere kjente og ukjente ekstreme påkjenninger?</i>	3.1 Plassering av bygg i forhold til klimautsatte områder 3.2 Krav til bygninger (klimarelatert) 3.3 Plassering og redundans av veiinfrastruktur i forhold til klimautsatte områder 3.4 Plassering og redundans av jernbane i forhold til klimautsatte områder 3.5 Plassering av underjordisk infrastruktur 3.6 Redundans i vannforsyning 3.7 Vedlikehold (for å opprettholde god standard og robusthet mot klimarelaterte hendelser) 3.8 Ressurser til klimatilpasningstiltak
4 Respondere/gjenvinne <i>Har virksomheten* kapasitet og evne til rask respons og evnen til å komme seg raskt på fote igjen etter ekstremhendelsen?</i>	4.1 Beredskapsplaner 4.2 Beredskapsøvelser 4.3 Tilgjengelighet av strøm, vann og avløp, veier, jernbane og fibernett 4.4 Ressurser for å håndtere ekstremværhendelser
5 Tilpasse/lære <i>Evner virksomheten* å lære i etterkant?</i>	5.1 Læring etter ekstremværhendelser (egne eller andres)

* Kommunen

Forhold som kompletterer de som er basert på indikatorforslagene til Menon er forhold 2.4, 3.2-3.5, 3.7-3.8, 4.2, 4.4 og 5.1. Ingen av indikatorforslagene til Menon var rettet mot fase 5 og læring etter ekstremværhendelser, og relativt få var rettet mot fase 4.

Trinn 6: Velg indikatorer for hvert forhold

HVORDAN måler vi disse viktige forholdene ved hjelp av indikatorer (ja/nei spørsmål, antall, andeler, frekvenser, osv.)? Hvilke indikatorer er relevante for de ulike forholdene (én eller flere per forhold)?

Her har vi som nevnt tatt utgangspunkt i indikatorforslagene til Menon (2018), og kun komplettert med indikatorer i fasene hvor det var relativt få relevante indikatorer. Dette gjelder spesielt for fase 4 og 5. Tabell 4.14 gir oversikt over aktuelle indikatorer. Nummer benyttet i Menon (2018) er angitt i hakeparentes. Ikke alle indikatorer vil være relevant for alle kommuner.

Tabell 4.14 Indikatorer (hvor ca. halvparten er hentet fra indikatorforslagene til Menon, 2018)

Fase	Forhold	Indikatorer [nr. benyttet av Menon (2018)]
1	Forstå risikoene	1.1 Kunnskap om klimatilpasningsutfordringer
		1.1.1 Er det utarbeidet overordnet ROS-analyse (etter Plan- og bygningsloven) for kommunen som helhet? [A1.1]
		1.1.2 Er det utarbeidet konkrete retningslinjer for hva en ROS-analyse skal inneholde? [C1.1]
		1.1.3 Har kommunen ledet arbeidet med å gjennomføre den overordnede ROS-analysen? [A1.3]
		1.1.4 Er det utarbeidet en overordnet klimasårbarhetsanalyse for kommunen som helhet? [A1.4]
2	Forberede/forutse	1.1.5 Jobber kommunen systematisk for å skaffe seg kunnskap og oversikt over hvilke klimatilpasningsutfordringer som kan inntreffe? [A1.5]
		2.1 Ansvarliggjøring og involvering
		2.1.1 Er det utpekt en koordinator for klimatilpasningsarbeidet i kommunen? [B1.10]
		2.1.2 Er det utpekt en ansvarlig for klimatilpasningsarbeidet i kommunen? [B1.11]
		2.1.3 Er det dedikert en tverrsektoriell faggruppe som jobber systematisk med klimatilpasning? [B1.12]
		2.2 Forankring i planverk og reguleringer
		2.2.1 Er det stilt krav til klimatilpasning i kommunens planstrategi? [B1.1]
		2.2.2 Er det utarbeidet en overordnet strategi for klimatilpasningsarbeid i kommunen? [B1.2]
		2.2.3 Blir klimatilpasning ivaretatt i kommuneplanens arealdel? [B1.4]
		2.2.4 Er det satt av midler i kommuneplanens handlingsdel til klimatilpasninger? [B1.5]
		2.2.5 Er klimatilpasning ivaretatt i kommunens område-reguleringer? [B1.7]
		2.2.6 Er klimatilpasning ivaretatt i kommunens detalj-reguleringer? [B1.8]
		2.3 Inkludering av klimatilpasning i behandling og vurdering av plan-saker og investerings-prosjekter
		2.3.1 Andel av kommunens egne investeringsprosjekter som har en kost-nytte-vurdering som inkluderer klimatilpasning [B1.13]
		2.3.2 Andel av (plan-)sakene som legges frem for Bystyret/kommunestyret som vurderer og dokumenterer konsekvenser av dagens og framtidige klimaendringer [C1.4]
		2.3.3 Andel av besluttede investeringsprosjekter ila. året som har synliggjort og vurdert konsekvenser av dagens og framtidige klimaendringer [C1.5]
		2.4 Overvåking
		2.4.1 Antall implementerte overvåkingsaktiviteter/systemer for veiinfrastruktur innenfor risikoutsatte områder (ras, flom, stormflo, etc.)
		2.4.2 Antall implementerte overvåkingsaktiviteter/systemer for jernbane innenfor risikoutsatte områder (ras, flom, stormflo, etc.)
3	Absorbere/motstå	3.1 Plassering av bygg i forhold til klimautsatte områder
		3.1.1 Andel godkjente byggeområder som ligger i klimarisikoutsatte områder* (ras, flom, stormflo, etc.) [D1.3]
		3.1.2 Andel av husholdninger eller m ² bygg innenfor kommunens geografiske avgrensning som ikke ligger i risikoutsatte områder* [A2.5], [A2.14], [A2.19]

Fase	Forhold	Indikatorer [nr. benyttet av Menon (2018)]
	3.2 Krav til bygninger (klimarelatert)	3.2.1 Andel av husholdninger eller m ² bygg innenfor kommunens geografiske avgrensning (i risikoutsatte områder*) som ble bygget før 1960
		3.2.2 Andel av husholdninger eller m ² bygg innenfor kommunens geografiske avgrensning (i risikoutsatte områder*) som ble bygget mellom 1960 og 2000
		3.2.3 Andel av husholdninger eller m ² bygg innenfor kommunens geografiske avgrensning (i risikoutsatte områder*) som ble bygget etter 2000
	3.3 Plassering og redundans av veiinfrastruktur i forhold til klimautsatte områder	3.3.1 Andel hovedveier (riksveier, fylkesveier) eller km hovedveier innenfor risikoutsatte områder* (ras, flom, stormflo, etc.)
		3.3.2 Andel hovedveier (riksveier, fylkesveier) eller km hovedveier innenfor risikoutsatte områder* uten alternative veier (f.eks. kommunale veier, fylkesveier)
		3.3.3 Andel kommunale veier eller km veier innenfor risikoutsatte områder* (ras, flom, stormflo, etc.)
		3.3.4 Andel kommunale veier eller km veier innenfor risikoutsatte områder* (ras, flom, stormflo, etc.) uten alternative veier (f.eks. kommunale veier, fylkesveier)
	3.4 Plassering og redundans av jernbane i forhold til klimautsatte områder	3.4.1 Andel jernbane eller km jernbane innenfor risikoutsatte områder* (ras, flom, stormflo, etc.)
		3.4.2 Andel jernbane eller km jernbane innenfor risikoutsatte områder* uten alternative forbindelser (f.eks. jernbane, kommunale veier)
	3.5 Plassering av underjordisk infrastruktur	3.5.1 Andel underjordisk infrastruktur (e.g., rørledninger, fiber, strømkabler) innenfor risikoutsatte områder* (ras, flom, etc.)
	3.6 Redundans i vannforsyning	3.6.1 Andel av kommunens husstander som har flere drikkevannskilder [A2.9]
	3.7 Vedlikehold (for å opprettholde god standard og robusthet mot klimarelaterte hendelser)	3.7.1 Antall ansatte per 100 km hovedveier som arbeider med vedlikehold
		3.7.2 Antall ansatte per 100 km kommunale veier som arbeider med vedlikehold
		3.7.3 Antall ansatte per 100 km jernbane som arbeider med vedlikehold
		3.7.4 Antall ansatte per 100 km vannforsyning som arbeider med vedlikehold
	3.8 Ressurser til klimatilpasningstiltak	3.8.1 Andel av kommunens budsjett som går til klimatilpasningstiltak
		3.8.2 Andel av kommunens budsjett for klimatilpasningstiltak som går til langsiktige tiltak
4	Respondere/gjenvinne	4.1 Beredskapsplaner
		4.1.1 Andel av kommunens drikkevannskilder det er utarbeidet beredskapsplaner for, med tanke på algeoppblomstring etc. [A2.8]
		4.1.2 Andel av kommunens skogarealer det er utarbeidet brannberedskapsplaner for [A2.21]
		4.1.3 Andel av kommunens populasjon som kan evakueres i en periode på inntil 1 uke
		4.1.4 Andel av kommunens populasjon som kan evakueres i en periode på inntil 3 måneder

Fase	Forhold	Indikatorer [nr. benyttet av Menon (2018)]
		4.1.5 Andel av kommunens befolkning som kan evakueres i en periode på inntil 1 år
	4.2 Beredskapsøvelser	4.2.1 Antall gjennomførte beredskapsøvelser knyttet til ekstremvær siste 3 år
	4.3 Tilgjengelighet av strøm, vann og avløp, veier, jernbane og fibernett	4.3.1 Antall husholdningstimer i året i kommunen som er uten strøm (nedetid multiplisert med husholdninger) [A2.16]
		4.3.2 Antall husholdningstimer i året i kommunen som er uten vann (nedetid multiplisert med husholdninger) [A2.17]
		4.3.3 Antall husholdningstimer i året i kommunen som er uten avløp (nedetid multiplisert med husholdninger)
		4.3.4 Antall husholdningstimer i året i kommunen som er uten tilførselsveg (nedetid multiplisert med husholdninger) [A2.18]
		4.3.5 Antall timer i året i kommunen med full eller delvis stengte hovedveier på grunn av ekstremvær
		4.3.6 Antall timer i året i kommunen med full eller delvis stengt jernbane på grunn av ekstremvær
		4.3.7 Antall husholdningstimer i året i kommunen som er uten tilgang til fibernett på grunn av ekstremvær
	4.4 Ressurser for å håndtere ekstremværhendelser	4.4.1 Andel av kommunens budsjett som går til ressurser for å håndtere ekstremværhendelser
		4.4.2 Antall ansatte per 100 km hovedveier som kan utbedre/rydde/gjenopprette mindre skader etter ekstremvær
		4.4.3 Antall ansatte per 100 km kommunale veier som kan utbedre/rydde/gjenopprette mindre skader etter ekstremvær
		4.4.4 Antall ansatte per 100 km jernbane som kan utbedre/rydde/gjenopprette mindre skader etter ekstremvær
		4.4.5 Antall ansatte per 100 km vannforsyning som kan utbedre/rydde/gjenopprette mindre skader etter ekstremvær
		4.4.6 Vedlikeholdes det en oppdatert oversikt over nabokommunenes ressurser for håndtering av ekstremværhendelser som kan forespørres/benyttas?
		4.4.7 Andel av de totale ressursene som nabokommunenes ressurser utgjør for håndtering av ekstremværhendelser
5	Tilpasse/lære	5.1 Læring etter ekstremværhendelser (egne eller andres)
		5.1.1 Antall ekstremværhendelser (egne eller andres) kommunen har lært av og som har resultert i konkrete endringer (i planer, tiltak, osv.)
		5.1.2 Antall arenaer kommunen deltar i hvor man kan lære av andre om klimatilpasning

* Risikoutsatte områder: områder med risiko for skader forårsaket av overvann (dersom det ikke er utarbeidet avrenningsløsninger), flomutsatte områder (dersom disse ikke er sikret mot flom), skredutsatte områder (dersom disse ikke er sikret mot skred), kvikkleireområder, områder som er utsatt for havnivåstigning og/eller stormflo (dersom det ikke er sikret mot slike forhold).

Indikatorene som er valgt ut er gjort skjønnsmessig og hovedsakelig på indikatorfaglig basis²³ og at indikatorene skal være mest mulig generelle og dermed relevante for flest mulig kommuner. I noen grad

²³ Øien (2001a, b), Øien m.fl. (2011a, b), Øien (2013), Øien (2016a).

baserer indikatorene seg på forslag fra domeneekspertise. Vurderingen bør imidlertid kompletteres av flere domene-eksperter og brukere, spesielt fra den aktuelle kommunen.

Vi har her tatt med 19 forhold og 60 indikatorer (hvorav 25 er hentet fra Menon), noe som i vanlig bruk av CIRAM er et litt lite antall forhold, og et noe lavt antall indikatorer spesielt når 14 av indikatorene er ja/nei-spørsmål, men det er ikke alle brukere som nødvendigvis ønsker en omfattende og dekkende resiliensvurdering. I det nevnte "indikatorprosjektet" til SINTEF Community (Sivertsen m.fl., 2021) hadde man et mål om maksimalt 10 indikatorer.²⁴ Vi velger derfor ut 8 indikatorer, slik at vi kan vise hvordan metoden kan anvendes videre for et veldig begrenset antall indikatorer. Vi velger også å lage kombinerte indikatorer av ja/nei-spørsmålene, fordi ja/nei-spørsmål enkeltvis gir svært begrenset informasjon. De 8 indikatorene er vist i tabell 4.15. De tre første indikatorene er kombinerte indikatorer.²⁵

Tabell 4.15 Begrenset utvalg indikatorer

Fase	Forhold	Indikatorer [nr. benyttet i Menon (2018)]
1 Forstå risikoene	1.1 Kunnskap om klimatilpasningsutfordringer	1.1.6 Grad av kunnskap om klimatilpasningsutfordringer (1.1.1-1.1.5)
2 Forberede/forutse	2.1 Ansvarliggjøring og involvering	2.1.4 Grad av ansvarliggjøring og involvering (2.1.1-2.1.3)
	2.2 Forankring i planverk og reguleringer	2.2.7 Grad av forankring i planverk og reguleringer (2.2.1-2.2.6)
3 Absorbere/motstå	3.1 Plassering av bygg i forhold til klimautsatte områder	3.1.1 Andel godkjente byggeområder som ligger i klimarisikoutsatte områder (ras, flom, stormflo, etc.) [D1.3]
	3.8 Ressurser til klimatilpasningstiltak	3.8.1 Andel av kommunens budsjett som går til klimatilpasningstiltak
4 Respondere/gjenvinne	4.2 Beredskapsøvelser	4.2.1 Antall gjennomførte beredskapsøvelser knyttet til ekstremvær siste år
	4.4 Ressurser for å håndtere ekstremværehendelser	4.4.1 Andel av kommunens budsjett som går til ressurser for å håndtere ekstremværehendelser
5 Tilpasse/lære	5.1 Læring etter ekstremværehendelser (egne eller andres)	5.1.1 Antall ekstremværehendelser (egne eller andres) man har lært av og som har resultert i konkrete endringer (i planer, tiltak, osv.)

Her er det bevisst valgt indikatorer som dekker alle de fem fasene, noe som er lett å sørge for med en resiliensbasert tilnærming. Dette er ikke tilfellet med tilnærmingen til Menon (2018) hvor man kun har benyttet en klassifisering i type indikator (status, prosess, tiltak, og resultat). De fire siste av de åtte indikatorene i tabell 4.15 inngår ikke i Menon (2018), men bidrar til å dekke alle faser. Eksempelvis vil læring etter ekstremhendelser (egne eller andres) være viktig. Menon (2018) omtaler også læring, men da i form av læring av arbeidet med klimatilpasning gjennom indikatorene som benyttes, ikke læring av håndtering av hendelser.

Vi vil understreke at forslagene til indikatorer ikke er gjennomarbeidet, og at dette må gjøres i samarbeid med den aktuelle kommune/bruker. Indikatorforslagene benyttes for å illustrere bruken av metoden.

²⁴ Opprinnelig hadde man dette som mål, men har underveis i prosjektet endt opp med et større antall indikatorer (ca. 50). Det vil uansett være opp til den enkelte kommune å velge ut et endelig sett med indikatorer, og dermed også muligheten for å avgrense antallet indikatorer.

²⁵ Det totale antallet indikatorer som inngår blir dermed 19, dersom hvert ja/nei spørsmål telles som en indikator.

Trinn 7: Fastsett grenseverdiene for hver indikator og angi vektor

Vi benytter en skår-skala fra 0-5, hvor 0 er verst og 5 er best, som angitt i tabell 4.16.

Tabell 4.16 Skår-skala

Skår	Resiliensnivå	Betegnelse
4-5	A	Svært bra
3-4	B	Bra
2-3	C	Middels
1-2	D	Dårlig
0-1	E	Kritisk

Hvert hele trinn i skårskalaen tilsvarer et resiliensnivå angitt med en karakter E-A, hvor E er verst (kritisk) og A er best (svært bra). Eksempelvis vil en skår mellom 3 og 4 tilsvare et resiliensnivå B (bra).

Hver enkelt indikator har sin måleskala som må tilpasses skårskalaen, det vil si at det må angis grenseverdier for hver indikator. På denne måten blir alle indikatorene tilpasset til og målt etter en felles skala, noe som er nødvendig for aggregering av verdiene til enkeltindikatorene.

Fastsettelse av grenseverdier må gjøres av brukerne – i dette tilfellet kommunen – og er erfaringsmessige krevende. (Hva er godt og hva er dårlig? Hva gir maksimal skår og hva gir minimal skår?) Det tar tid å fastsette disse første gang, og det er ofte behov for justering etter at man får erfaring gjennom målinger.

For de tre første indikatorene, som baserer seg på underliggende ja/nei-spørsmål, kan dette gjøres enkelt ved at nei på alle spørsmål gir skår 0, ja på alle spørsmål gir skår 5, og at mellomliggende skårverdier gis ut fra antall ja. Forslag til skårverdier i forhold til antall ja for de tre kombinerte indikatorene er vist i tabell 4.17.

Tabell 4.17 Antall ja-svar for de kombinerte indikatorene og tilhørende skårverdier

Indikator (antall underliggende ja/nei-spørsmål)	Antall JA						
	0	1	2	3	4	5	6
1.1.6 Grad av kunnskap om klimatilpasningsutfordringer (5)	0	1	2	3	4	5	
2.1.4 Grad av ansvarliggjøring og involvering (3)	0	1,67	3,33	5			
2.2.7 Grad av forankring i planverk og reguleringer (6)	0	0,83	1,67	2,5	3,33	4,17	5

Når det gjelder vektning kan man velge å ta utgangspunkt i fasene (f.eks. lik vektning av de fem fasene), forholdene, eller indikatorene. Her er det kun én indikator per forhold, dvs. at det er like mange forhold som indikatorer, og det spiller derfor ingen rolle om man gir vektor på forhold²⁶ eller indikatorer.

Siden man ikke opererer med forhold i Menon (2018), velger vi vektning direkte på indikatorer. I utgangspunktet velges lik vektning, dvs. 1/8 (=0,125=12,5%). Det vil være opp til brukerne/kommunen å vurdere om noen av indikatorene er viktigere enn andre og dermed gis høyere vekt. (Totalfordelingen må selvsagt være 100%).

²⁶ Med mange flere forhold og indikatorer ville vi normalt også vektet forholdene/"faktorene"/temaene, og dernest indikatorene. Dette kan betegnes som et "faktor-basert system for kvantifisering". (Her kunne man også skilt mellom ulike typer/dimensjoner av forhold/indikatorer, som økonomiske, samfunnsmessige, miljømessige, osv.).

Trinn 8: Angi måleverdier for indikatorene (utfør målingen)

Vi gjør en antakelse om at det svares JA på to av spørsmålene i hver av de tre kombinerte indikatorene, hvor vi da kan fastsette skår ut ifra tabell 4.17. For de øvrige indikatorene er vi avhengig av fastsettelse av grenseverdier, men for å vise beregningene gjør vi direkte antakelser om skårverdier. Disse er vist i tabell 4.18.

Tabell 4.18 Skårverdier (fiktive/antatte verdier)

Indikator	Skår
1.1.6 Grad av kunnskap om klimatilpasningsutfordringer	2,0
2.1.4 Grad av ansvarliggjøring og involvering	3,33
2.2.7 Grad av forankring i planverk og reguleringer	1,67
3.1.1 Andel godkjente byggeområder som ligger i klimarisikoutsatte områder (ras, flom, stormflo, etc.)	0,5
3.8.1 Andel av kommunens budsjett som går til klimatilpasningstiltak	4,0
4.2.1 Antall gjennomførte beredskapsøvelser knyttet til ekstremvær siste år	2,0
4.4.1 Andel av kommunens budsjett som går til ressurser for å håndtere ekstremværhendelser	2,5
5.1.1 Antall ekstremværhendelser (egne eller andres) man har lært av og som har resultert i konkrete endringer (i planer, tiltak, osv.)	3,0

Trinn 9: Gjennomfør beregningene (skår og resiliensnivå)

Når skårverdiene er fastsatt kan beregningene gjennomføres. Her er skårverdiene allerede beregnet/fastlagt som vist i tabell 4.18. Skårverdier og resiliensnivå er vist i tabell 4.19.

Tabell 4.19 Skårverdier og resiliensnivå

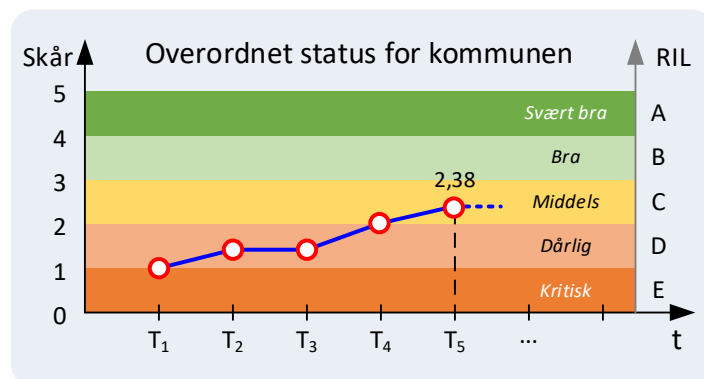
Indikator	Skår	Resiliensnivå
1.1.6 Grad av kunnskap om klimatilpasningsutfordringer	2,0	C
2.1.4 Grad av ansvarliggjøring og involvering	3,33	B
2.2.7 Grad av forankring i planverk og reguleringer	1,67	D
3.1.1 Andel godkjente byggeområder som ligger i klimarisikoutsatte områder (ras, flom, stormflo, etc.)	0,5	E
3.8.1 Andel av kommunens budsjett som går til klimatilpasningstiltak	4,0	A
4.2.1 Antall gjennomførte beredskapsøvelser knyttet til ekstremvær siste år	2,0	C
4.4.1 Andel av kommunens budsjett som går til ressurser for å håndtere ekstremværhendelser	2,5	C
5.1.1 Antall ekstremværhendelser (egne eller andres) man har lært av og som har resultert i konkrete endringer (i planer, tiltak, osv.)	3,0	B
Totalt	2,38	C

En total aggregert skårverdi fås som summen av vektete skårverdier for enkeltindikatorene. Siden vekten her er antatt lik (12,5%), kan vi summere skårverdien og dele på antallet indikatorer, altså $19/8=2,38$. Dette tilsvarer resiliensnivå C (middels).

Dersom vi har mange indikatorer og forhold, og ulik vekting, så kan beregningene bli såpass omfattende at vi benytter eksempelvis Excel eller et web-verktøy (slik som ResiliN web-verktøyet vist i vedlegg H). Da vil vi også få aggregerte skårverdier og resiliensnivå på forhold og faser, i tillegg til totalt for området/ kommunen.

Trinn 10: Vis status, trender, styrker og svakheter, forbedringsbehov, osv.

Statusen er vist i tabell 4.19, og trenden kan angis som vist i figur 4.29.



Figur 4.29 Overordnet status og trend for kommunens arbeid med klimatilpasning

Her er det antatt at det har vært gjort fire tidligere målinger, eksempelvis årlige målinger. Siste måling viser skårverdi 2,38.

Dersom det er benyttet mange forhold og indikatorer kan status på underliggende nivå vises med trestrukturdiagram (Tree Map), som benyttes i ResiliN web-verktøyet.

Med få indikatorer, som her, kan man se statusen direkte fra tabell 4.19. Spesielt indikator 2.2.7 og 3.1.1 er det behov for å forbedre, mens man skårer svært bra på indikator 3.8.1.

For den enkelte kommunen vil en tydelig synliggjøring av status og utvikling kunne motivere til kontinuerlig innsats og forbedring av klimatilpasningen, og for myndigheter som eksempelvis Miljødepartementet eller Statsforvalteren kan dette gi en god oversikt og innsikt med hensyn til kommunenes arbeid med klimatilpasning og benyttes i en løpende oppfølging.

De fleste av indikatorene i tabell 4.19 er generelle og kan til en viss grad benyttes for sammenlikning av kommunene, og dermed bidra til erfaringsutveksling mellom kommunene i arbeidet med klimatilpasning. Dette avhenger imidlertid av hvordan grenseverdiene fastsettes, og at de samme indikatorene benyttes, dvs. at man har et felles sett med indikatorer. I tillegg kan kommunene ha sine egne tilpassede indikatorer.

CIRAM og relasjon til begrepene risiko og sårbarhet i ROS-analyser

Anvendelsen av CIRAM for å måle og vurdere klimatilpasningsarbeidet, slik det er beskrevet her, er en "spesialanvendelse" av metoden. For å få en bedre forståelse av metoden og av resiliens i forhold til kommuners arbeid med styring av risiko, vil vi kort forklare en "normal" anvendelse av resiliensvurderingen.

Kommunene er pålagt å gjennomføre helhetlige risiko- og sårbarhetsanalyser (ROS-analyser), og DSB har laget en veileder for gjennomføring av ROS-analyser (DSB, 2014). Her vises det til standarder for risikoanalyse slik som NS 5814:2008 og ISO 31000:2009. NS 5814 viser til en rekke typer av risikoanalyser, hvorav én av disse er ROS-analyser. Standarden omtaler sårbarhet i liten grad, fordi dette begrepet ikke brukes i de fleste typer risikoanalyser. ISO 31000 nevner ikke sårbarhet ("vulnerability"). I den nylig utgitte nye versjonen av NS 5814:2021 inngår begrepet sårbarhet på tilsvarende måte som i DSBs veileder, og det vises til at dette begrepet innføres blant annet fordi det benyttes innenfor tilsiktede hendelser og sikring ("security").

Hvorfor denne diskusjonen rundt begrepet sårbarhet? Jo, fordi dette omtales som å være det motsatte av "robusthet", mens et mer dekkende begrep er "resiliens", hvor robusthet inngår som et av flere elementer.²⁷ Det vil si at en resiliensvurdering ligger nær opp mot en sårbarhetsvurdering i en ROS-analyse "bare med motsatt fortegn". I en sårbarhetsvurdering ser man på et systems manglende evne til å motstå en hendelse og manglende evne til å tåle en hendelse hvis den først inntreffer, mens man for en resiliensvurdering kan fjerne ordet "manglende", det vil si at det er evnen til å motstå og tåle en hendelse man vurderer.²⁸

Sårbarhetsvurderingen i en ROS-analyse er kvalitativ og relativt grov (DSB, 2019), mens dette kan gjøres mer detaljert og systematisk med CIRAM gjennom vurdering av fasene før, under og etter en hendelse. Dessuten er analysen med bruk av CIRAM semi-kvantitativ gjennom å beregne et resiliensnivå. På den annen side så er ikke analysen med bruk av CIRAM like dekkende hva angår typer av uønskede hendelser.

ROS-analysen dekker alle aktuelle (kjente) uønskede hendelser og vurderingen benyttes blant annet til å dimensjonere beredskapen gjennom etablering av beredskapsplaner, og bidrar dermed også til evnen til å motstå og tåle en hendelse, altså "resiliensen", ut fra en risikobasert tilnærming.

I CIRAM velges én eller et fåtall ekstremhendelser for å "stress-teste" hvor resilient man er mot denne/disse ekstremhendelsene. ROS-analyser og derigjennom forståelse av risiko bidrar både til resiliens og til valg av ekstremhendelser. Én aktuell ekstremhendelse er naturhendelse som følge av ekstremvær, som også kan være basert på informasjon om klimarelatert ekstremvær, hvor høye alternativer fra nasjonale framskrivninger legges til grunn (såkalt RCP8.5²⁹). Brukeren velger de ekstremhendelsene man er mest bekymret for uavhengig av sannsynlighet.³⁰ Dette kan også ta utgangspunkt i én ekstremhendelse innenfor hver av hovedtypene naturhendelser, store ulykker og tilsiktede hendelser, jfr. DSBs veileder (2014).

I henhold til forskrift for kommunal beredskapsplikt skal den helhetlige ROS-analysen blant annet dekke *"særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur"*. Slike utfordringer kan mer systematisk og detaljert avdekkes med CIRAM ved at man for hver ekstremhendelse vurderer hvordan alle relevante kritiske infrastrukturer innenfor området/kommunen vil kunne håndtere ekstremhendelsen. CIRAM kan også benyttes for det påfølgende punktet som krever at ROS-analysen skal dekke *"kommunens evne til å opprettholde sin virksomhet når den utsettes for en uønsket hendelse og evnen til å gjenoppta sin virksomhet etter at hendelsen har inntruffet."*³¹

"Spesialanvendelsen" av CIRAM til måling og vurdering av klimatilpasningsarbeidet er mer som et alternativ til steg 4 og 5 i MRE-rammeverket foreslått av Menon (2018). Anvendelsen av CIRAM er imidlertid bedre i samsvar med det opphavelige MRE-rammeverket (Monitoring, Reporting and Evaluation) foreslått av EEA (2015) hvor man går mer rett på måling ved hjelp av indikatorer.

²⁷ Bl.a. benyttes robusthet som mål på gjenværende kritisk funksjonsevne (jfr. figur 4.27), men sier ikke noe om varigheten av tap av kritisk funksjon. Hvor raskt man gjenvinner funksjonen ("rapid recovery") beskrives bl.a. med begrepet "rapidity" (hurtighet/gjenvinningshurtighet).

²⁸ Dette er også et aspekt ved resiliens som skiller det fra risiko og sårbarhet, dvs. at tankesettet er grunnleggende positivt gjennom å vektlegge hva som er bra, i stedet for feil og svakheter: Hva må til for å evne å motstå og tåle en hendelse?

²⁹ RCP står for Representative Concentration Pathway, og RCP8.5 er utviklingsbanen hvor vi fortsetter som i dag og ikke gjør noe for å begrense klimagassutslippene. Jorda vil per kvadratmeter oppta 8.5 watt ekstra i 2100.

³⁰ En "rasjonell" vurdering av sannsynlighet og konsekvens ved en risikobasert tilnærming gjør at man ikke fanger opp uforutsette og svært usannsynlige hendelser. Mange historiske hendelser har nettopp vært uforutsette og i forkant svært usannsynlige hendelser. Viktige antakelser i ROS-analysen som forhåndsevakuering kan vise seg å ikke holde stikk.

³¹ Selv om CIRAM benytter en indirekte vurdering av resiliens, og ikke ser direkte på resilienskurven (jfr. figur 4.27), så kan man inkludere en enkel vurdering av robustheten (gjenværende funksjonsevne) og hvor raskt man gjenopptar virksomheten etter hendelsen. Dette kan også sammenholdes med eventuelle krav eller mål.

Referanser

- Alexander, E., 2013. Resilience and disaster risk reduction: an etymological journey. *Nat Hazard Earth Syst Sci* 13:2707–16.
- Amundsen, H., Berglund, F., Westskogh, H., 2010. Overcoming barriers to climate change adaptation-a question of multilevel governance? *Environment and Planning C: Government and Policy* 28 (2): 276–89.
- Aven, T., 2017. How some types of risk assessments can support resilience analysis and management. *Reliability Engineering and System Safety* 167(2017), 536-543.
- Barzelay, U., I. Shapira, T. Knappe, and P. Klimek, 2018. SmartResilience D3.5: Interactive Visualization as support to indicator-based decision making. <http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.5.pdf>.
- Borge, A.I.H., 2010. Resiliens – risiko og sunn utvikling. Oslo: Gyldendal forlag.
- Cook, R. I., Woods, D. D. and Miller, C., 1998. A Tale of Two Stories: Contrasting Views on Patient Safety. Chicago, IL: National Patient Safety Foundation.
- Departementene, 2019. Nasjonal strategi for digital sikkerhet. <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/>
- Depina, I. og Øien, K., 2021. Klima-resilient infrastruktur. Klima 2050 Report No 27, ISBN: 978-82-536-1709-1.
- Direktoratet for samfunnssikkerhet og beredskap (DSB), 2014. Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen, ISBN 978-82-7768-344-7.
- Direktoratet for samfunnssikkerhet og beredskap (DSB), 2016. Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? ISBN 978-82-7768-412-3 (PDF).
- Direktoratet for samfunnssikkerhet og beredskap (DSB), 2019a. Analyser av krisescenarier 2019, ISBN 978-82-7768-472-7 (PDF).
- Direktoratet for samfunnssikkerhet og beredskap (DSB), 2018. DSB årsrapport 2017, ISBN 978-82-7768-465-9 (PDF).
- Direktoratet for samfunnssikkerhet og beredskap (DSB), 2019. DSB årsrapport 2018, ISBN 978-82-7768-475-8 (PDF).
- Direktoratet for samfunnssikkerhet og beredskap (DSB), 2020. DSB årsrapport 2019b. <https://www.dsb.no/rapporter-og-evalueringer/dsb-arsrapport-2019/>
- DNV GL, 2020. Resiliens mot cyberhendelser og kan blokkjede bidra? Rapport nr.: 2019-0825, Rev. 0.
- Drikkevannsforskriften, 2016. Forskrift om vannforsyning og drikkevann. (FOR-2016-12-22-1868). <https://lovdata.no/dokument/SF/forskrift/2016-12-22-1868?q=Forskrift%20om%20vannforsyning%20og%20drikkevann>
- EC, 2019. European Commission. The European Green Deal. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Brussels, 11.12.2019 COM(2019) 640 final.
- EEA, 2015. National monitoring, reporting and evaluation of climate change adaptation in Europe. EEA Technical Report, no. 20.
- Energiloven, 2018. Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (LOV-1990-06-29-50). <https://lovdata.no/dokument/NL/lov/1990-06-29-50>
- Etterretningstjenesten, 2020. Fokus 2020. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer. <https://forsvaret.no/fokus>
- Folkehelseinstituttet (FHI), 2020a. COVID-19, Ukerapport – uke 40, 07.10.2020, <https://www.fhi.no/contentassets/8a971e7b0a3c4a06bdf381ab52e6157/vedlegg/andre-halvar-2020/2020.10.07-ukerapport-uke-40-covid-19.pdf>
- Folkehelseinstituttet (FHI), 2020b. COVID-19, Ukerapport: 14 2020 (30.3-5.4.2020), <https://www.fhi.no/contentassets/8a971e7b0a3c4a06bdf381ab52e6157/vedlegg/forste-halvar-2020/07.04.20---ukerapport-14-covid-19.pdf>

- Folkehelseinstituttet (FHI), 2020c. COVID-19, Ukerapport – uke 45, 11.11.2020, <https://www.fhi.no/contentassets/8a971e7b0a3c4a06bdf381ab52e6157/vedlegg/andre-halvar-2020/2020.11.11-ukerapport-uke-45-covid-19.pdf>
- Forskrift om krav til beredskapsplanlegging, 2001. Forskrift om krav til beredskapsplanlegging og beredskapsarbeid mv. etter lov om helsemessig og sosial beredskap. (FOR-2001-07-23-881). <https://lovdata.no/dokument/SF/forskrift/2001-07-23-881>
- Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2015. Støtte og samarbeid – en beskrivelse av totalforsvaret i dag. ISBN 978-82-7924-080-8.
- FFI-Rapport 19/00363: Brynhild Stavland, Janita Andreassen Bruvoll, Resiliens – hva er det og hvordan kan det integreres i risikostyring? Mars 2019, <https://www.ffi.no/no/Rapporter/19-00363.pdf>
- Fisher R.E., Bassett G.W., Buehring W.A., Collins M.J., Dickinson D.C., Eaton L.K., ... Peerenboom J.P., 2010. Constructing a resilience index for the enhanced critical infrastructure protection program, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-10-9, Argonne, IL, USA.
- Grøtan, T.O., 2020. Training for Operational Resilience Capabilities (TORC); advancing from a positive first response. ESREL 2020 PSAM 15, Venice, Italy.
- Haimes, Y. V., 2009. On the Definition of Resilience in Systems. Risk Analysis 29(4), 498-501. Risk Analysis, Vol. 29, No. 4.
- Helseberedskapsloven, 2001. Lov om helsemessig og sosial beredskap. (LOV-2000-06-23-56). <https://lovdata.no/dokument/NL/lov/2000-06-23-56?q=helseberedskapsloven>
- Helsedirektoratet, 2020. <https://www.helsedirektoratet.no/faglige-rad/pandemiplanlegging/bakgrunn-for-pandemiplanlegging/ansvar-og-roller-ved-en-pandemi>
- Holling, C. S., 1973. Resilience and stability of ecological systems, Ann. Rev. Ecol. Syst., 4, 1–23.
- Hollnagel, E., 2008. The changing nature of risk. Ergonomics Australia, 22(1-2), 33-46.
- Hollnagel, E., 2015. Introduction to the Resilience Analysis Grid (RAG). <https://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf>
- Hollnagel, E., 2019. Hollnagel: What is Resilience Engineering? <https://www.resilience-engineering-association.org/blog/2019/11/09/what-is-resilience-engineering/>
- Hopkins, A., 2009. Thinking about process safety indicators. Safety Science 47, 460–465.
- HSAC, 2006. Report of the Critical Infrastructure Task Force. Homeland Security Advisory Council.
- IMPROVER Consortium, 2016. Deliverable 2.2: Report of criteria for evaluating resilience. www.improverproject.eu/2016/06/23/deliverable-2-2-report-of-criteria-for-evaluatingresilience/
- Instruks for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet beredskap og krisehåndtering, 2015. Instruks for fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet, beredskap og krisehåndtering. (FOR-2015-06-19-703). <https://lovdata.no/dokument/INS/forskrift/2015-06-19-703?q=FOR-2015-06-19-703>
- International Risk Governance Council, 2016a. Resilience: Approaches to Risk Analysis and Governance. In Resource Guide on Resilience. Lusanne: EPFL International Risk Governance Center.
- International Risk Governance Council, 2016b. Resilience in IRGC's Recommendations for Risk Governance (Risk Governance Framework). In Resource Guide on Resilience. Lusanne: EPFL International Risk Governance Center.
- IPCC, 2014. "Summary for Policymakers." In Climate Change 2014: Impacts, Adaptation and Vulnerability - Contributions of the Working Group II to the Fifth Assessment Report, edited by C.B. Field, V.R. Barros, D.J. Dokken, K.J. Mach, M.D. Mastrandrea, T.E. Bilir, M. Chatterjee et al. Cambridge and New York: Cambridge University Press.
- ISO 22301:2012. Societal security – Business continuity management systems – Requirements.
- ISO 31000:2009. Risikostyring: Prinsipper og retningslinjer. Norsk Standard NS-ISO 31000:2009.
- ISO 31000:2018. Risikostyring: Retningslinjer. Norsk Standard NS-ISO 31000:2018 (no).
- ISO 31050. Guidance for Managing Emerging Risks to Enhance Resilience. (Under utarbeidelse).
- ISO Guide 73:2009. Risikostyring: Terminologi. Standard Norge Guide SN-ISO 73:2009.

- JD, 2016. Risiko i et trygt samfunn. (Meld. St. 10 2016-2017). Oslo: Departementenes servicesenter, Informasjonsforvaltning.
- Jovanović, A., Klimek, P., Renn, O., Schneider, R. Øien, K., Brown, J., DiGennaro, M., Liu, Y., Pfau, V., Jelić, M., Rosen, T., Caillard, B., Chakravarty, S., Chhantyal, P, 2020. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. *Environment Systems and Decisions*, <https://doi.org/10.1007/s10669-020-09779-8>. © Springer Science+Business Media, LLC, part of Springer Nature 2020.
- Kaplan, S. and Garrick, B.J., 1981. On the Quantitative Definition of Risk. *Risk Analysis*, 1, 11-27. <http://dx.doi.org/10.1111/j.1539-6924.1981.tb01350.x>.
- Kraftberedskapsforskriften, 2019. Forskrift om sikkerhet og beredskap i kraftforsyningen. (FOR-2012-12-07-1157). <https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157>
- Lange, D., Honfi, D., Sjøstrøm, J., Theocharidou, M., Giannopoulos, G., Reitan, N.K., ... Lin, M.L., 2017. IMPROVER D5.1 Framework for implementation of resilience concepts to Critical Infrastructure. <http://media.improverproject.eu/2018/02/D5.1.pdf>.
- Leveson, N., 2020. Safety III: A Systems Approach to Safety and Resilience. MIT Engineering Systems Lab. <http://sunnyday.mit.edu/safety-3.pdf>.
- Lindley, D.V., 2006. Understanding Uncertainty. Wiley 2014. ISBN 9780470043837.
- Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... Thiel-Clemen, T., 2014. Changing the Resilience Paradigm. *Nature Climate Change* 4(6), 407–409. <http://www.nature.com/doi/10.1038/nclimate2227>.
- Meld. St. 33 (2012-2013). Klimatilpasning i Norge.
- Menon, 2018. MRE-system og indikatorer for lokal klimatilpasning. Menon-Publikasjon 91.
- National Academy of Sciences, 2012. Disaster Resilience – A National Imperative. The National Academies Press, Washington D.C.
- NOU 2010: 10. Tilpassing til eit klima i endring. Samfunnet si sårbarheit og behov for tilpassing til konsekvensar av klimaendringane.
- NOU 2000: 24. Et sårbart samfunn – utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.
- NS 5814:2008. Krav til risikovurderinger. Standard Norge.
- NS 5814:2021. Krav til risikovurderinger. Standard Norge.
- NS 5830:2012. Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi. Standard Norge.
- NS-IEC 31010:2019. Risikostyring – Metoder for risikovurdering.
- NSM/POD/PST, 2015. Terrorsikring: En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger (2015). Utgitt av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste. https://www.politiet.no/globalassets/03-rad-og-forebygging/beredskap/terssikring_en_veileder
- NSM, 2016. Risikovurdering for sikring. Håndbok, Nasjonal sikkerhetsmyndighet. <https://docplayer.me/67961188-Risikovurdering-for-sikring.html>
- NSM, 2020a. Risiko 2020. <https://nsm.no/aktuelt/risiko-2020>
- NSM, 2020b. NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0. <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt>
- NSM, 2020c. Støtteprodukter NSMs grunnprinsipper for IKT-sikkerhet, 2020-07-02. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/stotteprodukter/>
- NVE, 2010. Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. Veileder nr: 2-2010, ISSN: 1501-0678.
- NVE, 2018. Foreløpig tilleggsveileder til kraftberedskapsforskriften. Oppdateringer etter revisjon. Norges vassdrags- og energidirektorat, 2018.
- NVE, 2021. Veiledning til kraftberedskapsforskriften. <https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap/veiledning-til-kraftberedskapsforskriften/>

- Parsons, M., Glavac, S., Hastings, P., Marshall, G., McGregor, J., McNeill, J., Morley, P., Reeve, I. and Stayner, R., 2016. Top-down assessment of disaster resilience: A conceptual framework using coping and adaptive capacities. *International Journal of Disaster Risk Reduction* 19(2016), 1-11. doi: 10.1016/j.ijdr.2016.07.005
- Poulin, C. & Kane, M., 2021. Infrastructure Resilience Curves: Performance Measures and Summary Metrics. https://www.researchgate.net/publication/348958362_Infrastructure_Resilience_Curves_Performance_Measures_and_Summary_Metrics
- Petit, F.D., Bassett, G.W., Black, R., Buehring, W.A., Collins, M.J., Dickinson, D.C., ... Peerenboom J.P., 2013. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-13-01, Argonne, IL, USA.
- Petroleumstilsynet (Ptil), 2015. Veiledning til rammeforskriften. (16.12.2020). https://www.ptil.no/contentassets/332166193108427e978accb21449436c/rammeforskriften_veiledning_n-1.pdf
- Petroleumstilsynet (Ptil), 2017. Prinsipper for barrierestyring i petroleumsvirksomheten. Barrierenotat 2017. <https://www.ptil.no/contentassets/11851dc03a84473e8299a2d80e656356/barrierenotat--2017.pdf>
- Plan- og bygningsloven, 2008. Lov om planlegging og byggesaksbehandling. (LOV-2008-06-27-71). <https://lovdata.no/dokument/NL/lov/2008-06-27-71?q=Lov%20om%20planlegging%20og%20byggesaksbehandling>
- PST, 2020. Nasjonal trusselvurdering 2020. <https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/>
- Rasmussen, J., 1990. Role of Error in Organizing Behavior. *Ergonomics*, 33, 1185-1190.
- Reason, J., 1997. Managing the Risks of Organizational Accidents. Brookfield, VT: Ashgate Publishing Company.
- Regjeringen, 2020. Liste over kritiske samfunnsfunksjoner. <https://www.regjeringen.no/contentassets/8da70b8196a24296ae730eaf99056c1b/liste-over-kritiske-samfunnsfunksjoner-tabell.pdf>
- Regjeringen, 2020b. Tidslinje: myndighetenes håndtering av koronasituasjonen. <https://www.regjeringen.no/no/tema/Koronasituasjonen/tidslinje-koronaviruset/id2692402/>
- RESILENS Consortium, 2016a. Qualitative, Semi-Quantitative and Quantitative Methods and Measures for Resilience Assessment and Enhancement. Ireland. <http://resilens.eu/wp-content/uploads/2016/08/D2.2-Methods-for-Resilience-Assessment-Final.pdf>
- RESILENS Consortium, 2016b. Resilience Management Matrix and Audit Toolkit. Ireland. <http://resilens.eu/wp-content/uploads/2016/06/D2.3-Resilience-Management-Matrix-and-Audit-Toolkit.pdf>
- Riksrevisjonen, 2021. Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen. Dokument 3:7 (2020-2021). ISBN-978-82-8229-504-8.
- Rochlin, G. I., 1999. Safe operation as a social construct. *Ergonomics*, 42 (11), 1549-1560.
- Rosenqvist, H., Reitan, N.K., Petersen, L. and Lange, D., 2018. ISRA: IMPROVER societal resilience analysis for critical infrastructure. I Haugen, S., Barros, A., Gulijk, C., Kongsvik, T and Vinnem, J.E. (Red.), Safe Societies in a Changing World, 28th International European Safety and Reliability Conference (ESREL 2018) (s. 1923-1931). Taylor & Francis Group: London.
- Sachs, R., Florin M.-V. and Eller, E., 2019. SmartResilience D6.7: Views from Insurance about the SmartResilience Project. <http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD6.7.pdf>
- Samfunnssikkerhetsinstruksen, 2017. Instruks for departementenes arbeid med samfunnssikkerhet. (FOR-2017-09-01-1349). <https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349>
- Schönthaler, K., von Andrian-Werburg, S., 2015. Evaluation of the German Strategy for Adaption to Climate Change (DAS) – Reporting and Closing Indicator Gap. Dessau-Roßlau: Umweltbundesamt.

- Setola, R., Luijff, E., Theocharidou, M., 2016. Critical Infrastructures, Protection and Resilience. In R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures*, Studies in Systems, Decision and Control 90, DOI 10.1007/978-3-319-51043-9-1.
- Sikkerhetsloven, 2019. Lov om nasjonal sikkerhet. (LOV-2018-06-01-24). <https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven>
- SINTEF, 2014. Beredskapsplan, Fortrolig.
- Sivertsen, E., Sandberg, E., Fjellheim, K., Solli, J., Strømø, E-B., Lilledal, S., Andreassen, S-A. og Time, B., 2021. Indikatorer for måling av klimatilpasning av arealer, bygninger og infrastruktur i kommuner: Anvisning og rammeverk. Klima2050 Report No. 26, ISBN: 978-82-536-1708-4.
- Sivilbeskyttelsesloven, 2011. Lov om kommunal beredskapsplikt, sivilebeskyttelsestiltak og Sivilforsvaret. (LOV-2010-06-25-45). <https://lovdata.no/dokument/NL/lov/2010-06-25-45?q=sivilbeskyttelsesloven>
- Sletten, S., 2018. Oppdragsrelatert risikovurdering i politiet: Hvilken metodikk egner seg best? Masteroppgave, Universitetet i Stavanger.
- Smittevernloven, 2020. Lov om vern mot smittsomme sykdommer. (LOV-1994-08-05-55). <https://lovdata.no/dokument/NL/lov/1994-08-05-55>
- Solecki, W., Rosenzweig, C., Blake, R., de Sherbinin, A., Matte, T., et al. 2015. New York city panel on climate change 2015 report chapter 6: Indicators and monitoring. *Annals of the New York Academy of Sciences* 1336 (1): 89–106.
- SRA, 2018. Society for Risk Analysis Glossary. <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf>
- Tiernan, A., Drennan, L., Nalau, J., Onyango, E., Morrissey, L. and Mackey, B., 2019. A review of themes in disaster resilience literature and international practice since 2012, *Policy Design and Practice*, 2:1, 53-74, DOI: 10.1080/25741292.2018.1507240.
- UNISDR: Terminology on Disaster Risk Reduction. United Nations International Strategy for Disaster Risk Reduction, Geneva, 2009.
- Veglova, 2020. Lov om vegar. (LOV-1963-06-21-23). <https://lovdata.no/dokument/NL/lov/1963-06-21-23>
- VG.no, 2020. https://www.vg.no/spesial/2020/corona/verden/?utm_source=corona-widget&utm_term=d7#world
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D., 1999. Organizing for high reliability: Processes of collective mindfulness. *Research in Organizational Behavior*, 21, 13-81.
- Westrum R, and Adamski A., 1999. Organizational factors associated with safety and mission success in aviation environments. In: Garland DJ, Wise JA, Hopkins VD, eds. *Aviation human factors*. Hillsdale, NJ: Lawrence Erlbaum.
- Woods, D. D., Johannesen, L. J., Cook, R. I., & Sarter, N. B., 1994. *Behind Human Error: Cognitive Systems, Computers, and Hindsight* (State-of-the-art report). Wright-Patterson Air Force Base, OH: Crew System Ergonomics Information Analysis Center.
- Woods, D.D., and Wreathall, J., 2003. Managing Risk Proactively: The Emergence of Resilience Engineering. https://www.researchgate.net/publication/228711828_Managing_Risk_Proactively_The_Emergence_of_Resilience_Engineering
- Woods, D.D., 2006. Essential Characteristics of Resilience. In: N. Leveson, E. Hollnagel, and D.D. Woods (eds), *Resilience engineering: concepts and precepts*: 21–34. Aldershot: Ashgate.
- Wreathall, J., 2006. Properties of resilient organizations: an initial view. In: N. Leveson, E. Hollnagel, and D.D. Woods (eds), *Resilience engineering: concepts and precepts*: 21–34. Aldershot: Ashgate.
- Øien, K., 2001a. Risk indicators as a tool for risk control. *Reliability Engineering and System Safety*, 74 (2001) 129-146.
- Øien, K., 2001b. A framework for the establishment of organizational risk indicators. *Reliability Engineering and System Safety*, 74 (2001b) 147-168.
- Øien, K., I.B. Utne, and I.A. Herrera. 2011a. Building safety indicators. Part 1 – theoretical foundation. *Safety Science* 49, no.2: 148–61.

- Øien, K., Utne, I.B., Tinmannsvik, R.K., Massaiu, S., 2011b. Building Safety Indicators. Part 2 – Application, practices and results. *Safety Science* 49(2), pp. 162-171.
- Øien, K., Massaiu, S., Tinmannsvik, R.K., 2012. Guideline for implementing the REWI method; Resilience based Early Warning Indicators. SINTEF report A22026, Trondheim, Norway.
- Øien, K., 2013. Remote operation in environmentally sensitive areas: development of early warning indicators. *Journal of Risk Research*, Volume 16 (3-4) s. 323-336.
- Øien, K., 2016a. Two Applications of Resilience Concepts and Methods: Offshore Installations and Critical Infrastructures. IRGC (2016). Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center. v29-07-2016.
- Øien, K., 2016. Risikobegrepet i petroleumsvirksomheten. Notat, SINTEF Digital. <https://hdl.handle.net/11250/2757403>.
- Øien, K., Bodsberg, L. and Jovanovic, A., 2018. Resilience assessment of smart critical infrastructures based on indicators. *Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds).* 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7.
- Øien, K., Jovanović, A., Grøtan, T.O., Choudhary, A., Øren, A., Tetlak, K., Bodsberg, L. and Jelic, M., 2017a. SmartResilience D3.2: Assessing resilience of SCIs based on indicators. Initial report. <http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.2.pdf>.
- Øien, K., Bodsberg, L., Hoem, Å., Øren, A., Grøtan, T.O., Jovanović, A., ... Tuurna, S., 2017b. SmartResilience D4.1: Supervised RIs: Defining resilience indicators based on risk assessment frameworks. <http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD4.1.pdf>.
- Øien, K., Jovanović, A., Grøtan, T.O., Choudhary, A., Øren, A., Tetlak, K., Bodsberg, L. and Jelic, M., 2019a. SmartResilience D3.8: Assessing resilience of SCIs based on indicators. Update. <http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.8.pdf>.
- Øien, K., Jovanović, A., Bodsberg, L., Øren, A., Choudhary, A., Sanne, J., ... Bezrukov, D., 2019b. SmartResilience D3.6: Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures (SCIs). <http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.6.pdf>.
- Aall, C., Ekström, F., Heiberg, E., Storm, H., 2009. Lokal sårbarhet for klimaendringer. Demonstrasjon av metoder for kartlegging av den institusjonelle sårbarheten for klimaendringer. Vestlandsforskningsrapport 6/2009.
- Aall, C., Heiberg, E., Simonsen, M., Jakob, H., Ekström, F., 2012. Korleis vurdere effekten av ein regional klimapolitikk? Sluttrapport frå eit prosjekt om utvikling av eit indikatorbasert system for vurdering av måloppnåing i Fylkesdelplan klima og miljø for Sogn og Fjordane fylkeskommune. Vestlandsforskningsrapport, no. 7.
- Aall, C., Nordland, I., 2003. Indikatorer for vurdering av lokal klimasårbarhet. Vestlandsforskningsrapport, no. 15.

Vedlegg A: Resiliens generelt

Her skal vi se litt på ordet og begrepet resiliens generelt, opphavet til begrepet og andre fagområder hvor resiliens benyttes. Til slutt vil vi kort omtale Resilience Engineering (RE), som er en relativt ny retning innen fagområdet sikkerhet.

En av utfordringene med innføringen av resiliens i Norge kan antakelig tilskrives at vi ikke har noe forhold til ordet resiliens, og at det ikke finnes andre (godt nok) dekkende ord for resiliens. Forskjellige oversettelser har blitt foreslått, men FFI (2019) har, i likhet med mange andre, foreslått å bruke ordet resiliens på norsk, og ikke ord som robusthet eller motstandsdyktighet (som inngår i, men ikke er fullt ut dekkende for resiliens).

Innenfor noen fagområder har man benyttet det fornorskede ordet resiliens siden om lag 2010. Eksempelvis innenfor psykologi (Borge, 2010).

I engelskspråklige land er imidlertid resiliens (*resilience*) et allment kjent ord/begrep. Et eksempel på dette er hentet fra filmen Cliffhanger fra 1993 med Sylvester Stallone i hovedrollen. Skurken (Qualen), overrasket over at helten (Walker – spilt av Sylvester Stallone), dukker opp igjen etter å ha forsøkt å ta livet hans flere ganger, utbryter: "Walker. You **resilient** bastard. So, you're still alive".



Et annet eksempel er i sangteksten til bandet Born of Osiris:

*Death is not an option – The story is not over – It's unlikely we will die – **Resilience** is our power – Driven by our actions – Our lives are here and now.*

Begrepet oppsto imidlertid lenge før det kom inn i det engelske språket (Alexander, 2013), men ifølge Alexander ser det ut til at det er få forskere som kjenner til den lange historien til begrepet resiliens.

Resiliens stammer fra det latinske *resilire*, *resilio*, som betyr å sprette eller rekylere, som vist i sitatet under.

*Sagitta in lapidem numquam figitur, interdum **resiliens** percutit dirigentem.*

"An arrow never lodges in a stone: often it recoils upon its sender."

St John Chrysostom (ca. 347–407), Erkebiskop i Konstantinopel

Begrepet var i bruk allerede i det første århundre innenfor rettsvitenskap og litteratur. Senere ble det tatt i bruk innenfor statsvitenskap, og det ble brukt i forbindelse med etableringen av den moderne vitenskapelige metode (av Francis Bacon, som var den første til å bruke det engelske begrepet "resilience" vitenskapelig).

I første halvdel av det nittende århundre var resiliens fortsatt i bruk i betydningen sprette eller sprette tilbake (*bounce back*). Dette samsvarer også med å gjenvinne/gjenopprette (*recover*).

I 1858 ble begrepet første gang brukt i mekanikk for å beskrive styrken og seigheten til stålbjelker. En resilient stålbjelke tåler en last ved å motvirke den med styrke (stivhet) og absorbere den med deformasjon (seighet). Omtrent på samme tid ble begrepet også tatt i bruk innenfor kirurgi, anatomi og urmakerfaget.

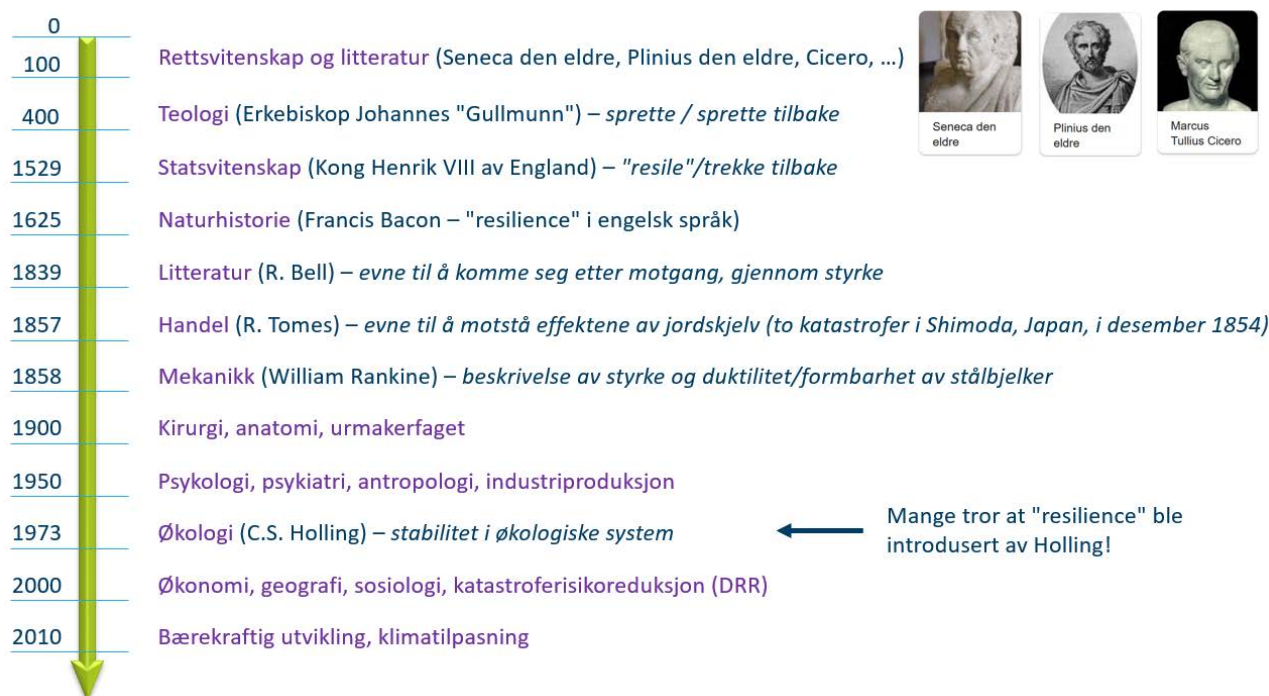
På 1950-tallet begynte man å bruke begrepet innenfor psykologi og etter hvert spesielt knyttet til psykiatriske problemer hos barn (herunder begrepet "løvetannbarn"). Det ble da også brukt innenfor antropologi og industriproduksjon. På 1960- og 1970-tallet ble begrepet tatt i bruk innenfor økologi, og arbeidet til Holling (1973) ble så kjent at mange tror at dette var starten på bruken av begrepet resiliens (inklusive Tiernan m.fl., 2019). Begrepet bredte seg videre innenfor samfunnsvitenskap takket være arbeid av økonomer og geografer.

Utgangspunktet for Alexander (2013) var å se på forhistorien til og bruken av begrepet resiliens innenfor håndtering og risikoreduksjon av katastrofer (*Disaster Risk Reduction – DRR*), hvor det ble tatt i bruk rundt år 2000. Han anser definisjonen til United Nations International Strategy for Disaster Risk Reduction - UNISDR (2009) til å være en god definisjon innenfor DRR:

"Evnen til et system eller samfunn eksponert for farer til å motvirke, absorbere, tilpasse seg til og gjenvinne fra effektene til en fare raskt og effektivt, inkludert bevarelse og gjenopprettelse av dets sentrale strukturer og funksjoner."

Senere har begrepet blitt tatt i bruk innenfor bærekraftig utvikling og klimatilpasning (Alexander, 2013).

En oppsummering av utviklingen er illustrert i figur A.1.



Figur A.1 Forhistorien til begrepet resiliens (basert på Alexander, 2013)

Alexander viser til at mengden litteratur om resiliens er så stor at han ikke har gjort noe forsøk på å gjennomføre en fullstendig kartlegging. Allikevel er det interessant å merke seg at han ikke nevner hverken resiliens av kritisk infrastruktur (CIR) eller Resilience Engineering (RE), som i 2013 hadde pågått i noen år. Ingen av de sentrale forskerne innen CIR eller RE inngår i noen av de 70 referansene til Alexander (2013). Dette viser at CIR og RE bare er to av svært mange fagområder/retninger hvor resiliens anvendes.

Alexander kommer også med noen "stikk" til utbredelsen og mangfoldet i bruken av begrepet resiliens. Han finner det påfallende hvordan begrepet er benyttet i ulike disipliner uten å referere til hvordan det benyttes i andre fagområder, som om det ikke var noe å lære eller overføre fra en gren av vitenskapen til en annen. Videre føler han at dersom man hadde benyttet et enklere språk i vitenskapelig arbeid om resiliens, så ville mye av debatten omkring hva begreper betyr og hvordan de skal forstås vært unødvendig.

Han er heller ikke imponert over forsøkene på å skape et resiliens-paradigme³² innenfor ulike fagdisipliner eller å bruke konseptet til å skaffe seg et hegemoni. Dessuten er det fare for "overforbruk" av konseptet og å forvente at det kan gi større innsikt og bedre modelleringskapasitet enn det er i stand til å levere.

Resilience Engineering (RE)

RE er første gang nevnt i 2003, i artikkelen "*Managing Risk Proactively: The Emergence of Resilience Engineering*" (Woods & Wreathall, 2003). RE oppsto som en naturlig utvikling fra prinsippene om organisatorisk pålitelighet (Reason, 1997; Weick et al., 1999; Westrum, 1999) og ny forståelse av faktorene bak menneskelig feil og ytelse (Rasmussen, 1990; Woods et al., 1994; Cook et al., 1998). Woods & Wreathall (2003) viser til at forskning har vist at organisasjoner med høy pålitelighet (HRO – High Reliability Organizations) skaper sikkerhet ved å forutse og planlegge for uventede hendelser og fremtidige overraskelser (Rochlin, 1999; Weick et al., 1999; Westrum & Adamski, 1999).

Resilience Engineering er noe misvisende, fordi det ikke hovedsakelig er en teknologisk forståelse som ligger i RE. Engineering ("engineering resilience") ble innført for å tydeliggjøre et skille i forhold til økologisk resiliens. RE dreier seg om karakteristikker ved resilient utførelse, hvordan vi kan gjenkjenne det, vurdere eller måle det, og forbedre det (Hollnagel, 2019).

I motsetning til kritisk infrastrukturesiliens (CIR), som var en naturlig og ukontroversiell utvikling fra kritisk infrastrukturbeskyttelse (CIP), har RE ofte fremhevet seg selv som en motsats til konvensjonell sikkerhetstenkning, herunder tradisjonell risikoanalytisk tenkning, gjennom å beskrive tidligere sikkerhetstenkning som såkalt "Safety-I" og sikkerhetstenkning i tråd med RE som såkalt "Safety-II". Dette har ført til et noe anstrengt forhold til disse tilgrensende fagdisiplinene.³³

RE ønsker nå i større grad å stå på egne ben og frigjøre seg fra tidligere referanserammer, herunder adskillelse av resiliens fra sikkerhet. Et resilient system bør også tilpasse seg muligheter, ikke bare tilpasse seg forstyrrelser (Hollnagel, 2019).

Et eksempel på definisjon av resiliens fra RE er: *Et system er resilient hvis det kan justere dets funksjoner før, under eller etter hendelser (endringer, forstyrrelser og muligheter), og derved opprettholde nødvendige operasjoner under både forventede og uventede forhold* (Hollnagel, 2019).³⁴

En definisjon av resiliens hentet fra risikostyring er: *Tilpasningskapasitet til en organisasjon i et komplekst og skiftende miljø* (ISO Guide 73, 2009).

³² Paradigme brukes om en fremherskende tenkemåte i vitenskapen. (Med henvisning til Thomas Kuhn i Erlend Hem's, "Inflasjon i paradigmer"; <https://tidsskriftet.no/2018/12/sprakspalten/inflasjon-i-paradigmer>).

³³ Et eksempel på dette er Prof. Nancy Leveson's "Safety III: A Systems Approach to Safety and Resilience", 7/1/2020, <http://sunnyday.mit.edu/safety-3.pdf>, hvor hun tar kraftig avstand fra Hollnagel's beskrivelse av konvensjonell sikkerhetstenkning (det såkalte "Safety I"). Hun mener Hollnagel bruker stråmannargumentasjon hvor han overdriver, fremstiller feil eller rett og slett fabrikerer det som tilsynelatende er andres oppfatninger, dvs. sikkerhetsingeniører de siste 70 årene, og deretter latterliggjør det sikkerhetsarbeidet som har vært utført i 70 år. I tillegg til å slakte Hollnagel's beskrivelse av "Safety I" som fullstendig feil, så anser hun "Safety II" til å være et gigantisk tilbakesteg, som mest sannsynlig vil gi dårligere sikkerhet. Til slutt foreslår hun en systemsikkerhetstilnærming, litt ironisk kalt "Safety III".

³⁴ <https://www.resilience-engineering-association.org/blog/2019/11/09/what-is-resilience-engineering/>

Vedlegg B: Resiliens og risiko

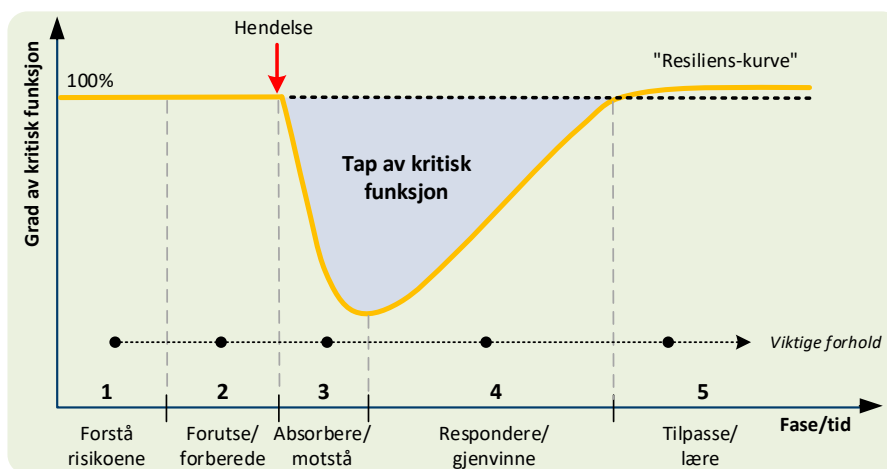
Her skal vi se litt på forholdet mellom resiliens og risiko, både hvordan metoden (CIRAM) relaterer seg til risiko og ulike betraktninger av dette forholdet, bl.a. fordi dette har betydning ved vurdering av nytteverdi.

Vår beskrivelse av resiliens og risiko er ingen fasit. Det finnes mange svar på hva resiliens og risiko er, og hvordan disse kan forstås. De tilpasses både ulike fagområder og ulike anvendelser innenfor fagområdene. Videre kan det være stor avstand mellom presise vitenskapelige definisjoner av begrepene og hvordan de forstås i dagligtale. Resiliens benyttes i dagligtale i engelsk-språklige land, mens risiko benyttes i dagligtale også i Norge.

Det skilles også mellom hva resiliens og risiko er, og hvordan disse kan beregnes eller måles (SRA, 2018). Selv om dette skillet er viktig, i hvert fall fra et akademisk perspektiv, så kompliserer det forståelsen for ikke-eksperter. Eksempelvis at *"risiko er virkningen av usikkerhet på mål"* (ISO 31000:2018) er ikke noe folk flest ville brukt som forklaring på hva risiko er. Det er en pedagogisk utfordring å forklare hva risiko er, og utfordringen er ikke noe mindre for resiliens.

Resiliens – resilienskurven

Dersom vi avgrenser oss til resiliens av kritisk infrastruktur³⁵, så er resilienskurven et bilde på resiliens, som vist i figur B.1. Dette er forklart i hoveddelen av veilederen.



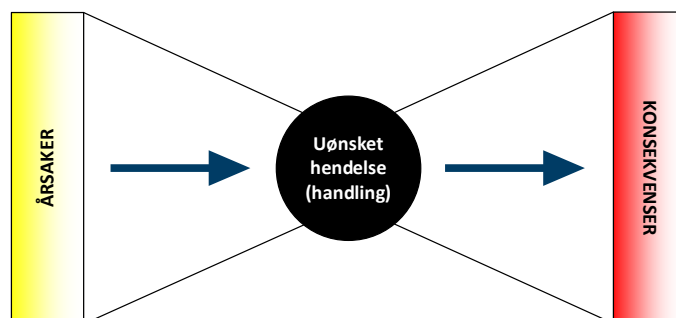
Figur B.1 Resilienskurven – bilde på "resiliens"

Som ethvert bilde eller modell er dette selvsagt en sterk forenkling og får ikke frem alle sider ved resiliens.

Risiko – sløyfediagram

Tilsvarende benyttes ofte sløyfediagram (bow-tie) som et bilde på risiko. Heller ikke her får man frem alle sider ved begrepet (risiko), men sløyfediagram har vist seg å kommunisere godt for ikke-eksperter. En enkel illustrasjon er vist i figur B.2.

³⁵ Andre retninger innenfor resiliens, slik som Resilience Engineering, forholder seg ikke til resilienskurven. De dekker ikke fasene kronologisk. Eksempelvis Resilience Analysis Grid (RAG) hvor Hollnagel (2015) viser til fire nødvendige evner for resiliens: Respond, Monitor, Learn og Anticipate (RMLA). Disse er ikke kronologiske, og de dekker kun fasene 2 og 5, samt responsdelen av fase 4. Valget av disse fire evnene er pragmatisk, og ikke teoretisk fundert.



Figur B.2 Sløyfediagram – bilde på "risiko" (uten inntegnede barrierer)

Sløyfediagram har vært brukt på mange måter. Generelt viser det årsak – virkning (mange – én – mange), hvor det for risiko kan være mange ulike årsaker til samme uønskede hendelse (eller handling), som igjen kan føre til mange ulike konsekvenser. Det har også blitt brukt til å vise hvor ulike risikoanalysemetoder kan benyttes, eksempelvis at det for venstre del kan benyttes feiltreanalyse, mens det for høyre del kan benyttes hendelsestreanalyse.

I tillegg er sløyfediagram-analyse en egen risikoanalysemetode, én av de rundt 40 metodene som beskrives i NS-IEC 31010 (2019). Her angis også fordeler og ulemper med metoden, som også er relevant selv når diagrammet bare brukes som et bilde på risiko.

Sløyfediagram-analyse benyttes for å vise en risiko³⁶ med en rekke mulige årsaker og konsekvenser. Den benyttes når situasjonen ikke krever kompleksiteten til en full feiltreanalyse eller når fokuset er mer på å sikre at det er en barriere eller et kontrolltiltak for hver feilsti (hendelseskjede). Den er nyttig når det er klare uavhengige stier som leder til feil.

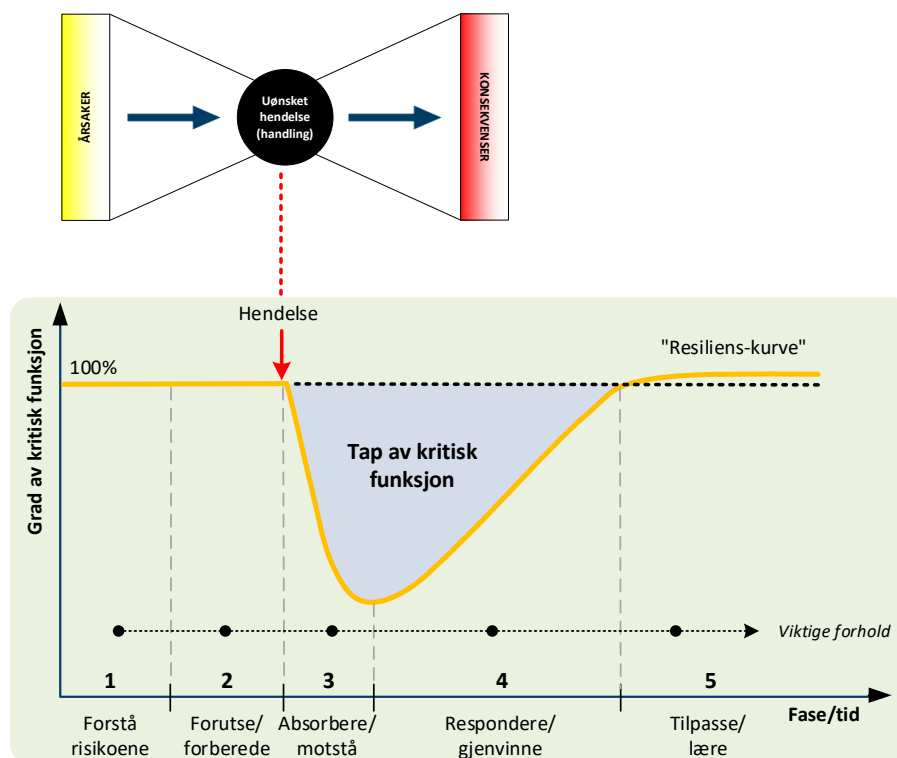
Av fordeler fremheves det at metoden er enkel å forstå, og at den gir et klart bilde av problemet. Videre retter den oppmerksomheten mot barrierer og kontroller som forventes å være på plass for forhindring og begrensning, samt deres effektivitet. Begrensningene inkluderer at den ikke kan fremstille flere samtidige årsaker (dvs. en OG-port i et feiltre). Videre kan den overforenkle komplekse situasjoner, spesielt når det forsøkes med kvantifisering.

Sløyfediagram benyttes eksempelvis i NS 5814:2021, DSBs "Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen" (2014), DSBs "Analyser av krisescenarioer" (2019) og NVEs "Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen" (2010).

Risiko versus resiliens – sløyfediagram versus resilienskurven

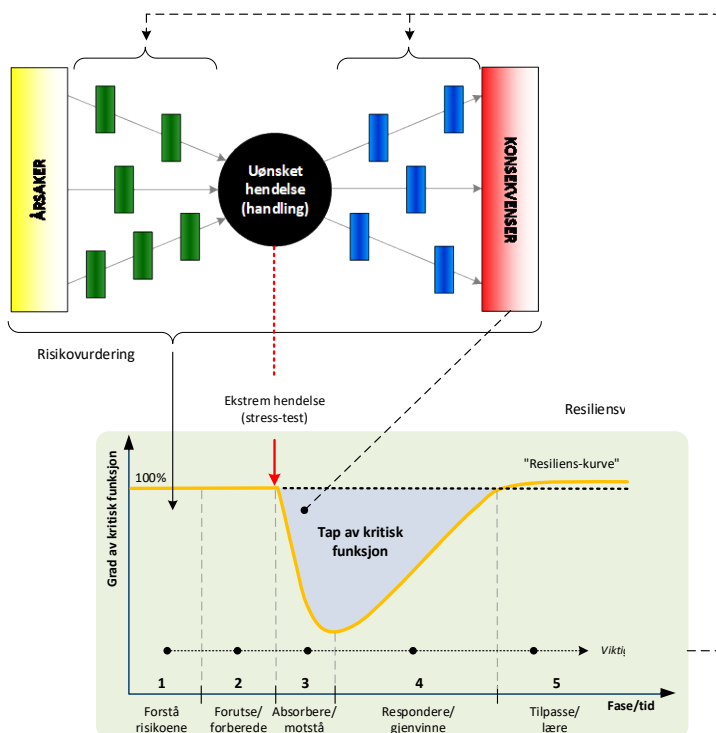
Det er ingen enkel eller direkte kopling mellom et sløyfediagram og resilienskurven, bl.a. på grunn av ulike tidsdimensjoner. Felles er en uønsket hendelse som inntreffer, som illustrert i figur B.3, men også her kan det være forskjeller – forskjeller i hva vi inkluderer som en uønsket hendelse i en risikovurdering versus en resiliensvurdering (noe vi kommer tilbake til).

³⁶ I NS-IEC 31010 (og også NS-ISO 31000) benyttes risiko ("risk") også om hendelsen (dvs. knuten i sløyfa), og man bruker derfor betegnelsen "risk identification" og ikke "hazard identification". Dette er grunnen til at man i NS 5814:2021 har gjort en tilpasning i forhold til NS-ISO 31000 ved at "risikoidentifisering" er presisert til å "identifisere uønskede hendelser".



Figur B.3 Sløyfediagram versus resilienskurven

Risikovurderinger og resiliensvurderinger er komplementære vurderinger, som illustrert i figur B.4. De gir kunnskap ut fra ulike perspektiv og kan utfylle hverandre.



- Risikovurdering gir input til risiko-forståelse (og systemforståelse)
- Herunder input om farer/trusler, sårbarheter og barrierer/tiltak
- Risikovurdering kan gi input om tap av kritisk funksjon som konsekvens

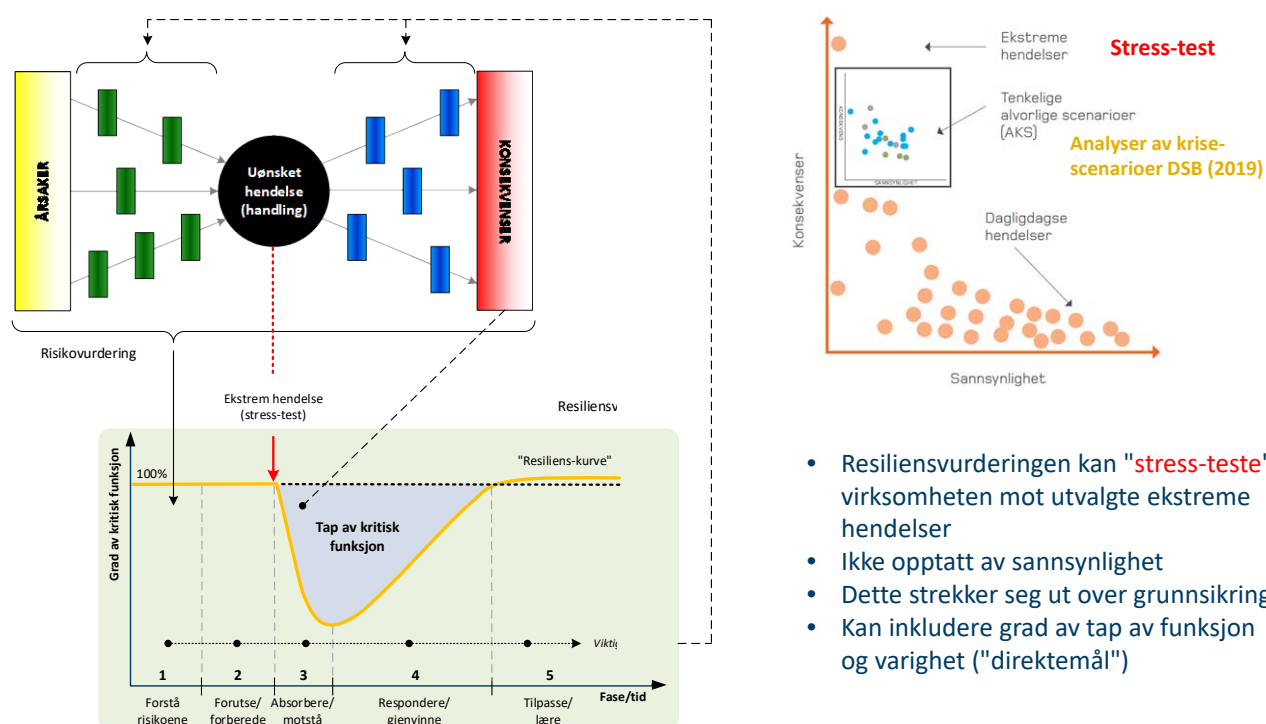


- Resiliensvurdering gir utfyllende informasjon om viktige forhold for å opprettholde kritisk funksjon
- Dette kan avlede ytterligere barrierer og tiltak
- Resiliensvurderingen kan "stress-teste" virksomheten mot utvalgte ekstreme hendelser

Figur B.4 Risikovurdering versus resiliensvurdering

Vi ser altså ikke på en resiliensvurdering som en erstatning for risikovurderinger, men som en komplementær tilleggsvurdering. Informasjon om risiko, herunder fra risikovurderinger, inngår i den første av de fem fasene CIRAM dekker. Risikoanalyser er påkrevd av myndighetene, mens resiliensvurderinger ikke er det. Risikoanalyser gir informasjon om risiko, herunder farer/trusler, sårbarheter og barrierer/tiltak, men også informasjon om systemene (systemkunnskap) som kan være nyttig informasjon for resiliensvurderinger. Risikovurderinger kan også gi informasjon om tap av kritisk funksjon som konsekvens.

Motsatt så kan resiliensvurderinger gi utfyllende informasjon om viktige forhold for å opprettholde kritisk funksjon, som igjen kan avlede ytterligere barrierer og tiltak. En resiliensvurdering kan også benyttes for å "stress-teste" virksomheten mot utvalgte ekstreme hendelser. Fokus på ekstreme hendelser utgjør en forskjell fra risikovurderinger. Dette er illustrert i figur B.5.



Figur B.5 Resiliensvurdering som "stress-test" (bl.a. basert på DSB, 2019)

Øvre høyre del av figuren viser at DSB i sine "Analyser av krisescenarier" (2019) har valgt ut "tenkelige alvorlige scenarier", dvs. ikke dagligdagse hendelser med høy sannsynlighet, men heller ikke ekstreme hendelser med svært lav sannsynlighet.

Resiliensvurderinger vil kunne utfylle risikovurderinger nettopp ved at man velger ekstreme hendelser, hendelser som ikke fanges opp av risikovurderinger. Risikovurderinger benytter generelt avskjæringskriterier ("cut-off"), dvs. de kutter ut hendelser som vurderes å være svært usannsynlig (eller ha liten konsekvens), mens en resiliensvurdering benyttet til stress-testing ikke er opptatt av sannsynlighet. Håndteringen av denne type ekstreme hendelser, innenfor de krav samfunnet stiller til maksimalt akseptabelt tap av kritisk funksjon, vil normalt kreve beskyttelse/resiliens som strekker seg ut over det som på noen områder omtales som grunnsikring. Samfunnets krav kan uttrykkes som direktemål på resilienskurven, eksempelvis maksimal grad av tap av kritisk funksjon og maksimal varighet av tapt eller redusert funksjon.

Risikoanalyser dekker kun det som er kjent og har en viss sannsynlighet, dvs. forventede hendelser, mens man i et resiliensperspektiv ønsker å kunne håndtere enhver hendelse, både kjente og ukjente, og forventede

og uventede. "Forvent det uventede" er brukt som slagord. Det betyr ikke at en resiliensvurdering dekker ukjente hendelser. Det som er ukjent kan man heller ikke resiliensvurdere, men man kan utvikle resiliente egenskaper som er nyttig for håndtering av hendelser etter at de har inntruffet, inkludert frem til da ukjente hendelser. Dette inkluderer egenskaper som tilpasning, fleksibilitet, improvisasjon, osv. Mange egenskaper vil være felles for ulike typer hendelser, og det er en underliggende antakelse at dersom man håndterer noen (kjente) ekstreme hendelser godt (har et høyt resiliensnivå), så vil man også være godt forberedt for andre både kjente og ukjente ekstreme hendelser. Øving på spesifikke resilienssegenskaper vil også bidra til å heve resiliensnivået. Et eksempel på metodikk og verktøy for dette er TORC (Training for Operational Resilience Capabilities) (Grøtan, 2020), et table-top øvingsspill som nå også finnes i digital utgave.

Risiko versus resiliens – generelt

Forholdet mellom risiko og resiliens er diskutert i litteraturen, og det er mange meninger om dette (Hollnagel, 2008, 2020; Haimes, 2009; IRGC 2016a, b; Aven, 2017, Lange m.fl., 2017, FFI, 2019).

FFI (2019) viser til at Aven (2017) mener at resiliensvurderinger kan gjennomføres uten at risiko inkluderes i vurderingene fordi resiliens i utgangspunktet ikke krever en spesifisering av hvilke hendelser som kan ramme systemet. Allikevel mener Aven at risiko bør integreres i resiliensvurderinger og at resiliens ikke bør vurderes uavhengig av spesifikke hendelser. Det samme mener Haimes (2009). Videre bør sannsynligheten for at en hendelse vil inntreffe også trekkes inn i vurderingene (Aven, 2017).³⁷ FFI (2019) viser til Aven (2017) når de argumenterer for at sannsynligheten for hendelser bør inngå, fordi det ikke vil være kostnads-effektivt, eller fornuftig, å investere i tiltak for å styrke resiliens overfor hendelser som med svært lav sannsynlighet vil inntreffe.

FFI (2019) viser også til IRGC (2016a, b) som betrakter risiko som en informasjonskilde for prosesser som skal styrke resiliens, noe tilsvarende som vi gjør i CIRAM. IRGC (International Risk Governance Council) understreker imidlertid at det er sprikende oppfatninger om forholdet mellom risiko og resiliens i forsknings-miljøet.

RE bygger på kritikk av risikoanalyser, bl.a. at metodene for å analysere risiko bærer preg av etterpåklokskap (Hollnagel, 2008), og ser ikke behov for å kople resiliens til risiko. Resiliens bør stå på egne ben, som allerede nevnt (Hollnagel, 2019), jf. vedlegg A.

Det andre ytterpunktet er en fullstendig integrering av resiliens som del av risikostyringen. FFI (2019) viser til EU-prosjektet IMPROVER (Lange m.fl., 2017) som inkluderer resiliensstyring som separate trinn i risikostyringsprosessen i ISO 31000, litt tilsvarende som Ptil gjør med integrering av barrierestyring i risikostyring, hvor også ISO 31000 legges til grunn (Ptil, 2017). FFI (2019) anbefaler at en slik tilnærming utforskes videre, men det bør i denne sammenheng bemerkes at deres mandat er å svare på hvordan resiliens kan integreres i – og eventuelt styrke – helhetlig risikostyring, dvs. det er et premiss at resiliens skal forsøkes integrert i risikostyring. I tilnærmingen til IMPROVER (Lange m.fl., 2017) mener de at risikoidentifisering er en forutsetning for resiliensvurderingsprosessen og at resiliensanalysen vil bygge på risikoidentifiseringen. Det er derfor ikke behov for en tilsvarende identifiseringsprosess for resiliens (FFI, 2019).³⁸

³⁷ Utfordringen med dette er at man da ikke dekker uspesifiserte (ukjente/uventede) og veldig usannsynlige hendelser (ekstreme hendelser). Valg av hendelser er på "risikoanalysens premisser". Dessuten er det delte meninger om hensiktsmessigheten av å sette en sannsynlighet på tilsiktede hendelser.

³⁸ Da er vi igjen tilbake til at det er risikoanalysen som legger premissene for hvilke hendelser som inkluderes, dvs. uspesifiserte dekkes ikke, og heller ikke de "litt for usannsynlige" som er bevisst kuttet ut fordi de ikke har et tilstrekkelig risikobidrag.

DSB (2019a) inkluderer også resiliens (via sårbarhet) i sine risikoanalyser (analyser av krisescenarioer – AKS). Her analyserer de 25 utvalgte scenarioer som dekker et bredt spekter av hendelser (naturhendelser, store ulykker, forsyningssvikt og tilsiktede hendelser) som det norske samfunnet kan utsettes for, både nasjonalt og lokalt. Hendelsene skal ifølge DSB *"ha potensielt svært alvorlige konsekvenser for befolkningen (definert som samfunnsverdier) og utfordre eksisterende beredskap, og ikke være helt utenkelig"*. Dvs. det er svært alvorlige hendelser, men ikke de mest ekstreme hendelsene man kan forestille seg, jf. figur B.5.

Tidligere analyserte DSB risikoen til de enkelte hendelsene gjennom *sannsynlighet* og *konsekvenser*, men har nå lagt til *sårbarhet* og *usikkerhet* som nye risikoelementer. Usikkerhet vurderes ut fra kunnskapsgrunnlaget og hvor sensitive resultatene er for endringer i forutsetningene. Sannsynlighet, konsekvenser og usikkerhet angis på en skala fra 1-5, med unntak av tilsiktede hendelser hvor sannsynlighet ikke vurderes!

Sårbarhet definerer DSB (2019a) i henhold til NOU 2000:24: *"Sårbarhet er et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt problemer det får med å gjenoppta sin funksjon"*. Videre hevder de at *"det motsatte av sårbarhet kalles ofte robusthet eller resiliens"*, men skiller mellom robusthet og resiliens ved å vise til at resiliens *"forbindes med en mer generell og dynamisk evne til å tåle stress, for eksempel gjennom en fleksibel og tilpassningsdyktig organisering"*.³⁹

Gjennom å forstå resiliens som det motsatte av sårbarhet får man en snever fortolkning av resiliens, slik det ble brukt tidligere (jf. vedlegg A), og ikke slik det nå brukes innenfor resiliens av kritisk infrastruktur hvor man dekker et bredere tidsperspektiv. Slik DSB bruker resiliens favner det hovedsakelig fase 3 og 4 i de fem fasene i CIRAM. Dette fremgår også av hovedspørsmålet de stiller: *"I hvilken grad evner systemet å motstå (hindre?) at hendelsen inntreffer eller får alvorlige konsekvenser?"*, som ikke reflekterer forståelse av risikoene (fase 1), være forutseende og forberedt (fase 2), eller lære av hendelsen og tilpasse seg (fase 5). Spørsmålet retter seg mot risikoelementene sannsynlighet og konsekvenser, og vurderingen av sårbarhet/resiliens benyttes da også som innvirkning på sannsynlighet og konsekvenser, og ikke som en separat vurdering slik DSB gjør for usikkerhet.

En annen viktig forskjell mellom tilnærmingen i CIRAM og tilnærmingen til DSB er at CIRAM gjør en indirekte vurdering av de forholdene som skal bidra til resiliens (i de ulike fasene), mens DSB ser på de direkte effektene (eksempelvis reduserte konsekvenser uttrykt som antall døde). Dette kan sammenliknes med bruken av ledende (*"leading"*)/proaktive indikatorer (CIRAM) versus *"lagging"*/reaktive indikatorer (DSB).⁴⁰

Dessuten ser ikke CIRAM på direkte effekter av hendelser, men utelukkende på indirekte effekter via tap av kritiske funksjoner i kritiske infrastrukturer. Noen infrastrukturer er definert som kritiske nettopp fordi de utfører kritiske funksjoner *for samfunnet*. I tillegg kan de rammes direkte av en hendelse, eksempelvis et terrorangrep på en flyplass som tar livet av et antall reisende. Et tilsvarende terrorangrep i et konsertlokale vil kunne få langt større direkte konsekvenser (antall døde), men et konsertlokale er ikke en kritisk infrastruktur. Samfunnet klarer seg uten funksjonen til et konsertlokale, mens en flyplass per definisjon er en kritisk infrastruktur hvor tap av funksjon – transport av passasjerer og gods – er vurdert som kritisk for samfunnet.

³⁹ I årsrapportene fram til og med 2020 (DSB 2018, 2019b, 2020) bruker ikke DSB ordet/begrepet resiliens, men de skriver bl.a. "Bestemmelsene om kommunal beredskapsplikt skal bidra til at kommunen – som er Norges aller viktigste aktør for å skape trygge, utholdende og motstandsdyktige lokalsamfunn – står bedre rustet til å forebygge og håndtere uønskede hendelser" (DSB, 2018). Her kunne det stått " ... trygge og resiliente lokalsamfunn ...".

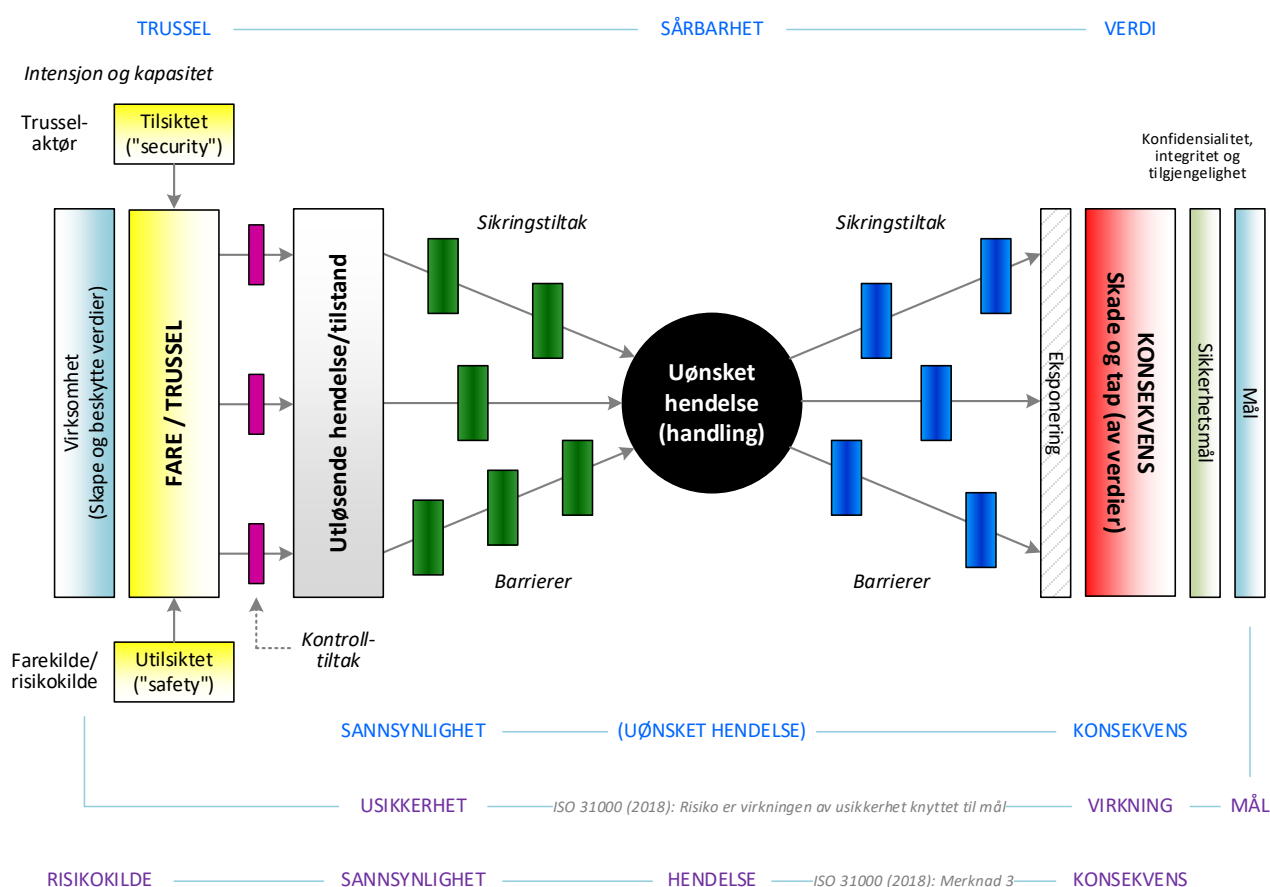
⁴⁰ I tillegg kan vi som tidligere nevnt ved "stress-testing" inkludere direkte mål på grad av tap av kritisk funksjon og varighet av tapt eller redusert funksjon.

Mens DSB gjennom AKS ser på risikoen for utvalgte hendelser med potensielt svært alvorlige konsekvenser og peker på noen mulige tiltak, så kartlegger og vurderer CIRAM status (og utvikling) på de forhold som skal bidra til å verne mot og håndtere ekstreme hendelser, herunder tiltak i form av planverk (slik som tiltaksplanen i nasjonal beredskapsplan mot pandemisk influensa). CIRAM vurderer hvor resilient kritiske infrastrukturer er i forhold til ekstreme hendelser, uavhengig av sannsynlighet og konsekvenser (risiko). CIRAM kan også benyttes i ettertid til å vurdere hvordan en hendelse ble håndtert, eksempelvis i hvilken grad planverk ble fulgt, og tilpasningsevnen i forhold til det spesifikke scenariet som inntraff.

Det kan også nevnes at en ny ISO-standard som ser på forholdet mellom risiko og resiliens (ISO 31050 "Guidance for Managing Emerging Risks to Enhance Resilience") er under etablering og er planlagt ferdig i 2021. Her vektlegger man ny/fremvoksende risiko (*emerging risks*) og ikke velkjent risiko.

Risiko – noen definisjoner og betraktninger

Figur B.6 viser et mer detaljert sløyfediagram og eksempler på elementer som inngår i risikodefinitjoner, samt deres plassering i forhold til sløyfediagrammet. Her er det to viktige skiller vi ønsker å få frem. Det første er forskjellen i risikodefinitjoner avhengig av om man ser på tilsiktede hendelser (øvre del av sløyfediagrammet) eller utilsiktede hendelser (nedre del av sløyfediagrammet). Disse risikoelementene er vist med blå tekst. Den andre forskjellen er teoretiske definisjoner av hva risiko er som fenomen kontra definisjoner for å uttrykke risiko. Disse risikoelementene er vist med lilla tekst, og vi benytter ISO 31000 som eksempel.



Figur B.6 Sløyfediagram med risikoelementer som inngår i risikodefinitjoner

For tilsiktede hendelser benyttes tradisjonelt risikoelementene trussel, sårbarhet og verdi. Et eksempel på definisjon av risiko innenfor denne "tre-faktor-modellen" er: *Risiko er et uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor denne spesifiserte trusselen* (NS 5830:2012). Denne definisjonen benyttes av Nasjonal sikkerhetsmyndighet (NSM), Politidirektoratet (POD) og Politiets sikkerhetstjeneste (PST) (NSM, 2016; NSM/POD/PST, 2015).

Trusselvurderingen baserer seg på en vurdering av trusselaktører og deres intensjon og kapasitet. Sårbarhetsvurderingen retter seg mot (manglende) sikringstiltak⁴¹, både sannsynlighetsreducerende og konsekvensreducerende. Verdivurderingen innbefatter kartlegging av virksomhetens verdier og en vurdering av hvilke konsekvenser det kan få dersom verdiene rammes. Konsekvensene kategoriseres i henhold til de overordnede sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet.

Det er en nær kopling mellom risikodefinisjon og risikovurdering. Risikovurderingen inneholder imidlertid noen flere elementer/trinn, f.eks.: *Verdi – sikringsmål – trussel – scenario – sårbarhet – risiko* (NSM, 2016).

For utilsiktede hendelser benyttes tradisjonelt risikoelementene sannsynlighet og konsekvens. Et eksempel på definisjon av risiko innenfor denne "to-faktor-modellen"⁴² er: *Risiko er et uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse* (NS 5814:2008). Også denne risikodefinisjonen ligger nær opp til hvordan risiko skal uttrykkes (måles/beregnes).

Nyere definisjoner av risiko har tendert mot å beskrive risiko som fenomen, dvs. teoretiske definisjoner hvor forklaringer til mulige måter å uttrykke risiko på er angitt eksempelvis som merknader til definisjonen⁴³. Et eksempel på en slik teoretisk definisjon er: *Risiko er virkningen av usikkerhet knyttet til mål* (ISO 31000, 2018). Et eksempel på en praktisk fortolkning er: *Risiko uttrykkes ofte i form av risikokilder, potensielle hendelser, deres konsekvenser og sannsynligheten for at de skal forekomme* (ISO 31000:2018, Merknad 3).

ISO 31000 har et vidt utgangspunkt hvor man også dekker det å skape verdier, i tillegg til å beskytte verdier. Målene kan derfor være både positive og negative. Merknad 3 dekker negative konsekvenser ved uønskede hendelser.

De fleste nyere definisjoner av risiko, etter 2009 når ISO 31000 ble utgitt første gang, argumenterer med at de er i tråd med ISO 31000, og de har **usikkerhet** med som et element i definisjonen. Eksempler er:

- *Risiko er en vurdering av om en hendelse kan skje, hva konsekvensene vil bli og usikkerhet knyttet til dette* (DSB, 2014)
- *Risiko er konsekvensene av virksomheten, med tilhørende usikkerhet* (Ptil, 2015)
- *Risiko knyttet til informasjonssikkerhet gjelder virkningen av usikkerhet på konfidensialitet, integritet og tilgjengelighet* (NVE, 2018)
- *Risiko er usikkerhet knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den kan få* (NS 5814, 2021)

Samtidig er det få standarder eller veiledninger som definerer begrepet *usikkerhet*. Dette gjelder eksempelvis for ISO 31000:2018 og NS 5814:2021. I et informativt vedlegg til NS 5814:2021 diskuteres usikkerhet, og

⁴¹ Innenfor sikring (security) benyttes begreper som sikringstiltak, mottiltak, o.l., og sjelden begrepet "barriere".

⁴² Denne har blitt betegnet som "to-faktor-modell" (f.eks. Sletten, 2018), men elementet *uønsket hendelse* inngår også i definisjonen, og også i Kaplan & Garrick's klassiske "triplet" (1981), slik at man like gjerne kunne omtalt den som en "tre-faktor-modell".

⁴³ SRA (2018) omtaler dette som henholdsvis overordnede kvalitative definisjoner og deres tilhørende målinger.

det vises til en definisjon av Lindley (2006): *Usikkerhet er en tilstand der det er mangel på informasjon, manglende forståelse av eller kunnskap om en hendelse, dens konsekvenser eller muligheten for at den skal forekomme.*

At fremtiden er usikker er ikke noe nytt, ei heller er inkludering av usikkerhet i risikovurderingene (Øien, 2016b). Debatten dreier seg nå om hvordan man best kan synliggjøre usikkerhet eller grad av usikkerhet i risikovurderingene, hvor et begrep som *kunnskapsstyrke* har blitt benyttet. Basert på definisjonen til Lindley (2006), så handler usikkerhet også om mangel på informasjon (herunder data). Det kan derfor virke fremmedgjørende snarere enn klargjørende å bruke "kunnskapsstyrke" som det eneste målet på usikkerhet. I tillegg kan teoretiske definisjoner av risiko hvor begrepet usikkerhet inngår (uten å bli definert) også virke fremmedgjørende snarere enn klargjørende for de som utfører og bruker risikovurderinger.

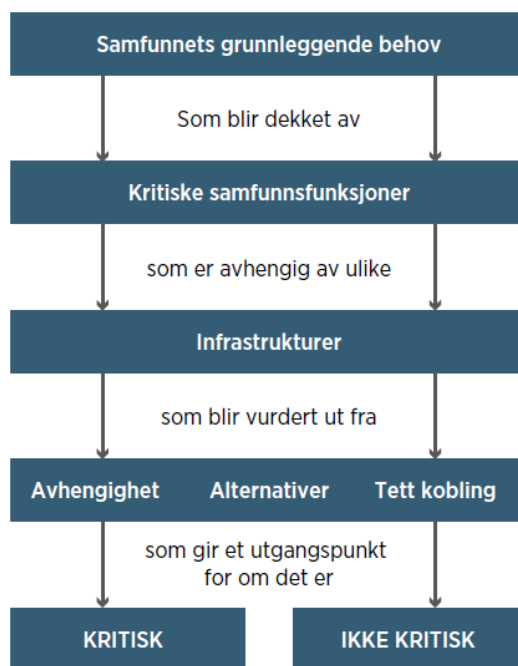
Oppsummering

Avslutningsvis oppsummeres hva vi legger til grunn i denne veilederen vedrørende resiliens og risiko.

1. Resiliens av kritisk infrastruktur er definert ut ifra de fem fasene og er dermed *evnen til å forstå risikoene som kan true den kritiske funksjonen til infrastrukturen, forberede for forutsette og uforutsette hendelser, absorbere eller motstå effektene, respondere og gjenvinne fra dem, og tilpasse infrastrukturen basert på læring etter hendelser.*
2. En resiliensvurdering er ikke en erstatning for risikovurderinger, men en komplementær tilleggs-vurdering – innhenting av kunnskap ut fra et annet perspektiv.
3. Risiko er et utgangspunkt for resiliensvurdering, ved at god forståelse av risikoene inngår i fase 1. Denne forståelsen fås gjennom risikoanalyser uavhengig av hvilken definisjon av risiko som er lagt til grunn.

Vedlegg C: Kritiske infrastrukturer i Norge

Hva som er kritiske infrastrukturer i Norge er definert av DSB (2016), og er nært knyttet til kritiske samfunnsfunksjoner, som illustrert i figur C.1.



Figur C.1 Vurdering av hva som er kritiske infrastrukturer (DSB, 2016)

Definisjonene av kritiske samfunnsfunksjoner, kritisk infrastruktur og grunnleggende behov er (DSB, 2016):

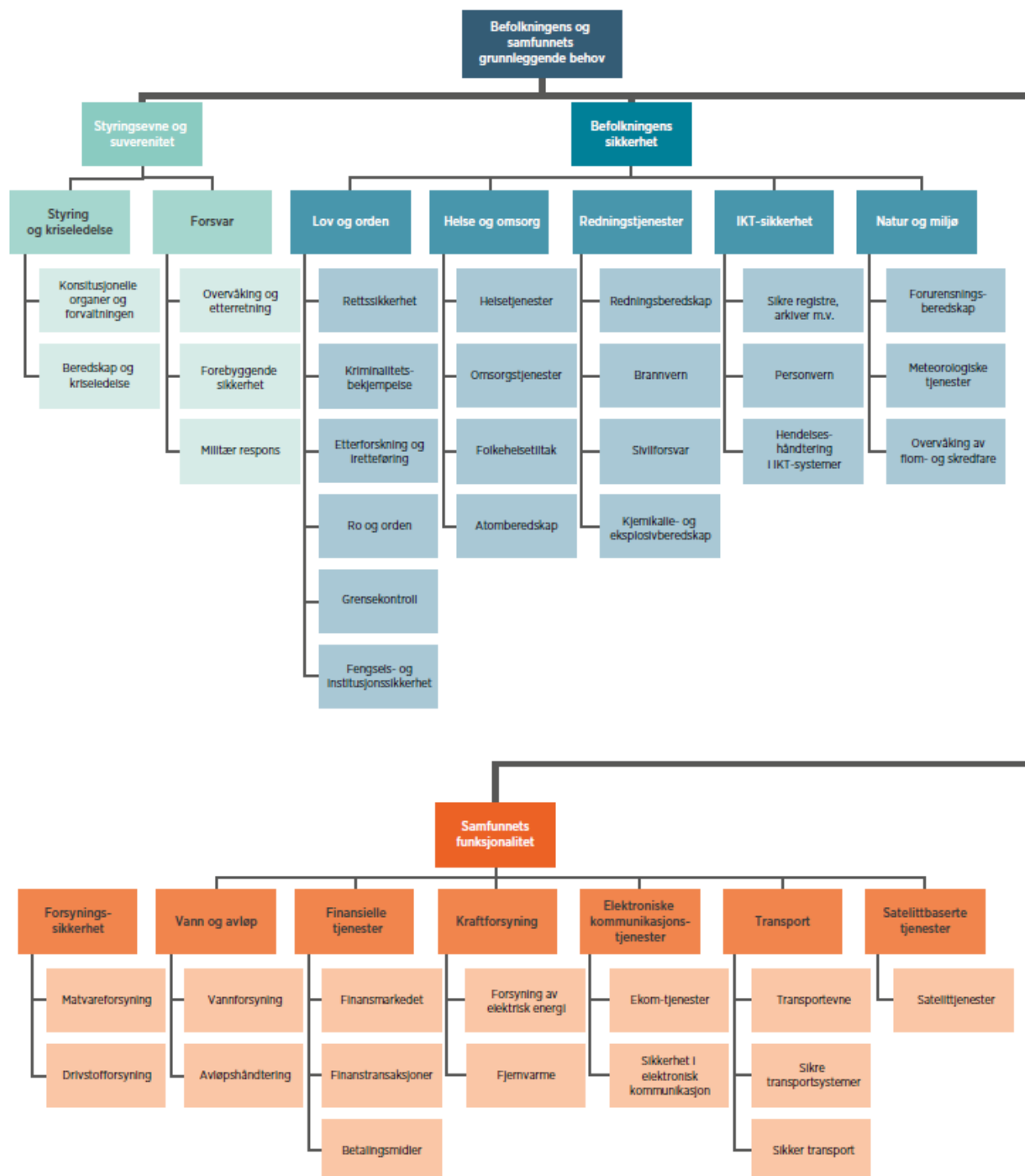
- *Kritiske samfunnsfunksjoner er de funksjoner som er nødvendige for å dekke samfunnets grunnleggende behov og befolkningens trygghetsfølelse.*
- *Kritisk infrastruktur er de anlegg og systemer som er nødvendige for å opprettholde eller gjenopprette samfunnets kritiske funksjoner.*
- *Grunnleggende behov er definert som mat, vann, varme, trygghet og lignende.*

Premisser som er lagt til grunn for valg av kritiske samfunnsfunksjoner er:

- Avgrensning i tid: Begrepet kritisk samfunnsfunksjon forbeholdes funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at dette truer befolkningens sikkerhet og/eller trygghet.
- Det forutsettes at det inntreffer hendelser som medfører at det oppstår behov for beredskapsressurser i løpet av syvdøgnperioden.

Figur C.2 viser de 14 kritiske samfunnsfunksjonene som DSB har identifisert/definert (DSB, 2016)⁴⁴.

⁴⁴ En slik definering er ikke helt enkel. Under Korona-pandemien la man til tre nye kritiske samfunnsfunksjoner og seks nye *viktige* samfunnsfunksjoner (altså en ny kategori samfunnsfunksjoner) (Regjeringen, 2020).



Figur C.2 Oversikt over kritiske samfunnsfunksjoner (DSB, 2016)

Det laveste nivået i figur C.2, delfunksjonene, betegnes for kapabiliteter (yteevner).⁴⁵

⁴⁵ Strengt tatt er det funksjonsevnen til delfunksjonen som er selve kapabiliteten.

Kritiske infrastrukturessystemer på nasjonalt nivå er vist i tabell C.1 (DSB, 2016). Disse inngår i 8 av de 14 kritiske samfunnsfunksjonene. Listen over funksjoner er en blanding av overordnede samfunnsfunksjoner og delfunksjoner (sistnevnte merket med *), i henhold til DSB's kategorisering.

Tabell C.1 Oversikt over kritiske infrastrukturessystemer på nasjonalt nivå

Samfunnsfunksjoner/ delfunksjoner *	Infrastruktur (anlegg og systemer)
IKT-sikkerhet	Systemer og registre, spesielt de som er klassifisert som «nasjonale felleskomponenter»
Matforsyning *	Produksjonsanlegg, distribusjoner, logistikk-systemer, butikker
Drivstofforsyning *	Raffinerier, havneanlegg, tankanlegg, bensinstasjoner
Vann og avløp	Vannverk, renseanlegg, pumper, høydebasseng, ledninger og rør
Finansielle tjenester	Finansiell infrastruktur
Elektrisk energi *	Kraftverk, transformatorer, kraftnett osv.
Fjernvarme *	Fjernvarmeanlegg, pumpestasjoner, ledningsnett
Ekom ¹	Kjernenett, regionalnett, aksessnett, svitsjer
Transport	Veinett, jernbanelinjer, havner, terminaler, trafikkstyringssystemer
Satellitt-tjenester	Satellitter, bakkestasjoner

¹ Ekom – elektronisk kommunikasjon

Denne oversikten over kritiske infrastrukturer (anlegg og systemer) er ikke komplett. Eksempelvis inngår ikke sykehus, som helsetjenester er avhengig av, i oversikten.

DSB argumenterer med at mange infrastrukturer ikke er så kritiske på samfunnsnivå at de bør inngå i sentrale myndigheters fokusområder. *"En vurdering av hva som er kritisk infrastruktur bør derfor foretas av de myndigheter eller virksomheter som kjenner den aktuelle infrastrukturen best. En slik vurdering kan gjøres på ulike nivåer: på et makronivå for systemer som helhet (kraftsystemet, ekomsystemene osv.) eller på et mikronivå (hvilke infrastrukturer er sykehuset avhengig av?) eller på nivå som ligger mellom disse. Identifisering av kritisk infrastruktur inngår som en naturlig videreutvikling av den identifiseringen av kritiske funksjonsevner som gjøres i denne rapporten, og bør gjøres gjennom analyser av hvilke avhengigheter som knytter seg til de ulike kapabilitetene. Ansvar for dette bør ligge hos sektormyndigheter, i kommunene og i den enkelte samfunnskritiske virksomhet."* (DSB, 2016).

I tillegg skal "skjermingsverdige objekter" med betydning for kritiske funksjoner for det sivile samfunn identifiseres i henhold til sikkerhetsloven.

Vedlegg D: Definisjoner og forkortelser

Definisjoner

Innen fagområdene resiliens, risikoanalyse og samfunnssikkerhet finnes det mange ulike definisjoner av de samme begrepene. Vi vil her ta med noen begreper, men med ulike alternative definisjoner der det er relevant og kan gi en økt forståelse av begrepet.

Fare: Forhold som kan føre til en uønsket hendelse (NS 5814:2021)
MERKNAD Fare brukes i tilknytning til utilsiktede hendelser i dette dokumentet.

Trussel: Tilsiktet handling som kan føre til en uønsket hendelse (NS 5814:2021)
MERKNAD Trussel brukes i tilknytning til tilsiktede hendelser i dette dokumentet.

Uønsket hendelse:
Hendelse som kan medføre tap av verdier (NS 5814:2021)
MERKNAD En uønsket hendelse kan være tilsiktet eller utilsiktet.

Kritisk samfunnsfunksjon:
Kritiske samfunnsfunksjoner er de funksjoner som er nødvendige for å dekke samfunnets grunnleggende behov og befolkningens trygghetsfølelse (DSB, 2016)

Kritisk infrastruktur:
Kritisk infrastruktur er de anlegg og systemer som er nødvendige for å opprettholde eller gjenopprette samfunnets kritiske funksjoner (DSB, 2016)

Resiliens i kritisk infrastruktur:
Infrastrukturresiliens er evnen til å forstå risikoene som kan true den kritiske funksjonen til infrastrukturen, forberede for forutsette og uforutsette hendelser, absorbere eller motstå effektene, respondere og gjenvinne fra dem, og tilpasse infrastrukturen basert på læring etter hendelser (basert på Øien m.fl., 2018)

Risiko (1): Usikkerhet knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den kan få (NS 5814:2021)
MERKNAD Usikkerhet kan uttrykkes gjennom sannsynlighet.

Risiko (2): En vurdering av om en hendelse kan skje, hva konsekvensen vil bli og usikkerhet knyttet til dette (DSB, 2014)

Risikoanalyse: Systematisk framgangsmåte for å beskrive risiko (NS 5814:2021)

ROS-analyse: Helhetlig ROS-analyse er en vurdering av 1) hvilke uønskede hendelser som kan komme til å skje, 2) sannsynlighet for at en uønsket hendelse vil inntreffe, 3) sårbarhet ved systemer som påvirker sannsynligheten og konsekvensene, 4) hvilke konsekvenser hendelsen eventuelt vil få og 5) usikkerheten knyttet til vurderingene (DSB, 2014)

Sannsynlighet: Hvor trolig det er at en hendelse vil inntreffe (NS 5814:2021)

Konsekvens: Tap av verdier som følge av en uønsket hendelse (NS 5814:2021)

Sårbarhet: Analyseobjektets manglende evne til å motstå en uønskede hendelser eller varige påkjenninger, samt å opprettholde eller gjenoppta sin funksjon etterpå (NS 5814:2021)

MERKNAD 1 Et analyseobjekt kan være sårbart mot at en uønsket hendelse inntreffer og mot at hendelsen får negative konsekvenser.

MERKNAD 2 Robusthet er det motsatte av sårbarhet.

Sikkerhet: Reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare (NS 5830:2012)

Samfunnssikkerhet:

Ivaretagelse av sivilbefolkningens liv, helse og trygghet, og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade (FD og JD, 2015)

Sikring: Bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger (NS 5830:2012)

MERKNAD En tilsiktet uønsket handling er en type uønsket hendelse.

Beredskap: Forberedt evne til på kort varsel å kunne øke sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller evne til å gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand (NS 5830:2012)

MERKNAD 1 Beredskap kan for eksempel innebære å ha en dokumentert beredskapsplan som er innøvd.

MERKNAD 2 Tilfredsstillende tilstand er ikke nødvendigvis samme tilstand som før den uønskede hendelsen.

Beredskapstiltak:

Forberedt tiltak som på kort varsel kan iverksettes for å øke sikkerhetsnivå, håndtere en uønsket hendelse eller tilstand, eller gjenopprette tilfredsstillende tilstand etter en uønsket hendelse eller tilstand (NS 5830:2012)

Virksomhetskontinuitet:

Organisasjonens evne til å fortsette levering av produkter eller tjenester på akseptable forhåndsdefinerte nivåer etter forstyrrende hendelse (ISO 22301:2012)

Virksomhetskontinuitetsplan:

Dokumenterte prosedyrer som veileder organisasjoner til å respondere, gjenvinne, gjenoppta og gjenopprette til et forhåndsdefinert driftsnivå etter forstyrrelser (ISO 22301:2012)

MERKNAD Vanligvis dekker dette ressurser, tjenester og aktiviteter som kreves for å sikre kontinuitet i viktige forretningsfunksjoner.

Sikringstiltak: Tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger (NS 5830:2012)

MERKNAD 1 Tiltakene kan grupperes i teknologiske, organisatoriske og menneskelige tiltak.

MERKNAD 2 Risiko kan reduseres gjennom reduksjon av sårbarhet eller påvirkning av trusselaktørene.

Teknologisk sikringstiltak:

Fysisk, elektronisk eller logisk sikringstiltak (NS 5830:2012)

Fysisk sikringstiltak:

Fysisk barriere som hindrer eller forsinker uønsket adgang til verdier (NS 5830:2012)

EKSEMPEL Dører, låser, gjerder, utnyttelse av naturgitte forhold.

Elektronisk sikringstiltak:

Tiltak som bruker elektroteknisk utstyr og løsninger for å støtte, supplere eller erstatte fysiske sikringstiltak (NS 5830:2012)

EKSEMPEL Automatisk innbruddsalarmanlegg (AIA), automatisk adgangskontroll (AAK), TV overvåking (TVO).

Logisk sikringstiltak:

Tiltak for sikring av informasjon som lagres eller overføres elektronisk (NS 5830:2012)

EKSEMPEL IKT-programvare som brannmurer og antivirusprogrammer.

Organisatoriske sikringstiltak:

Tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak (NS 5830:2012)

Menneskelig sikringstiltak:

Tiltak som påvirker persepsjon, vurderingsevne, kunnskap, adferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak (NS 5830:2012)

MERKNAD 1 Eksempler på tiltak som påvirker adferd, er holdningsskapende arbeid og bevisstgjøring.

MERKNAD 2 Eksempel på tiltak som påvirker reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak, er opplæring.

Forkortelser

AAK	Automatisk adgangskontroll
AIA	Automatisk innbruddsalarmanlegg
AKS	Analyser av krisescenarioer
ANL	Argonne National Laboratory
BLEVE	Boiling Liquid Expanding Vapor Explosion (kokende væskeekspanderende dampeksplasjon)
CIP	Critical Infrastructure Protection (kritisk infrastruktur beskyttelse)
CIR	Critical Infrastructure Resilience (kritisk infrastruktur resiliens)
CIRAM	Critical Infrastructure Resilience Assessment Method
COVID-19	Corona Virus Disease 2019
CRES	Climate Resilience
D	Deliverable (leveranse)
DNV GL	Det Norske Veritas Germanischer Lloyd
DRR	Disaster Risk Reduction
DSB	Direktoratet for samfunnssikkerhet og beredskap
EC	European Commission
EEA	European Environmental Agency
Ekom	Elektronisk kommunikasjon
EPFL	École Polytechnique Fédérale de Lausanne (Swiss Federal Institute of Technology Lausanne)
E-tjenesten	Etterretningstjenesten
EU	Europeisk Union
EØS	Det Europeiske Økonomiske Samarbeidsområdet
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FHI	Folkehelseinstituttet
FN	De Forente Nasjoner

GP	Grunnprinsipp
H	Høy
HH	Høy-høy
HMS	Helse, miljø og sikkerhet
HOD	Helse- og omsorgsdepartementet
HRO	High Reliability Organization
HSAC	Homeland Security Advisory Council
HSC	Health Safety Committee
IaaS	Infrastructure as a Service (infrastruktur som en tjeneste)
ID	Identitet
IEC	International Electrotechnical Commission
IKT	Informasjons- og kommunikasjonsteknologi
IMPROVER	Improved Risk Evaluation and Implementation of Resilience Concepts to Critical Infrastructure
IPCC	Intergovernmental Panel on Climate Change
IRGC	International Risk Governance Council
ISBN	International Standard Book Number
ISO	International Organization for Standardization
JD	Justis- og beredskapsdepartementet
KIKS	Kritisk Infrastruktur og Kritiske Samfunnsfunksjoner
L	Lav
LL	Lav-lav
LPG	Liquefied Petroleum Gas (flytende petroleumsgass)
M	Middels
Meld. St.	Melding til Stortinget
MIT	Massachusetts Institute of Technology
MRE	Måle, Rapportere, Evaluere (rammeverk)
N	Nedre (grense)
NAS	National Academy of Science
NAV	Ny arbeids- og velferdsforvaltning (nå Arbeids- og velferdsforvaltningen)
NIS	Naftna Industrija Srbije (Petroleum Industry of Serbia)
NOU	Norges Offentlige Utredninger
NS	Norsk Standard
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OED	Olje- og energidepartementet
POD	Politidirektoratet
PST	Politiets sikkerhetstjeneste
Ptil	Petroleumstilsynet
RAG	Resilience Analysis Grid
RCP	Representative Concentration Pathway
RE	Resilience Engineering
ResiliN	Resiliensvurdering i Norge
REWI	Resilience Early Warning Indicators
RI	Resilience Indicators
RIL	Resilience Level (Resiliensnivå)
ROS	Risiko- og sårbarhet (analyse)
SARS	Severe Acute Respiratory Syndrome

SCI	Smart Critical Infrastructure
SEP	Strategisk egenfinansiert prosjekt
SFO	Skolefritidsordningen
SIL	Safety Integrity Level
SN	Standard Norge
SRA	Society of Risk Analysis
t	Tid (kalendertid)
T	Tid (før, under og etter en hendelse)
TORC	Training for Operational Resilience Capabilities
TVO	TV overvåking
UNISDR	United Nations International Strategy for Disaster Risk Reduction
WHO	World Health Organization
Ø	Øvre (grense)

Vedlegg E: Generelle karakteristika og bakgrunn for metoden

Rammeverk for operasjonalisering og måling av resiliens i et system kan beskrives og kategoriseres ut fra følgende fem karakteristika: (i) top-down eller bottom-up prosess, (ii) kvantitative eller kvalitative vurderinger, (iii) basert på primær- eller sekundærdata, (iv) lokalt eller nasjonalt nivå, (v) tidsperspektiv som dekker prosesser i forkant, under og/eller i etterkant av en hendelse (FFI, 2019; NAS, 2012; Parsons m.fl., 2016).⁴⁶

Tabell E.1 angir hvordan CIRAM er i forhold til disse karakteristikkene.

Tabell E.1 Generelle karakteristika for CIRAM

Karakteristikk		CIRAM karakteristikk	CIRAM utdyping
i)	Top-down eller bottom-up	Kombinasjon	Strukturen er top-down (i seks nivå), og informasjonen gis bottom-up i henhold til strukturen.
ii)	Kvantitative eller kvalitative vurderinger	Semi-kvantitativt resultat (kvantitative og kvalitative indikatorer)	Indikatorene kan være både kvantitative (antall, andel, frekvens, osv.) og kvalitative (kvalitative uttrykk, ja/nei spørsmål, osv.). Resultatet er en semi-kvantitativ vektet skår mellom 0-5, og en tilhørende karakter og farge for hvert hele trinn i skalaen.
iii)	Primær- eller sekundærdata	Begge deler (enten eller)	Normalt vil det være primærdata som brukes, men det kan også benyttes sekundærdata.
iv)	Lokalt eller nasjonalt nivå	Alle nivå fra en enkelt infrastruktur til nasjonalt	Nivåene er typisk en enkelt infrastruktur, flere infrastrukturer i et lokalt område, en by, et fylke, en region, eller hele landet.
v)	Før, under eller etter en hendelse	Alle faser	To faser før hendelsen, én under hendelsen, og to etter hendelsen. (Kan også være to faser under hendelsen og én etter, avhengig av varighet – akutt eller vedvarende).

Metoden er svært fleksibel. Det er kun strukturen (de seks nivåene) og de fem fasene (på nivå 4) som er forhåndsdefinert. Dette innebærer imidlertid at behovet for medvirkning er stort, spesielt når det gjelder nivå 5 og 6, jf. figur 2.1: relevante og dekkende forhold, representative indikatorer, og pålitelige indikatorverdier. Metoden er i høyeste grad medvirkningsbasert. Kvaliteten på og nytteverdien av resiliensvurderingen påvirkes direkte av omfanget av medvirkning (herunder god lokalkunnskap og domenekunnskap).

Det er også rom for, og vil noen ganger være behov for, ("kreativ") tilpasning av metoden i bruk. F.eks. kan det være behov for mer enn ett nivå med forhold.

Metoden er basert på gjennomgang, tilpasning og videreutvikling av relevante referansemetoder som har sine røtter i teori om høypålitelige systemer⁴⁷ (Wreathall, 2006), Resilience Engineering (Woods, 2006), og resiliensvurderinger av kritiske infrastrukturer (Fisher m.fl., 2010, Petit m.fl., 2013, Linkov m.fl., 2014). Dette er beskrevet i Øien m.fl. (2018).

⁴⁶ Det kan nevnes at Rosenqvist m.fl. (2018) mener at det foreløpig ikke er utarbeidet et rammeverk som er fullstendig operasjonaliserbart.

⁴⁷ HRO – High Reliability Organizations (eksempler: hangarskip, flygeledersentraler, osv.)

Vedlegg F: Forslag til forhold som påvirker resiliensen i hver fase (trinn 5)

Tabell F.1 Beskrivelse av forhold – generelle kandidater (referanser /x/ gitt under tabellen)

ID	Navn på forhold	Beskrivelse av forhold
1	Fase 1 – Forstå risikoene	Forstå risikoene, systemene, konteksten og tidligere farer, trusler og hendelser
	Risikoforståelse /1/	Hvordan vi oppnår kunnskap og erfaring om risiko og hendelser
1.1	Systemkunnskap /1/	Kunnskap om hvordan de tekniske systemene fungerer og samspillet mellom systemer, og kunnskap om designforutsetninger og driftsforhold. Denne kunnskapen gir innsikt i hvordan systemer kan svikte, og mulige konsekvenser.
1.2	Informasjon og kunnskap om risiko /1/	Risikoforståelse forbedres av grunnleggende kunnskap om risikobegrepet, og av spesifikk kunnskap om risikoen på det aktuelle anlegget, installasjonen, etc. beskrevet i forskjellige risikoanalyser. Det kreves et visst grunnleggende kunnskapsnivå om risiko for å utnytte informasjonen om risikoanalyser og / eller for å utføre risikoanalyser.
1.3	Kriteriene for sikker drift godt definert og forstått /1/	For å forstå når det er behov for assistanse, er det nødvendig at kriteriene for sikker drift er godt definert og forstått.
1.4	Kunnskap om konteksten/omgivelsene /3/	Kunnskap om de spesifikke farene/truslene og konteksten/ omgivelsene de inntreffer i (situasjonsbetingede faktorer).
1.5	Kunnskap om avhengigheter /5/	Kunnskap om avhengigheter mellom egen kritisk infrastruktur og andre kritiske infrastrukturer, inkludert uventede og ikke-intuitive avhengigheter.
1.6	Hendelsesrapportering /1/	Informasjon om reelle hendelser og ulykker gir kunnskap om hva som har skjedd i fortiden, og som også gir innsikt i hva som kan gå galt i fremtiden.
1.7	Innsamling av feildata /3/	Feildata gir informasjon om statusen til de kritiske infrastruktur-systemene og mulige årsaker til hendelser.
1.8	Informasjon om kvaliteten til barrierene /1/	Informasjon om kvaliteten på barrierene, f.eks. basert på testresultater eller reelt behov, gir kunnskap om hvor godt disse beskytter mot farer, trusler og hendelser. Det gir innsikt i de systemene og tiltakene som forhindrer utviklingen av en hendelse.
1.9	Informasjon om kvaliteten på støttefunksjonene for barrierene /1/	Informasjon om kvaliteten på støttefunksjonene for barrierene, f.eks. forebyggende vedlikehold, utkoplinger, osv. inkludert menneskelige og organisatoriske elementer, gir kunnskap om i hvilken grad barrierene er driftsklare. Det gir innsikt i de operasjonelle støttesystemene som er nødvendige for at barrierene skal fungere.
1.10	Diskusjoner om risiko, sikkerhet, og resiliens i relevante møter og fora /1/	Utveksling og formidling av informasjon om utfordringer med risiko, sikkerhet, og resiliens i relevante møter og fora øker bevisstheten rundt risiko, sikkerhet, og resiliens i organisasjonen.
1.11	Resultater og ytelse knyttet til risiko, sikkerhet, og resiliens etterspurt av toppledelsen /1/	Når resultater og ytelse av arbeidet med risiko, sikkerhet, og resiliens etterspørres av toppledelsen, signaliserer det viktigheten av risiko, sikkerhet, og resiliens generelt og de spesifikke spørsmålene som blir adressert spesielt. Det øker bevisstheten om viktigheten av risiko, sikkerhet, og resiliens i organisasjonen.
1.12	Kommunisere risiko og resiliens på alle nivåer i organisasjonen /1/	For å oppnå bred risikobevissthet i organisasjonen er det viktig at informasjon om risiko og resiliens blir formidlet ordentlig, grundig og regelmessig på alle nivåer i organisasjonen. Dette kan oppnås gjennom forskjellige kanaler, f.eks. møter, sikkerhetsvarsler, oppslag, osv.

ID	Navn på forhold	Beskrivelse av forhold
2	Fase 2 – Forberede/forutse	Forberedelse, planlegging, proaktiv tilpasning og årvåkenhet for farer og trusler
	Forvente/forutse /1/	Hva vi kan forvente
2.1	Risiko/fare identifikasjon /1/	Systematisk risiko-/fareidentifikasjon er en forutsetning for å kunne forutse hva som kan gå galt. Det utvider repertoaret av hendelser/ulykker som har blitt erfart.
2.2	Læring fra egne hendelser og erfaringer /1/	Den mest åpenbare kilden til informasjon om hva som kan gå galt (og hvordan man håndterer slike situasjoner) er erfaringen fra hendelser og ulykker i egen organisasjon. Det er en spesiell forpliktelse for enhver organisasjon å unngå gjentakelse av hendelser. Læring av suksesshistorier, dvs. "hva som gikk bra", bør også inkluderes.
2.3	Læring fra andres hendelser og erfaringer /1/	Manifesteringen av mulige hendelser i reelle hendelser utgjør bare en liten prosentandel av de mulige hendelsene. Derfor er det viktig å lære mest mulig også av andres hendelser og ulykker. Dagens tilgjengelighet av informasjon gjør at organisasjonsgrenser ikke er noen unnskyldning for å lære utenom egen organisasjon. Læring av suksesshistorier, dvs. "hva som gikk bra", bør også inkluderes.
	Oppmerksomhet/årvåkenhet /1/	Hva vi bør være oppmerksomme på og hvordan vi kan være årvåkne
2.4	Driftsforstyrrelser /1/	Eventuelle driftsforstyrrelser, spesielt de som fører til aktivering av kontroll- og/eller sikkerhetssystemer, bør føre til økt oppmerksomhet siden de kan føre til initiering av ulykkeshendelser.
2.5	Utkopling av kontroll- og sikkerhetsfunksjoner /1/	Hvis kontroll- og sikkerhetsfunksjoner deaktiveres, gir disse barrierene falsk trygghet. Barrierene er ineffektive mot uønskede hendelser ved utkoplinger. Det er derfor viktig å ha kunnskap om og oversikt over, samt følge opp, alle utkoplinger og forbikoplinger i barrieresystemene.
2.6	Aktivitetsnivå og samtidige operasjoner /1/	Muligheten for at noe går galt øker med aktivitetsnivået generelt og med samtidig operasjoner spesielt. Uventede interaksjoner mellom aktiviteter kan øke ulykkesrisikoen. Dermed er det viktig å være spesielt årvåken i perioder med høy aktivitet eller høyt antall samtidige operasjoner.
2.7	Status på risiko, hendelser og kvalitet på barrierer, osv. /5/	Status på risiko, hendelser, kvalitet på barrierer, osv. sammenlignet med grenseverdier, gir informasjon om hvor det er behov for forbedringer.
2.8	Utvikling i risiko, hendelser og kvalitet på barrierer, osv. /1/	Økning i rapporterte hendelser eller negativ utvikling i kvaliteten på barrierer er tydelige indikasjoner på behovet for å iverksette tiltak for å avhjelpe situasjonen.
2.9	Risikohåndteringstiltak (planer/systemer) /3/	Kontinuerlig oppfølging av identifiserte risikohåndteringstiltak, f.eks. tiltak identifisert i risikoregistreringssystem (risikoregistre).
2.10	Behov for økt beredskap under visse situasjoner/forhold /5/	Øke beredskapen basert på forhåndsdefinerte signaler/advarsler/målinger av trusler, situasjonsfaktorer, osv.
2.11	Ny (framvoksende) risiko /5/	Årvåkenhet med hensyn til å identifisere nye risikoer tidlig, bruke risikoradarer, osv.
2.12	Forvente det uventede (se i horisonten) /5/	Evne til å forutse konsekvenser, spesielt å "finne opp" unike men meningsfylte utfall/alternativer før man "oppdager" dem.
2.13	Systemer for tidlig varsling /1/	Tidlige advarsler / svake signaler gir informasjon om potensielt forverret sikkerhet før dette kommer til uttrykk i trender. Det gir en mulighet til å være proaktiv og iverksette tiltak på et tidlig tidspunkt.
2.14	Informasjon om kontinuierlig oppdaterte trusselvurderinger /5/	Søke aktivt etter informasjon om trusselvurderinger ("trusselnivåer") fra f.eks. myndigheter.

ID	Navn på forhold	Beskrivelse av forhold
2.15	Varslingssystemer /5/	Bruk av faste tekniske varslingssystemer, identifisering av farer/trusler og/eller økt fare-/trusselnivå.
2.16	Overvåkning /3/	Kontinuerlig overvåking av mulige farer og trusler.
2.17	Endringer (tekniske/organisatoriske/eksterne) /1/	Enhver endring, enten den er bevisst eller ikke, kan føre til utilsiktede effekter på sikkerhet og sikring. Endringer med potensielt negative effekter bør gis nødvendig oppmerksomhet.
2.18	Tilsyn /3/	Regelmessig søken etter problemer/svakheter/feil gjennom tilsyn (interne og/eller eksterne).
2.19	Fokus og bruk av ressurser på sikkerhets-/resiliensforhold /1/	Sikkerhet hevdes ofte å være førsteprioritet. Dette bør også gjenspeiles i oppmerksomheten som blir gitt til sikkerhet og resiliens, f.eks. i beslutningsprosesser og ressursbruk.
2.20	Budsjett for beredskaps- og responsressurser (økning/reduksjon) /5/	Utvikling (økning eller reduksjon) i budsjetter/ressurser som er avsatt til beredskap og respons.
	Resilient design /3/	Hvordan forberede et resilient design
2.21	Robusthet (funksjoner/systemer) /5/	Resiliens gjennom robust design, f.eks. store sikkerhetsmarginer.
2.22	Redundans (funksjoner/systemer) /5/	Resiliens gjennom redundante funksjoner og systemer.
2.23	Diversitet (funksjoner/systemer) /5/	Resiliens gjennom diversitet i funksjoner og systemer.
2.24	Reserveløsninger (funksjoner/systemer) /5/	Interne reserveløsninger eller alternativer.
2.25	Ekstern redundans /3/	Redundans gjennom eksterne ressurser.
	Resilient drift /5/	Hvordan forberede for resilient drift
2.26	Resiliensplaner /5/	Forberede for resiliens gjennom dedikerte resiliensplaner.
2.27	Sikkerhetsplaner /5/	Forberede for resiliens gjennom dedikerte sikkerhetsplaner.
2.28	Sikringsplaner /5/	Forberede for resiliens gjennom dedikerte sikringsplaner.
2.29	Beredskapsplaner (og kriseorganisasjon) /5/	Forberede for resiliens gjennom beredskapsplaner, inkludert forhåndsplanlagt kriseorganisering.
2.30	Kontinuitetsplaner /5/	Forberede for resiliens gjennom kontinuitetsplaner.
2.31	Overholdelse av planer/prosedyrer/regler /5/	Overholdelse av, og sikring av vilkår for å følge, forhåndsdefinerte planer/prosedyrer.
2.32	Trenings- og øvelsesplaner (simulatorøvelser, skrivebordsøvelser, beredskapsøvelser, osv.) /1/	Trenings- og øvelsesplaner for hvordan man skal håndtere potensielle scenarier er avgjørende for å vite hva man skal gjøre, ikke bare med hensyn til identiske eller lignende scenarier som de man trener på, men også med hensyn til respons på andre (uventede) scenarier. Dette inkluderer bruk av simulatorer, skrivebordsøvelser, beredskapsøvelser, osv.
2.33	Felles øvelsesplaner /4/	Forberedelse til resilient beredskapsrespons gjennom planer for fellesøvelser med eksterne aktører.
2.34	Tilpasningsevne/fornyelse av trening og øvelser (regelmessige revisjoner) /1/	Repertoaret av trenings- og øvelsesscenarier bør gjennomgås og tilpasses regelmessig basert på erfaringer fra egne og andres ulykker, og treningsmateriellet oppdateres deretter. Opplæringen skal dekke et tilstrekkelig bredt spekter av scenarier.
2.35	Erfaring med håndtering av unntak/fravik /1/	Håndtering av unntak/fravik gir praktisk erfaring i håndtering av uvante situasjoner. Slike unntak kan oppleves under igangkjøring og oppstart av nye anlegg og systemer. Det er verdifullt å ha tilgang til personell med erfaring fra igangkjøring og oppstart, i tillegg til personell som har erfaring med å håndtere unntak under normal drift.

ID	Navn på forhold	Beskrivelse av forhold
2.36	Samarbeidsavtaler (eksterne ressurser) /3/	Forhåndsplanlagte avtaler om bruk av eksterne ressurser i krisesituasjoner.
2.37	Kunnskap om ekstern støtte/ressurser /5/	Kunnskap om mulige eksterne ressurser på forskjellige nivåer; lokale, regionale, nasjonale, og internasjonale.
2.38	Interoperabilitet i kommunikasjon (intern) /3/	Kompatibilitet mellom interne kommunikasjonssystemer.
2.39	Interoperabilitet i kommunikasjon (eksternt) /3/	Kompatibilitet med eksterne kommunikasjonssystemer.
2.40	Fysisk adgangskontroll /3/	Fysiske barrierer og andre systemer for å forhindre uautorisert adgang til områder, bygninger, rom, osv.
2.41	Digital tilgangskontroll /3/	Barrierer og systemer for å forhindre uautorisert tilgang til IT-systemer.
2.42	Planlagt vedlikehold /3/	Planlagt vedlikehold av kritiske systemer og utstyr for å sikre at de er funksjonsdyktige.
2.43	Økonomiske ressurser / forsikring /3/	Nødvendige økonomiske ressurser for å opprettholde resilient drift og å være økonomisk forberedt på større hendelser/avbrudd.
3	Fase 3 – Absorbere/motstå	Evne til å absorbere og motstå hendelser
	Iboende absorberende evne /5/	Hvordan den fysiske kritiske infrastrukturen er i stand til å absorbere (fange opp/dempe) hendelser
3.1	Passive sikkerhetssystemer /5/	Innebygde passive sikkerhetssystemer for å forhindre utvikling/ eskalering av en hendelse.
3.2	Absorbering/skadebegrensning /3/	Energi absorberes for å begrense skadene, som del av en resilient utforming av den kritiske infrastrukturen.
	Resilient umiddelbar reaksjon /5/	Hvordan den kritiske infrastrukturen er i stand til umiddelbart å reagere resilient for å motstå hendelser
3.3	Aktive sikkerhetssystemer /5/	Automatiske og manuelle sikkerhetssystemer for å oppdage/forhindre/ motstå en hendelse umiddelbart.
3.4	Varsling/alarm /2/	Varsel om en hendelse, f.eks. ved å utløse en alarm så snart som mulig til den ansvarlige enheten, f.eks. et kontrollsenter.
3.5	Bekreftelse av hendelse /2/	Bekrefter at hendelsen er reell, og hva slags hendelse det er.
3.6	Aksjonsplaner - reaksjon (tilgjengelighet, kjennskap, og bruk) /2/	Tilgjengelighet, kjennskap til og bruk av forhåndsplanlagte aksjonsplaner for umiddelbar reaksjon på en hendelse.
3.7	Kompetent og erfarent personell /5/	Kompetent og erfarent personell er viktig for å oppnå en resilient umiddelbar reaksjon for å motstå en (forventet eller uventet) hendelse.
3.8	Lokalkunnskap /5/	Personell med detaljert lokalkunnskap om hvor man kan finne hva (f.eks. bygninger, systemer, ressurser, osv.) er viktig for å få en rask resilient reaksjon.
3.9	Improvisasjon og tilpasning (av reaksjon) /5/	Evne til å identifisere alternative (herunder improviserte) løsninger og skille mellom deres respektive konsekvenser.
3.10	Fleksibilitet i organisasjonsstruktur (autonomi/ omgruppering) /1/	Organisasjonen som håndterer forstyrrelser, hendelser og beredskapssituasjoner skal være tydelig gjenkjennelig for alt personell. Overgangen fra normal drift til en nødsituasjon og tilbake til normal drift bør være klart definert og trent for. Organisasjonen må også være fleksibel og kunne tilpasse seg utviklingen i situasjonen, inkludert erstatte for skadet eller på annen måte utilgjengelig personell.
3.11	Evne til å ta riktige beslutninger /1/	Fullmakt til, støtte og opplæring i å ta kritiske beslutninger, inkludert beslutninger med potensielt store økonomiske konsekvenser.
3.12	Intern varsling /2/	Varsle personell som kan være i umiddelbar fare.

ID	Navn på forhold	Beskrivelse av forhold
3.13	Alternative rømningsveier og samlingsplasser /2/	Vurder om alternative - annet enn forhåndsdefinerte - rømningsveier og/eller samlingsplasser/mønstringssteder må velges.
3.14	Intern kunngjøring /2/	Intern kunngjøring over høyttalere om situasjonen, og hvordan personell skal forholde seg.
3.15	Mobilisering av beredskapsledelsen /2/	Mobilisering/utkalling av beredskapsledelsen.
3.16	Alternativt beredskapssenter /2/	Vurdere å bruke (et forhåndsetablert) alternativt beredskapssenter i tilfelle det normale beredskapssenteret er eller kan bli påvirket av hendelsen.
3.17	Varsling til beredskapsressurser /2/	Varsling til interne og eksterne beredskapsressurser i henhold til aksjonsplan.
3.18	Tidlig situasjonsforståelse /5/	Få oversikt og se hele situasjonsbildet (unngå blindsoner). Etterspørre og samle så mye relevant informasjon som mulig.
3.19	Kunngjøring av skadestedssenter (beliggenhet) /2/	Bestemme seg for samt kunngjøre plasseringen av skadestedssenteret.
3.20	Personalsporing /2/	Oversikt over personell (lokalisering og antall personer).
3.21	Ekstern varsling og kommunikasjon /2/	Varsling, informasjon og kommunikasjon med relevante eksterne aktører, f.eks. hovedkontor, myndigheter, osv. (ut over eksterne beredskapsressurser som allerede er varslet).
3.22	Tilpass (reduser/stopp) driften/produksjonen /2/	Tilpasning av driften i henhold til hendelsen, f.eks. redusere, minimere eller stoppe driften.
3.23	Sikre utrykkingspersonell /2/	Utplassering av beredskapspersonell (f.eks. brannmenn, røykdykkere, osv.) kun når det anses som trygt.
3.24	Start bekjempelse/håndtering av hendelse /2/	Bekjempelse av hendelse med nødvendige tilgjengelige ressurser.
3.25	Evakuering av ikke-essensielt personell /2/	Evakuering av ikke-essensielt personell (dvs. personell som ikke er en del av beredskapen) til sikkert sted.
3.26	Statusoppdatering i tidlig reaksjonsfase /2/	Regelmessig oppdatering av situasjonsstatus i den første reaksjonsfasen (innledende respons). Informasjon til beredskapsledelse.
3.27	Kommunikasjon om status i tidlig reaksjonsfase /2/	Kommuniser relevant situasjonsstatus under den første responsen (internt og eksternt). Informasjon fra beredskapsledelse.
3.28	Myndighetskontakt under den første responsen /2/	Etablere kontakt med myndigheter og kommunisere regelmessig under den første responsen. (Forhåndsetablert myndighetskontakt).
3.29	Mediehåndtering under den første responsen /2/	Bruk av dedikerte ressurser for mediehåndtering under den første responsen. (Forhåndsetablert medieansvarlig).
	Beslutningsstøtte /1/	Hvordan vi gir beslutningsstøtte (løser målkonflikter) for å opprettholde kritiske funksjoner
3.30	Beslutningsstøtte-bemanning (tilgjengelighet og kunnskap) /1/	Tilstrekkelig bemanning som gir beslutningsstøtte, enten lokalt eller eksternt, innebærer at bemanning er tilgjengelig når det er nødvendig og med nødvendig kunnskap, erfaring og autoritet/fullmakt til å gi eller foreslå beslutninger og handlinger. Dette kan også angå målkonflikter.
3.31	Beslutningsstøtte IKT-systemer (og IKT-personell) /1/	Beslutningsstøtte krever ofte hensiktsmessige (evt. fjerndriftede) IKT-beslutningsstøttesystemer på plass. Dette inkluderer også støtte for IKT-systemene selv, dvs. tilgjengelighet av IKT-personell. Det er avgjørende å unngå sammenbrudd eller funksjonsfeil i disse systemene i en kritisk situasjon dersom man er avhengig av slike systemer.
3.32	Ekstern beslutningsstøtte (på forskjellige nivåer) /1/	En situasjon kan kreve støtte fra utenfor egen organisasjon. I så fall må nødvendig ekstern støtte, inkludert tilhørende IKT-systemer, være tilgjengelig når det er nødvendig.

ID	Navn på forhold	Beskrivelse av forhold
3.33	Forståelse og vilje til å bruke ekstern støtte /5/	Håndtering av en kompleks situasjon kan kreve ekstern ekspertise for å forstå situasjonen tilstrekkelig til å ta passende beslutninger, og vilje til å motta slik støtte utenfra.
3.34	Koordinering mellom aktører (på forskjellige nivåer), internt /5/	Koordinering innad i hvert beredskapslag, koordinering av alle ressurser/lag på skadestedet (eller i nærheten), lokal koordinering av hele beredskapsoperasjonen fra et sentralt beredskapssenter osv. Deling av informasjon.
3.35	Koordinering mellom aktører (på forskjellige nivåer), eksternt /5/	Ekstern koordinering med områderessurser, regionale ressurser eller utenforliggende ressurser, inkludert hovedkvarter, myndigheter, osv. Deling av informasjon.
	Redundans i beslutningsstøtte /1/	Hvordan vi kompenserer for degradering gjennom redundans for å opprettholde kritiske funksjoner
3.36	Redundans av beslutningsstøttefunksjoner /1/	Kritiske støttefunksjoner, interne og eksterne, bør være redundante for å sikre tilgjengeligheten av beslutningsstøtte.
3.37	Redundans i informasjonsbehandling /1/	Kritiske informasjonssystemer bør være redundante for å sikre nødvendig informasjonsflyt for beslutningsstøtte.
4	Fase 4 – Respondere/gjenvinne	Kapasitet og evne til rask respons og gjenvinning etter hendelser
	Responskapasitet og -hurtighet /1/	Hvordan vi kan sikre tilstrekkelig respons til rett tid
4.1	Interne beredskapsressurser /5/	Interne beredskapsressurser og respons-/mobiliseringstid. Utstyr (fast/mobilt, automatisk/manuelt, osv.), personell, organisasjon, osv.
4.2	Ressursallokering og bemanning (inkludert bufferkapasitet) /1/	Tilstrekkelig antall personer som ivaretar kritiske funksjoner, inkludert reserve-/avløserpersonell i tilfelle ytterligere behov, tilgjengelighet av personell eller bytte av personell. Ordninger som muliggjør tilstrekkelig mobilisering for å gi god respons til rett tid er viktig.
4.3	Eksterne beredskapsressurser /5/	Eksterne ressursressurser og respons-/mobiliseringstid. Utstyr, personell, organisering, avtaler/kontrakter, osv.
4.4	Kommunikasjon mellom aktører under respons /1/	Respons er ofte avhengig av informasjon fra andre aktører. Det er viktig at de (lokale) informasjons- og kommunikasjonssystemene er tilgjengelige under hele situasjonens varighet til kontroll er gjenvunnet. Informasjonen må være forståelig for alle involverte aktører (inkludert bruk av felles språk).
4.5	Rettidig oppdatering av informasjon via IKT-systemer /1/	Respons til rett tid krever oppdatering av nødvendig informasjon om situasjonen til rett tid samt kommunisering av dette mellom de involverte aktørene via IKT-systemer.
	Resilient respons og gjenvinning /1/	Hvordan vi kan sikre fullføring av respons og gjenvinning (uten skader)
4.6	Utholdenhet av ansvarlig funksjon /1/	Utholdenhet til kritiske funksjoner for å fullføre responsen. Dette inkluderer personell med ansvar for kritiske oppgaver samt opprettholdelse av kritiske systemer.
4.7	Organisatorisk robusthet (stedfortredere) /1/	Selv om enkeltpersoner av en eller annen grunn ikke er tilgjengelige, bør de kritiske funksjonene sikres gjennom forhåndsplanlagte erstattere, f.eks. av stedfortredere som har fått samme opplæring som hovedansvarlige.
4.8	Utholdenhet av respons /5/	Tilstrekkelig med responsressurser, f.eks. flere skift/lag/ressurspool, osv. for å sikre fullføring av responsen.
4.9	Redundans i ferdigheter; flerferdighet /1/	Redundans i ferdigheter og flerferdighet/flerfaglighet gir organisasjonen muligheter til å erstatte kritiske funksjoner. Dette strekker seg utover det som er forhåndsplanlagt.

ID	Navn på forhold	Beskrivelse av forhold
4.10	Aksjonsplan – respons (tilgjengelighet, kjennskap, og bruk) /2/	Tilgjengelighet, kjennskap til og bruk av aksjonsplaner for respons.
4.11	Trening og øvelser (simulatortrening, skrivebordsøvelser, beredskapsøvelser, osv.) /1/	Trening og øvelse i hvordan man skal håndtere potensielle scenarier er avgjørende for å vite hva man skal gjøre, ikke bare med hensyn til identiske eller lignende scenarier som de man trener på, men også med hensyn til respons på andre (uventede) scenarier. Dette inkluderer bruk av simulatorer, skrivebordsøvelser, beredskapsøvelser, osv.
4.12	Fellesøvelser /4/	Resilient respons og gjenvinning gjennom fellesøvelser med eksterne aktører.
4.13	Improvisasjon og tilpasning (av respons og gjenvinning) /5/	Evne til å identifisere alternative (herunder nye improviserte) løsninger ved å kombinere og bruke ressurser på en annen måte enn forutsatt.
4.14	Overvåke effekter og tilpasse underveis /5/	Overvåke effekten av valgte responsstrategier eller aksjoner, og løpende tilpasning etter behov.
4.15	Bekjempe hendelsen /2/	Bekjemp hendelsen til situasjonen er fullstendig under kontroll. Dette kan kreve utskifting av utmattet responspersonell.
4.16	Søk og redning /2/	Søk etter og redning av savnet personell.
4.17	Medisinsk behandling /2/	Medisinsk behandling av skadet personell på åstedet.
4.18	Medisinsk evakuering /2/	Evakuering av skadet personell for (videre) medisinsk behandling.
4.19	Generell evakuering /2/	Generell evakuering av området, inkludert beredskapsressurser.
4.20	Statusoppdatering under respons og gjenvinning /2/	Jevnlig oppdatering av situasjonsstatus under respons og gjenvinning.
4.21	Kommunikasjon under respons og gjenvinning (statusoppdatering) /2/	Kommuniser relevant situasjonsstatus under respons og gjenvinning (internt og eksternt).
4.22	Myndighetskontakt under respons og gjenvinning /2/	Oppretthold kontakt med myndigheter og kommuniser regelmessig under respons og gjenvinning.
4.23	Mediehåndtering under respons og gjenvinning /2/	Bruk av dedikerte ressurser til mediehåndtering under respons og gjenoppretting. (Forhåndsetablert medieansvarlig).
4.24	Sikring av området /2/	Sikre området og begrense tilgangen til relevant respons- og etterforskningspersonell (inkludert sikring av bevis).
4.25	Registrer involvert personell /2/	Registrer alt involvert personell; beredskapspersonell, skadet personell og omkomne.
4.26	Reparer skadene (uplanlagt vedlikehold) /2/	Reparer eventuelle skader på den kritiske infrastrukturen.
4.27	Risikovurder og avklar omstart/videreført drift /2/	Gjennomfør risikovurdering og foreta avklaringer (inkludert godkjenninger) før omstart/fortsettelse av driften.
4.28	Forsikringskrav /5/	Fremme eventuelle forsikringskrav for å kompensere for økonomiske tap for å gjenvinne økonomisk styrke.
5	Fase 5 – Tilpasse/lære	Læring, reaktiv tilpasning og forbedringer etter farer, trusler og hendelser
	Læring/forbedring /5/	Hvordan vi lærer fra hendelsen og responsen, og forbedrer oss
5.1	Debriefing av hendelse og respons /2/	Debriefing av hendelsen og responsen/håndteringen til personell som var direkte involvert.
5.2	Oppfølging av skadet personell /2/	Oppfølging av skadet personell, inkludert langsiktig oppfølging av psykisk stress og traumer.

ID	Navn på forhold	Beskrivelse av forhold
5.3	Håndtering av pårørende /2/	Ivaretagelse av pårørende (reiser, hotell, skjerming mot media, informasjon, prester, begravelser, osv.)
5.4	Mediehåndtering etter hendelsen /2/	Gi informasjon til media om hva som skjedde, responsen/håndteringen, undersøkelser, oppfølging av involverte personer, osv.
5.5	Hendelsesgransking og rapportering inkludert anbefalinger for tilpasning/forbedring /5/	Gransking av hendelsen, inkludert underliggende årsaker, og anbefalinger for tilpasning/forbedring (fysiske, tekniske, operasjonelle, organisatoriske, osv.).
5.6	Presentasjon/formidling av hendelsesgransking /5/	Presentasjon og formidling av resultatene av granskingen internt og eksternt (sikkerhetsvarsler, rapporter, presentasjoner, pressekonferanser, osv.).
5.7	Implementering og oppfølging av anbefalinger for tilpasning/forbedring /5/	Implementere og følge opp anbefalte tilpasninger og resiliensforbedringer.
5.8	Rapportering av responsen/håndteringen inkludert erfaringer /5/	Rapportering av responsen/håndteringen og eventuelle erfaringer og lærepunkter for forbedring av fremtidig respons og resiliens.
5.9	Implementering og oppfølging av erfaringer fra håndteringen /5/	Implementering og oppfølging av erfaringene/lærepunktene fra responsen/håndteringen (ressurser, evner, osv.).
5.10	Presentasjon/formidling av håndteringen /5/	Presentasjon og formidling av erfaringene fra håndteringen internt og eksternt.
5.11	Tilbakemelding og læring fra vellykkede aspekter av håndteringen /5/	Gi tilbakemelding og læring fra vellykkede aspekter ved håndteringen av hendelsen (lære av det som gikk bra) i tillegg til hendelsesgranskingen, som vektlegger forbedring av det som gikk galt.
5.12	Kontinuerlig resiliensforbedring /5/	Kontinuerlig oppmerksomhet mot og forbedring av forholdene som vil bidra mest til økt resiliens.
5.13	Lagring av kunnskap om hendelser og håndteringen av disse /5/	System/arkiv for å lagre og hente frem kunnskap og erfaringer fra hendelser og respons/håndtering.

De to viktigste kildene til forholdene i tabellen er en retningslinje for implementering av en metode for etablering av resiliens-indikatorer kalt REWI (Resilience-based Early Warning Indicators) (Øien m.fl., 2012), og en beredskapsplan utviklet av SINTEF (2014, fortrolig). Noen forhold er hentet fra EU-prosjektet IMPROVER (2016), og noen få fra EU-prosjektet RESILIENS (2016a, b), mens resten er input fra SINTEF i EU-prosjektet SmartResilience (Øien m.fl., 2017a). Noen forhold er tatt direkte fra originalkildene, mens andre er tilpasset.

Vedlegg G: Generelle formler for beregning av skårverdier

De matematiske formlene presenteres fra laveste nivå (indikatorer – nivå 6) og til det totale resiliensnivået på øverste nivå (område – nivå 1).

Nivå 6: indikatorer

Hvert forhold måles med én eller flere indikatorer. Anta at forhold nummer k , Fk , måles med n_k indikatorer, $k=1, \dots, m$. Måleverdien for indikator nummer j for forhold k , I_{kj} , betegnes m_{kj} . Måleverdien gjøres om til en skårverdi mellom 0-5, betegnet s_{kj} .

For å definere skårverdien for indikatorene, s_{kj} , fastsettes grenseverdier til endepunktene, dvs. en nedre verdi m_{kj}^N , som tilsvarer en verste verdi (LL_N), og en øvre verdi m_{kj}^O , som tilsvarer en beste verdi (HH_O). Mellom disse grenseverdiene (forankringsverdiene), beregnes skårverdier etter en lineær skala, som vist i likning 1.

$$s_{kj} = 5 \left(\frac{m_{kj} - m_{kj}^N}{m_{kj}^O - m_{kj}^N} \right) \quad (1)$$

For indikatorverdier (måleverdier) lavere enn nedre grenseverdi er skårverdien 0, dvs. $s_{kj} = 0$, dersom $m_{kj} < m_{kj}^N$, og for indikatorverdier over høyeste verdi er skårverdien 5, dvs. $s_{kj} = 5$, dersom $m_{kj} > m_{kj}^O$.

Bruk av en lineær skala mellom yttergrensene, og fastsettelse av skårverdier gjennom interpolasjon som vist her er en forenkling. Det er også mulig å bruke en trinnvis lineær skala, dvs. at intervallene [0-1>, [1-2>, osv. ikke trenger å være like. Dette er vist i tabell 2.7 under trinn 7.

Bruk av en ikke-lineær skala er også mulig, men vil komplisere beregningene, og forfølges ikke videre her.

En ytterligere forenkling, som også er vist i tabell 2.7 i trinn 7, er at skårverdiene i hvert intervall angis som middelerdier (0,5, 1,5, 2,5, 3,5, 4,5) i stedet for en mer eksakt interpolasjon. Da slipper man å bruke likning 1, men skårverdiene blir mindre nøyaktig.

Nivå 5: Forhold

Måleverdiene til indikatorene, m_{kj} , som er omformet til en indikator skårverdi, s_{kj} , iht. likning 1, vektet for å gi et vektet gjennomsnitt av de indikatorene som benyttes for å måle et gitt forhold. Dette gir en skårverdi s_{Fk} for forholdet Fk , som vist i likning 2.

$$s_{Fk} = \sum_{j=1}^{n_k} v_{kj} \cdot s_{kj} \quad (2)$$

Summen av vektene skal, som vanlig, være lik 1, dvs. $\sum_{j=1}^{n_k} v_{kj} = 1$.

Nivå 4: Faser

Faser betegner vi med P for å skille de fra forhold. For hver fase P_j , ($j=1, \dots, 5$), beregnes faseskår s_{Pj} som vektet gjennomsnitt av skårverdiene til tilhørende forhold, s_{Fk} , som vist i likning 3. Fase nummer j består av m_j faser, $j=1, \dots, m$.

$$s_{Pj} = \sum_{k=1}^{m_j} w_{Fk} \cdot s_{Fk} \quad (3)$$

Også her vil summen av vektet være lik 1, dvs. $\sum_{k=1}^{m_j} w_{Fk} = 1$.

Nivå 3: Trussel/fare/hendelse; Nivå 2: Kritisk infrastruktur; Nivå 1: Område

Tilsvarende som for forhold og faser vil skårverdier for trusler/farer/hendelser, kritiske infrastrukturer og området beregnes som vektet gjennomsnitt av skårverdiene på nivået under, ved å bruke tilsvarende likninger som likning 2 og 3.

På alle nivå vil skårverdien (s) tilsvare et resiliensnivå (RIL) mellom E-A, som følger:

$RIL = E$ dersom $0 \leq s < 1$

$RIL = D$ dersom $1 \leq s < 2$

$RIL = C$ dersom $2 \leq s < 3$

$RIL = B$ dersom $3 \leq s < 4$

$RIL = A$ dersom $4 \leq s \leq 5$

Notasjon:

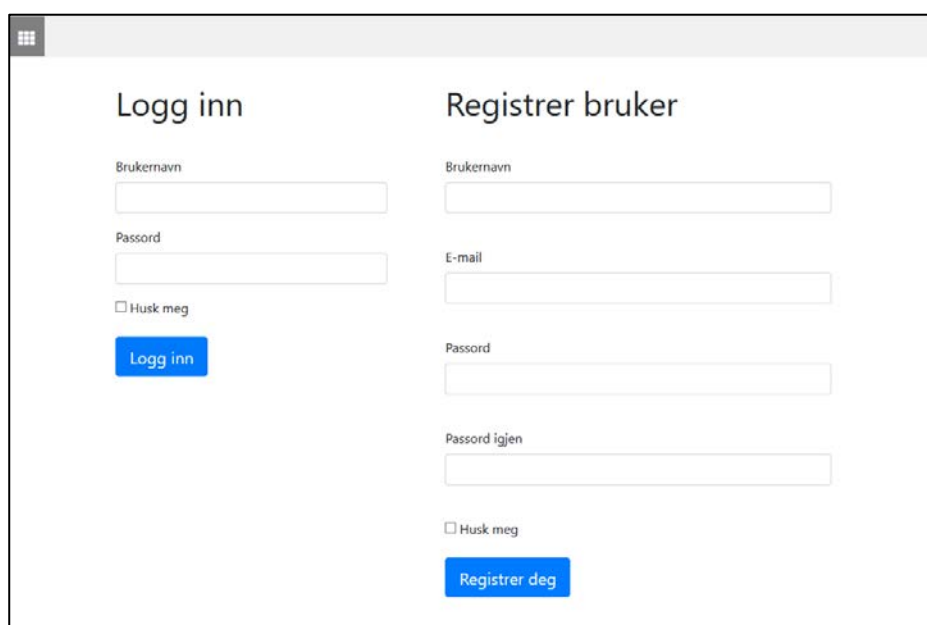
LL	-	Lav-lav
L	-	Lav
M	-	Middels
H	-	Høy
HH	-	Høy-høy
N	-	Nedre
Ø	-	Øvre
n	-	Antall indikatorer per forhold
m	-	Antall forhold per fase
m_{kj}	-	Måleverdi for indikator nummer j for forhold nummer k
$m_{kj}^{\text{Ø}}$	-	Øvre grenseverdi, dvs. beste realistiske verdi for indikator nummer j for forhold nummer k
m_{kj}^{N}	-	Nedre grenseverdi, dvs. verste realistiske verdi for indikator nummer j for forhold nummer k
s	-	Skår
s_{kj}	-	Skårverdi for indikator nummer j i forhold nummer k
s_{Fk}	-	Skårverdi for forhold nummer k
s_{pj}	-	Skårverdi for fase nummer j
RIL	-	Resiliensnivå
v_{kj}	-	Vekt av indikator nummer j i forhold nummer k
w_{Fk}	-	Vekt av forhold nummer k i fase nummer j
w_{pj}	-	Vekt av fase nummer j

Vedlegg H: Verktøy for beregninger og visualisering av resultater

Verktøyet ResiliN er laget av Torbjørn Vallestad (NTNU) og Peter Halland Haro (SINTEF), og er til intern bruk av SINTEF ved gjennomføring av resiliensvurderinger.⁴⁸

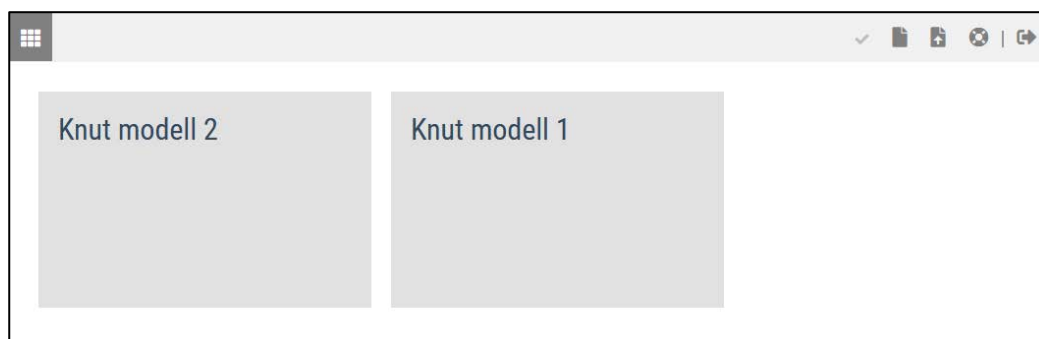
Dette er et enkelt web-basert verktøy for beregninger og visualisering av resultater. Det tar utgangspunkt i at strukturen er definert, dvs. alle nivå fra område og til indikatorer. Videre tar det utgangspunkt i at vektorer er gitt på alle nivå (hvor standard er lik vekt), inkludert alle forhold og alle indikatorer, og det tar utgangspunkt i at måleverdier for alle indikatorene foreligger.

Det må først opprettes en bruker som vist i figur H.1.



Figur H.1 Registrering av bruker og innlogging

Etter innlogging kommer man til forsiden som vist i figur H.2.



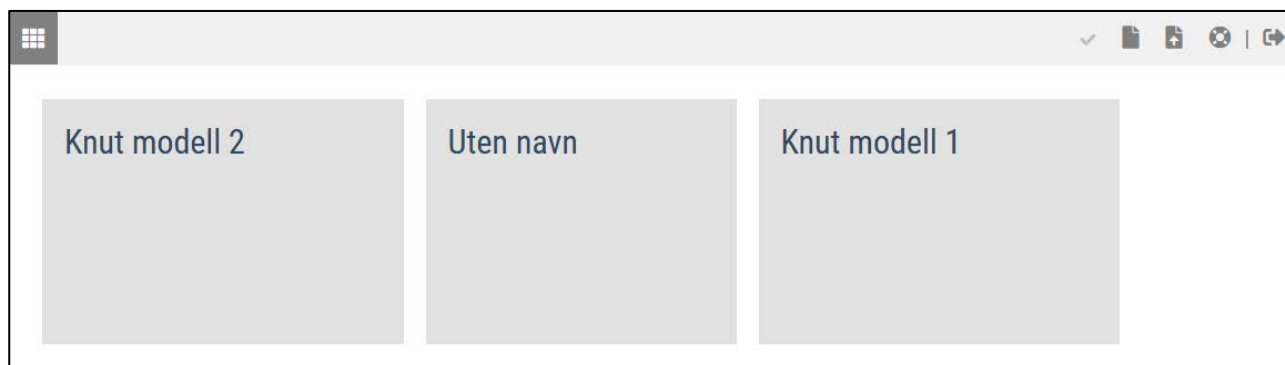
Figur H.2 Forside med eksisterende modeller

⁴⁸ Vedrørende verktøyet (applikasjonen) sikkerhet så sender det krypterte data over https og har brukerautentisering via JWT og OAuth2. Dataene lagres i databaser. Administrator har tilgang til alle data.

Ikonene opp til høyre (vist under her) angir henholdsvis "INDIKATOR FOR LAGRINGSSTATUS", "NY MODELL", "LAST OPP MODELL FRA EXCEL FIL", "BRUKERGUIDE" og "LOGG UT". Ikonet opp til venstre er (tilbake) til forsiden.



NY MODELL vil komme opp som "Uten navn", som vist i figur H.3.



Figur H.3 Ny modell (Uten navn)

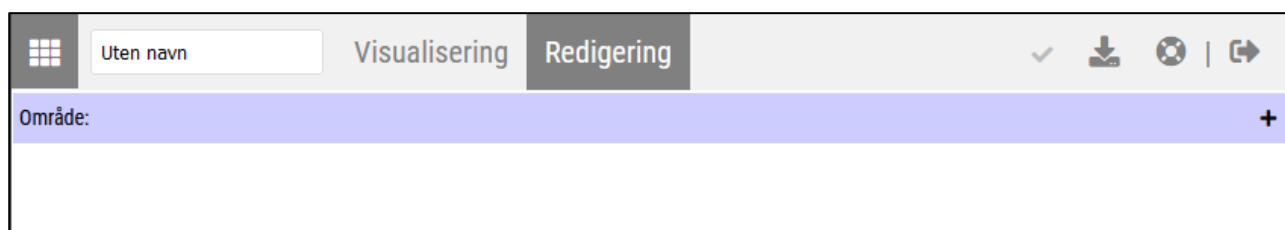
Ved å velge den nye modellen kommer man til inngangssiden for visualisering eller redigeringssiden, hvor man også kan gi den nye modellen et navn (endre "uten navn"). Inngangssiden er vist i figur H.4.



Figur H.4 Inngangssiden for visualisering eller redigering (og navngiving)

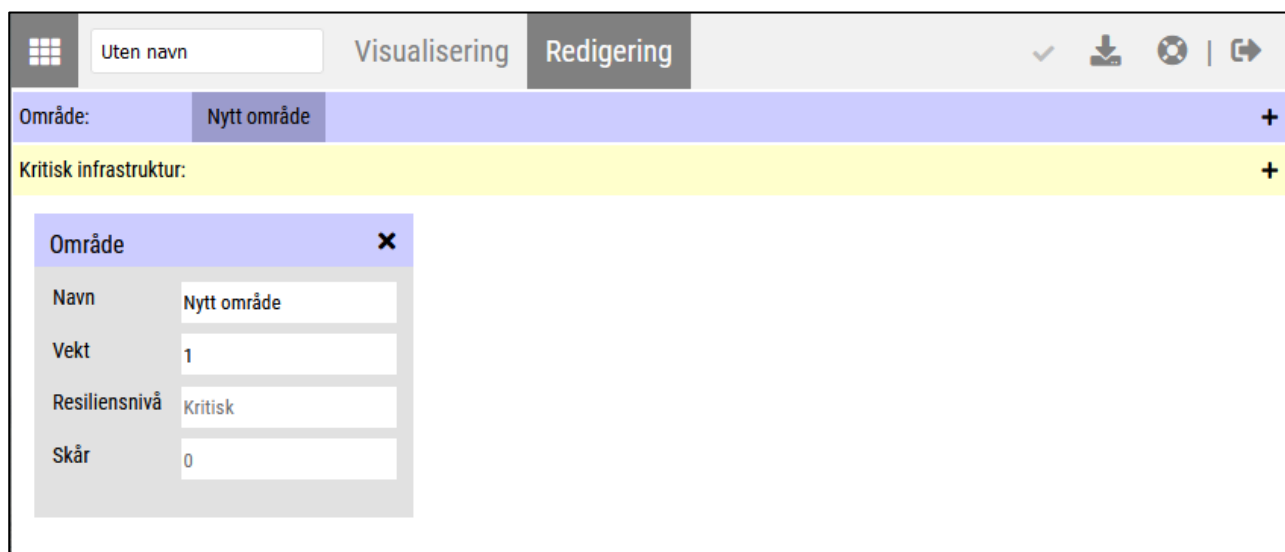
Inngangssiden for en ny modell er tom, som vist i figur H.4.

For en ny modell starter man med å legge inn strukturen ved å velge "redigere". Da får man opp øverste nivå (nivå 1 – område), som vist i figur H.5.



Figur H.5 Start redigering med øverste nivå (nivå 1 – område)

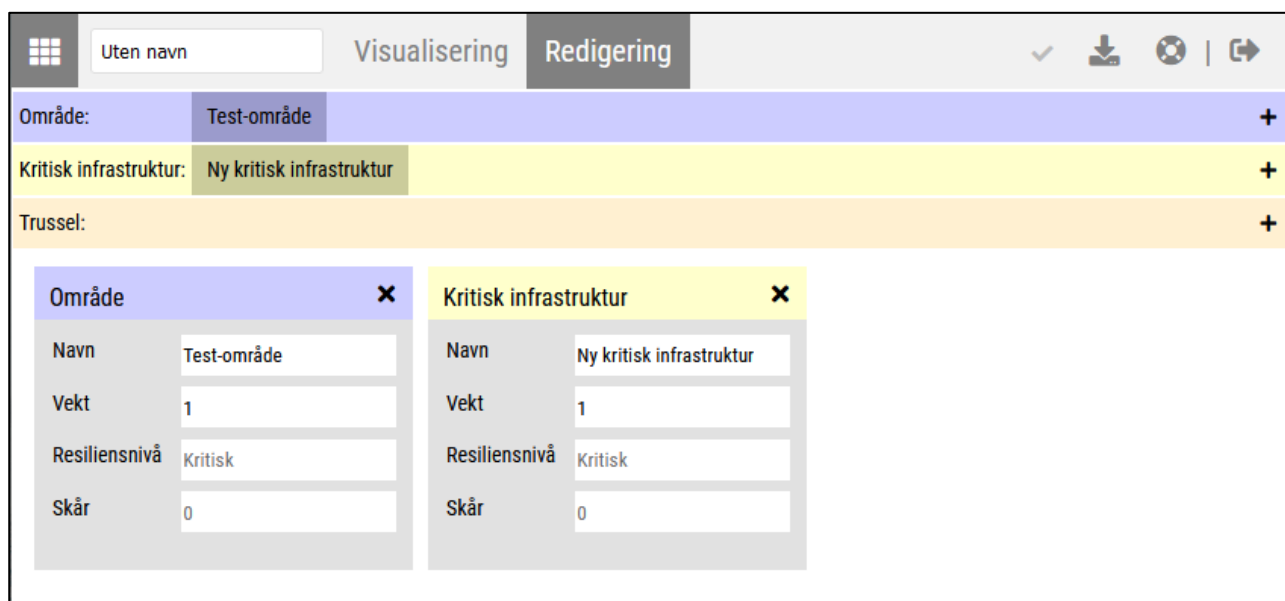
Ved å trykke på "+" til høyre i områdefeltet får man opp en boks for å fylle inn navn på område, samt at neste nivå (nivå 2 – kritisk infrastruktur) kommer opp som nytt felt under område-feltet. Dette er vist på figur H.6.



Område	
Navn	Nytt område
Vekt	1
Resiliensnivå	Kritisk
Skår	0

Figur H.6 Informasjons-boks for nivå 1 (område) og felt for nivå 2 (kritisk infrastruktur)

Her gir man navn på område, og trykker på "+" for kritisk infrastruktur, og får opp boks for å fylle inn informasjon om kritisk infrastruktur. Dette er vist på figur H.7.

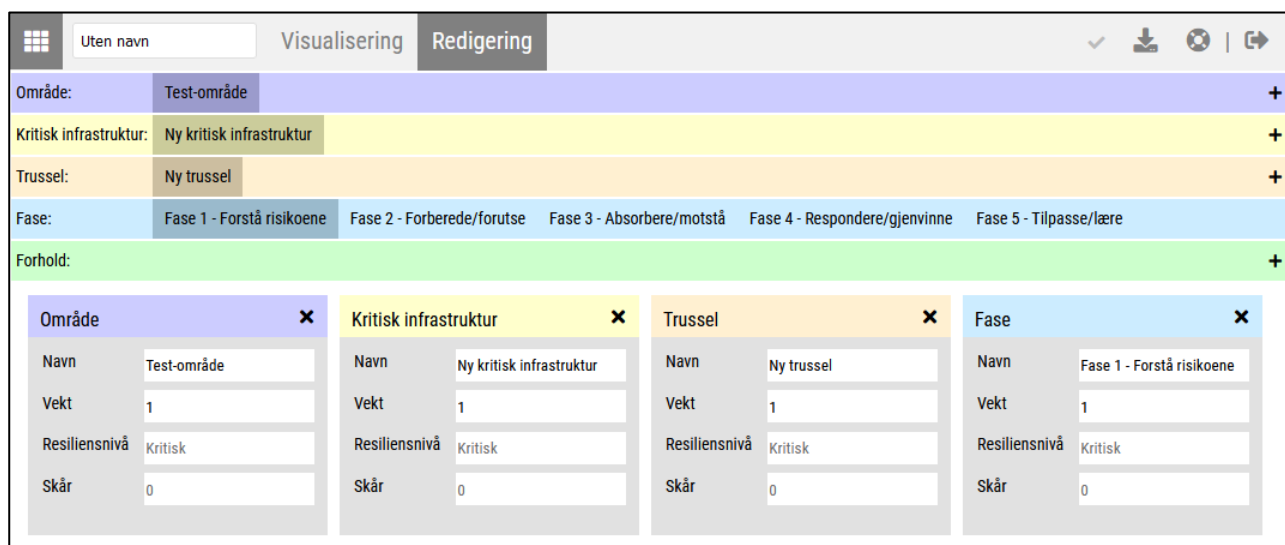


Område	
Navn	Test-område
Vekt	1
Resiliensnivå	Kritisk
Skår	0

Kritisk infrastruktur	
Navn	Ny kritisk infrastruktur
Vekt	1
Resiliensnivå	Kritisk
Skår	0

Figur H.7 Informasjons-boks for nivå 1 og 2, og felt for nivå 3 (trussel)

Her gir man navn på kritisk infrastruktur, og trykker på "+" for trussel, og får opp boks for å fylle inn informasjon om trussel. Dette er vist i figur H.8. Man kan også velge å legge inn flere kritiske infrastrukturer (ved å trykke "+"). Dette er ikke vist i figur H.8.

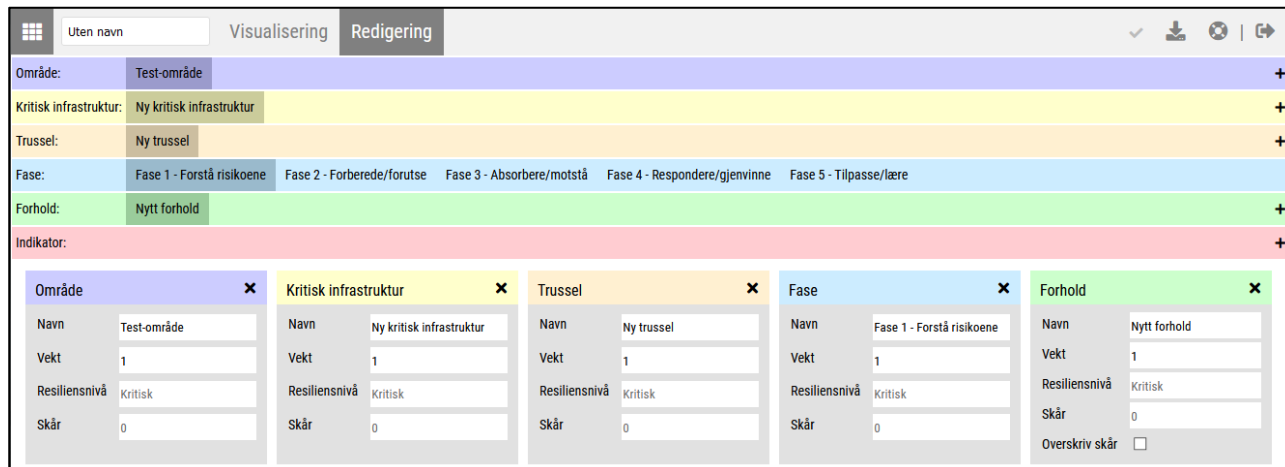


The screenshot shows the 'Informasjons-boks' for level 1, 2, 3, and 3, and level 5 (forhold). The interface includes a header with 'Uten navn', 'Visualisering', and 'Redigering' tabs. Below the header, there are five main sections: 'Område', 'Kritisk infrastruktur', 'Trussel', 'Fase', and 'Forhold'. Each section has a dropdown menu and a '+' button. The 'Forhold' section is highlighted in green. Below these sections, there are four detailed boxes for 'Område', 'Kritisk infrastruktur', 'Trussel', and 'Fase'. Each box contains fields for 'Navn', 'Vekt', 'Resiliensnivå', and 'Skår'.

Område	Kritisk infrastruktur	Trussel	Fase
Navn: Test-område	Navn: Ny kritisk infrastruktur	Navn: Ny trussel	Navn: Fase 1 - Forstå risikoene
Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1
Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk
Skår: 0	Skår: 0	Skår: 0	Skår: 0

Figur H.8 Informasjons-boks for nivå 1, 2, 3 og 3, og felt for nivå 5 (forhold)

Her gir man navn på trussel, og får automatisk opp alle fem fasene. Disse ligger fast, og skal ikke velges eller endres av bruker. Man står i utgangspunktet på fase 1 (forstå risikoene), og når man trykker på "+" for forhold (nivå 5), så gjelder disse for fase 1. Dette er vist i figur H.9. Man flytter seg mellom fasene ved å trykke på feltet for faser.



The screenshot shows the 'Informasjons-boks' for level 1, 2, 3, 4, and 5, and level 6 (indikator). The interface is similar to Figure H.8, but with an additional 'Indikator' section at the bottom. The 'Indikator' section is highlighted in pink. Below the 'Indikator' section, there are five detailed boxes for 'Område', 'Kritisk infrastruktur', 'Trussel', 'Fase', and 'Forhold'. Each box contains fields for 'Navn', 'Vekt', 'Resiliensnivå', and 'Skår'. The 'Forhold' box also includes an 'Overskriv skår' checkbox.

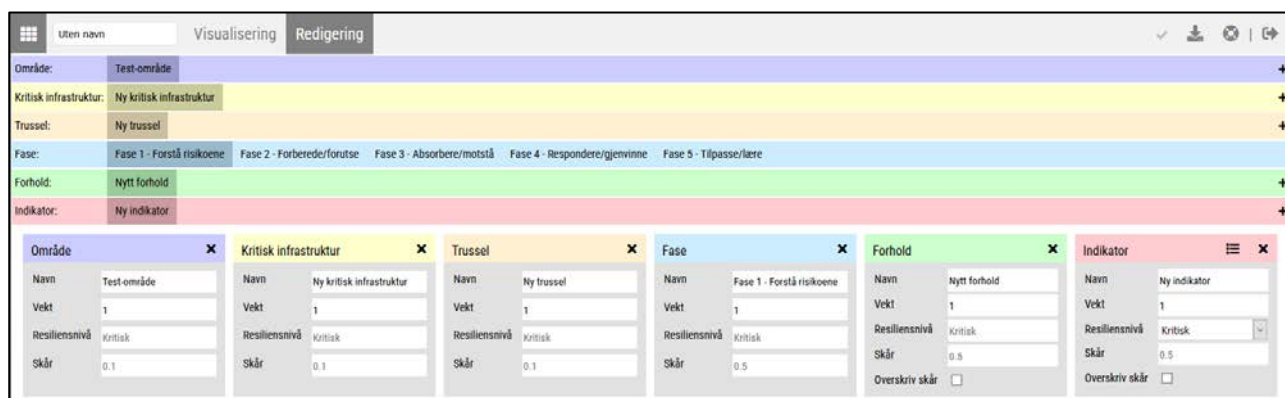
Område	Kritisk infrastruktur	Trussel	Fase	Forhold
Navn: Test-område	Navn: Ny kritisk infrastruktur	Navn: Ny trussel	Navn: Fase 1 - Forstå risikoene	Navn: Nytt forhold
Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1
Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk
Skår: 0	Skår: 0	Skår: 0	Skår: 0	Skår: 0
				Overskriv skår: ☐

Figur H.9 Informasjons-boks for nivå 1, 2, 3, 4 og 5, og felt for nivå 6 (indikator)

Fasene ligger altså fast, mens man gir navn på forhold, og trykker på "+" for indikator, og får opp boks for å fylle inn informasjon om indikator, som er laveste nivå (nivå 6). Dette er vist på figur H.10.

Man legger inn så mange indikatorer man ønsker innenfor hvert forhold, og så mange forhold man ønsker innenfor hver fase.

Når dette er gjort har man strukturen på plass og kan begynne å fylle inn skårverdier for indikatorene, samt vekter dersom man har ulik vektning. Ulik vektning kan legges inn på alle nivå.



Område	Kritisk infrastruktur	Trussel	Fase	Forhold	Indikator
Navn: Test-område	Navn: Ny kritisk infrastruktur	Navn: Ny trussel	Navn: Fase 1 - Forstå risikoene	Navn: Nytt forhold	Navn: Ny indikator
Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1
Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk	Resiliensnivå: Kritisk
Skår: 0.1	Skår: 0.1	Skår: 0.1	Skår: 0.5	Skår: 0.5	Skår: 0.5

Figur H.10 Informasjons-bokser for alle nivå

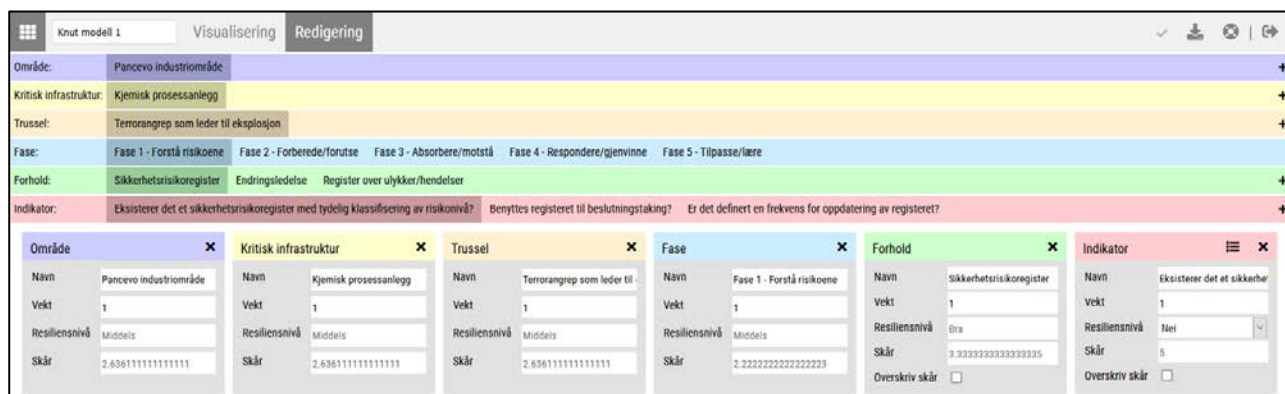
I den videre beskrivelsen av innlegging av skår og vekter benytter vi eksempelet fra kapittel 4.1.

Før vi gjør det kan vi ta med betydningen av ikonene opp til høyre i redigeringsmodus:



Fra venstre er dette "INDIKATOR FOR LAGRINGSSTATUS", "LAST NED SOM EXCEL FIL" og "LOGG UT". (NB! BRUKERGUIDE-ikonet fjernet fra redigerings- og visualiseringsmodus).

Figur H.11 viser strukturen på informasjonen i eksempelet fra kapittel 4.1 – eksplosjon i kjemisk anlegg. Her er kun den første av tre trusler tatt med.



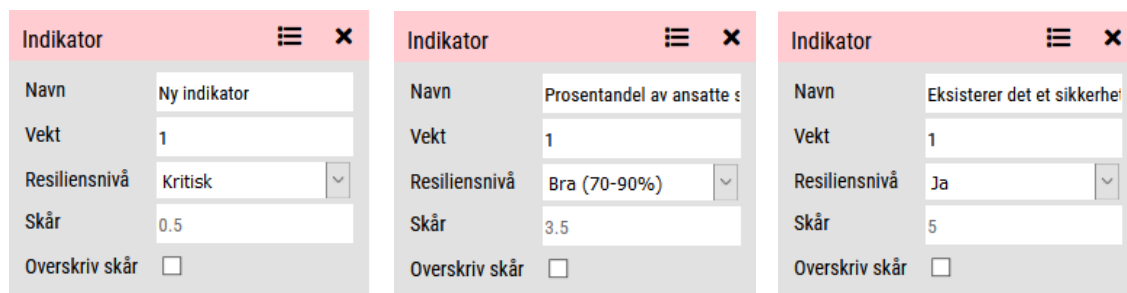
Område	Kritisk infrastruktur	Trussel	Fase	Forhold	Indikator
Navn: Pancevo industriområde	Navn: Kjemisk prosessanlegg	Navn: Terrorangrep som leder til eksplosjon	Navn: Fase 1 - Forstå risikoene	Navn: Sikkerhetsrisikoregister	Navn: eksisterer det et sikkerhetsrisikoregister
Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1	Vekt: 1
Resiliensnivå: Middels	Resiliensnivå: Middels	Resiliensnivå: Middels	Resiliensnivå: Middels	Resiliensnivå: Går	Resiliensnivå: Nei
Skår: 2.636111111111111	Skår: 2.636111111111111	Skår: 2.636111111111111	Skår: 2.222222222222222	Skår: 3.333333333333333	Skår: 5

Figur H.11 Informasjons-bokser for alle nivå i eksempelet "eksplosjon i kjemisk anlegg"

Strukturen er lagd ovenfra og ned, dvs. fra nivå 1 (område) og ned til nivå 6 (indikator). Verdier (skår og vekter) legges inn nedenfra og opp, dvs. vi starter med nivå 6 (indikatorer).

Skår legges i utgangspunktet inn kun for indikatorer, og beregnes for de øvrige nivåene. Men, det er mulig å overstyre beregnet skårverdi både for indikatorer og forhold. Vekter kan legges inn på alle nivå hvor det er mer enn én "enhet". Normalt er det kun ett område (nivå 1), som da får vekt 1.0 (100%). Lik vekt er standardverdi på alle nivå, og legges inn automatisk. Ved lik vekt trenger man ikke legge inn verdier på vekter.

Skårverdier for indikatorer fastsettes ut fra virkelig indikatorverdi og indikatorskala for den enkelte indikator. "Verdien" som legges inn (velges) i verktøyet er enten Ja/Nei (for Ja/Nei-spørsmål) eller en av de kvalitative betegnelsene på resiliensnivå (med angivelse av kvantitative representative verdier), dvs. en av verdiene kritisk – dårlig – middels – bra – svært bra (som igjen tilsvarer resiliensnivå E-A). Dette er illustrert i figur H.12.



Figur H.12 Ny indikator-boks til venstre, fem-delt resiliensnivå i midten, og Ja/Nei til høyre

En ny indikatorboks fremkommer som til venstre i figur H.12. Den har i utgangspunktet kritisk resiliensnivå, som tilsvarer en standard skårverdi 0,5. Man kan endre nivået med en nedtrekks-meny. Dette er vist i midten i figur H.12, hvor man har endret resiliensnivået fra kritisk til bra (som betyr at man ligger mellom 70-90%), som tilsvarer skårverdi 3.5. Innlegging av representative indikatorverdier for de fem resiliensnivåene gjøres ved å trykke på menyen oppe til høyre, og så skrive inn verdiene for hvert nivå, som vist i figur H.13.



Figur H.13 Innlegging av representative indikatorverdier for de fem resiliensnivåene (eksempel)

Når man har et Ja/Nei-spørsmål som indikator, som vist til høyre i figur H.12, så må man først trykke på menyen oppe til høyre, og så velge Ja eller Nei, trykke en gang til på meny-ikonet, og deretter velge Ja eller Nei fra nedtrekks-menyen. Dette er vist fra venstre mot høyre i figur H.14.

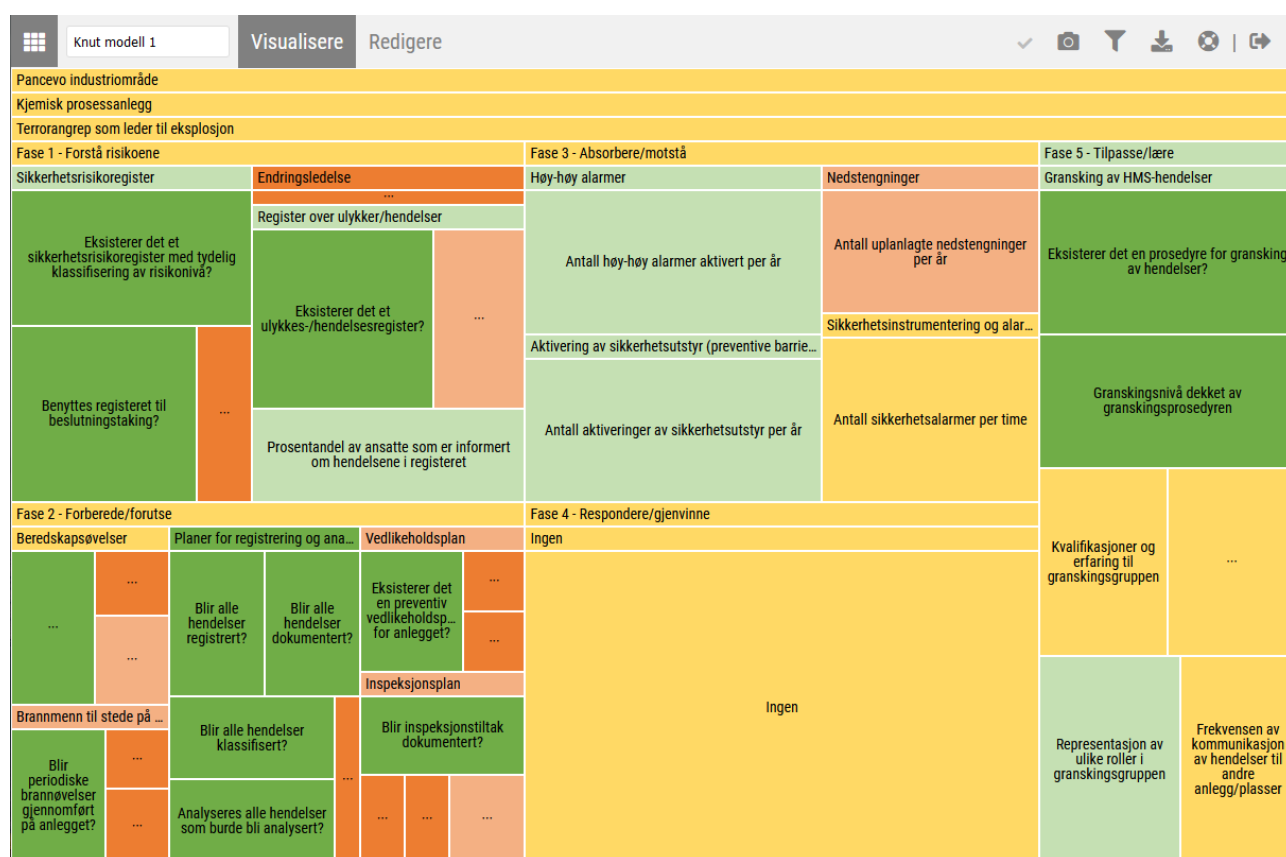


Figur H.14 Endring til, og valg av Ja eller Nei for Ja/Nei-spørsmål som indikator

Dersom man vil overstyre den beregnede skårverdien, f.eks. fra 5 (til høyre i figur H.14) til 4,8 må man først krysse av i den nederste boksen "Overskriv skår". Dette kan man også gjøre for forhold, som vist i figur H.11.

Vekt kan angis på to måter. I eksempelet (se figur H.11) har vi tre indikatorer for det første forholdet. Ved lik vekt er standard verdi på alle lik 1. Dvs. at de teller like mye (1/3 hver). Dette kunne også vært angitt som 0.33 for hver indikator. Dersom den første skal telle 50%, den neste 30% og den siste 20% kan dette angis enten som 0.5, 0.3 og 0.2 eller 5, 3 og 2. Man må imidlertid selv passe på at dette summerer seg til en vekt lik 1.0 (100%), dvs. det gis ingen feilmelding dersom summen av vekter avviker fra 1.0 (100%).

For å vise resultatet velger man visualiseringsmodus (trykker på "visualisering" i menylinja). Dette er vist i figur H.15. (Samme figur uten menylinje på toppen er vist i figur 4.13 i kapittel 4).



Figur H.15 Trestruktur-diagram som viser resultatet på alle nivå

Også her tar vi med ikonene oppe til høyre på menylinja og hvilken betydning de har:



Fra venstre har vi "INDIKATOR FOR LAGRINGSSTATUS", "LAST NED SOM BILDE", "FILTER", "LAST NED SOM EXCEL FIL" og "LOGG UT". (NB! BRUKERGUIDE-ikonet er nå fjernet fra redigerings- og visualiseringsmodus. Det vises kun på forsiden.)

Figur 4.13 i kapittel 4 er lastet ned som bilde (som da ikke tar med menylinja). Filter gir mulighet for eksempelvis å se kun på en utvalgt fase, eller elementer som er kritisk dårlige (mørk rød) eller svært bra (mørk grønn).

Vedlegg I: Påkrevde analyser og planer

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
Styring og kriseledelse	Grunnloven			
	Sivilbeskyttelsesloven (2020)	Kommuner	Helhetlig risiko- og sårbarhetsanalyse (ROS) § 14	Beredskapsplan § 15
		Europeisk kritisk infrastruktur ⁴⁹	Risikoanalyse med grunnlag i alvorlige trusselscenarioer, hver aktivas sårbarheter og potensielle konsekvenser (§ 24 b)	Operatørsikkerhetsplan § 24b
		Departementer	Annet hvert år utarbeide en generell rapport om de typer risiko, trusler og sårbarhet som er registrert mot sektorer hvor det er utpekt europeisk kritisk infrastruktur § 24d	
	Politoloven			
	Beredskapsloven			
	Næringsberedskapsloven			
	Energiloven			
	Helseberedskapsloven	Se Helse og omsorg under		
	Samordningsinstruksen			

⁴⁹ Identifisert og utpekt av hvert enkelt departement innenfor sitt myndighetsområde. Eier eller operatør av objektet plikter overfor departementet å foreslå hvilke objekter som potensielt kan være europeisk kritisk infrastruktur (Sivilbeskyttelsesloven, 2011, § 24a)

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Samfunnssikkerhetsinstruksen (2017)	Departementene	Systematiske risiko- og sårbarhetsanalyser med grunnlag i vurdering av tilsiktede og utilsiktede hendelser som kan true departementets og sektorens funksjonsevne og sette liv, helse og materielle verdier i fare (pkt. IV)	Planverk for håndtering av uønskede hendelser. Kontinuitetsplaner og departementets egen underliggende plan til Sivilt beredskapssystem. Tiltaksplan med funn og læringspunkter etter evaluering av hendelser og øvelser (pkt. IV)
		Hovedansvarlige departementer for enkelte kritiske samfunnsfunksjoner	Risiko- og sårbarhetsanalyser for de kritiske samfunnsfunksjonene (pkt. V)	
	Vedtak om Sivilt beredskapssystem (SBS)			
	Vedtak om Beredskapssystem for Forsvaret (BFF)			
	Instruks for Fylkesmannens og Sysselmannen på Svalbards arbeid med samfunnssikkerhet og beredskap og krisehåndtering (2015)	Fylkesmannen	Risiko- og sårbarhetsanalyse (fylkesROS) for fylket (pkt. IV)	4-årig oppfølgingsplan med ansvarsavklaringer (oppdateres årlig) (pkt. IV)
				Beredskapsplan (egen-beredskap) inkl. plan for krisekommunikasjon (pkt. VIII)
	Instruks for Fylkesmannens ansvar for samordning av krisehåndtering ved uønskede hendelser i fylket			
	Forskrift om kommunal beredskapsplikt	Kommuner	Helhetlig risiko- og sårbarhetsanalyse (§ 2). Avdekkes behov for videre detaljanalyser skal ytterligere	Utarbeide langsiktige mål, strategier, prioriteringer og plan for oppfølging av samfunnssikkerhets- og

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
			analyser foretas, ev oppfordre andre relevante aktører til å gjennomføre disse	beredskapsarbeidet (§ 3). Overordnet beredskapsplan (§ 4)
	Forskrift om krav til beredskapsplanlegging (2001)	Stat, kommuner, fylkeskommuner, regionale helseforetak, helseforetak, Mattilsynet og vannverk	Risiko- og sårbarhetsanalyser (skal alltid omfatte selve virksomheten, dets ansvarsområde og lokale forhold som innvirker på virksomhetens sårbarhet) § 3	Beredskapsplan § 2 (skal også omfatte informasjonstiltak § 5)
	Forskrift om virksomheten i Norsk rikskringkasting under beredskap og krig	Norsk rikskringkasting		
Forsvar	Grunnloven			
	Beredskapsloven			
	Sikkerhetsloven (2019)	Statlige, fylkeskommunale og kommunale organer	Regelmessige risikovurderinger (§ 4-2)	
		Andre virksomheter ⁵⁰	Regelmessige risikovurderinger (§ 4-2)	
	Lov om Etterretningstjenesten			
	Rekvisisjonsloven			
	Instruks for Forsvarssjefen			
	Instruks om Forsvarets bistand til politiet			
	Vedtak om Beredskapssystem for Forsvaret (BFF)			
	Vedtak om Sivilt beredskapssystem (SBS)			

⁵⁰ Et departement skal innenfor sitt ansvarsområde fatte vedtak om at loven helt eller delvis skal gjelde for virksomheter som a) behandler sikkerhetsgradert informasjon, b) råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller c) driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner (Sikkerhetsloven, 2019, § 1-3)

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Direktiver for militære befalingsmenn og militære sjefer ved væpnet angrep på Norge			
	Instruks for Politiets sikkerhetstjeneste			
Lov og orden	Grunnloven			
	Politielloven			
	Sikkerhetsloven (2019)	Se Forsvar over		
	Straffeloven 2005			
	Straffeprosessloven			
	Utlendingsloven			
	Tolloven			
	Straffegjennomføringsloven			
	Psykisk helsevernloven			
	Alminnelig tjenesteinstruks for politiet			
	Instruks for Politiets sikkerhetstjeneste			
	Påtaleinstruksen			
Helse og omsorg	Helseberedskapsloven (2001)	Kommuner, fylkeskommuner, regionale helseforetak og staten		Beredskapsplan for de helse- og omsorgstjenester eller sosialtjenester de skal sørge for et tilbud av eller er ansvarlige for (§ 2-2)
		Sykehus som omfattes av § 1-3 første ledd bokstavene a og b, og virksomheter nevnt i bokstavene d og e		Beredskapsplan for virksomheten (§ 2-2)
	Spesialisthelsetjenesteloven			
	Helseforetaksloven			
	Psykisk helsevernloven			
	Pasient- og brukerrettighetsloven			

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Helse- og omsorgstjenesteloven			
	Sosialtjenesteloven			
	NAV-loven			
	Smittevernloven (2020)	Kommunelegen		Utarbeide forslag til plan for helse- og omsorgstjenestens arbeid med vern mot smittsomme sykdommer, herunder beredskapsplaner og -tiltak, og organisere og lede dette arbeidet (§ 7-2)
		Regionale helseforetak		Plan om det regionale helseforetakets tiltak og tjenester for å forebygge smittsomme sykdommer eller motvirke at de blir overført (§ 7-3)
		Folkehelseinstituttet	Helseanalyser (§ 7-9)	
	Folkehelseloven			
	Matloven			
	Legemiddeloven			
	Apotekloven			
	Arbeidsmiljøloven			
	Strålevernloven			
	Atomenergiloven			
	Forskrift om krav til beredskapsplanlegging (2001)	Se styring og kriseledelse over		
	Prioriteringsforskriften			
	Akuttmedisinforskriften			
	Psykisk helsevernforskriften			

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Forskrift om internkontroll i helse- og omsorgstjenesten			
	Forskrift om Meldingssystem for smittsomme sykdommer (MSIS-forskriften)			
	Forskrift om varsling av og tiltak ved alvorlige hendelser av betydning for internasjonal folkehelse (IHR-forskriften)			
	Drikkevannsforskriften (2016)	Se Vann og avløp under		
	Strålevernforskriften			
	Mandat for og sammensetning av Kriseutvalget for atomberedskap med rådgivere, samt mandat for fylkesmannen			
	Delegering av kongens myndighet etter strålevernsloven § 16, annet ledd til Kriseutvalget for atomberedskap			
	Atomberedskap – sentral og regional organisering			
Redningstjenester	Politi-loven			
	Brann- og eksplosjonsloven			
	Helseberedskapsloven (2001)	Se helse og omsorg over		
	Helse- og omsorgstjenesteloven			
	Spesialisthelsetjenesteloven			
	Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret			
	Kystvaktloven			
	Heimevernloven			
	Havne- og farvannsloven			
	Brann- og eksplosjonsvernloven			
	Forurensningsloven			

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Petroleumsloven			
	Folkehelseloven			
	Plan- og bygningsloven (2013)	Kommuner		Kommunal planstrategi, kommuneplan og reguleringsplan (§ 3-3)
		Fylkesting		Regional planstrategi, regionale planer og regional planbestemmelse (§ 3-4)
		Planmyndighet	Risiko- og sårbarhetsanalyse for planområdet (§ 4-3)	
	Arbeidsmiljøloven			
	Eksportkontrollloven			
	Konvensjon om forbud mot utvikling, produksjon, lagring og bruk av kjemiske våpen samt ødeleggelse av slike av 1993			
	Organisasjonsplan for redningstjenesten			
	Politiinstruksen – Alminnelig tjenesteinstruks for politiet			
	Forskrift om krav til akuttmedisinske tjenester utenfor sykehus			
	Instruks om Forsvarets bistand til politiet			
	Instruks for fylkesmannens og Sysselmannens arbeid med samfunnssikkerhet, beredskap og krisehåndtering (2015)	Fylkesmannen	Risiko- og sårbarhetsanalyse (fylkesROS) for fylket (pkt. IV)	4-årig oppfølgingsplan med ansvarsavklaringer (oppdateres årlig) (pkt. IV)
				Beredskapsplan (egenberedskap) inkl. plan for krisekommunikasjon (pkt.

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
				VIII)
	Storulykkeforskriften	Storulykkevirksomheter ⁵¹	Strategi for å forebygge og begrense storulykker (§ 7). Sikkerhetsrapport (§ 9)	Intern beredskapsplan (og sørge for at relevante nød- og beredskapsetater og kommune får tilstrekkelig info til sine eksterne beredskapsplaner) (§ 11)
	Forskrift om håndtering av farlig stoff			
	Forskrift om håndtering av eksplosjonsfarlig stoff			
	Forskrift om håndtering av utgangsstoffer for eksplosiver			
	Forskrift om landtransport av farlig gods			
	Forskrift om deklarering av kjemikalier til produktregisteret			
	Forskrift om registrering, vurdering, godkjenning og begrensnings av kjemikalier			
	Forskrift om klassifisering, merking og emballering av stoffer og stoffblandinger			
	Forskrift om helse, miljø og sikkerhet i petroleumsvirksomhet			
	Internkontrollforskriften			
	Forskrift om industrivern			
	Forskrift om internkontroll			

⁵¹ Ethvert privat eller offentlig foretak hvor farlige kjemikalier forekommer, og der mengden kjemikalier er lik eller større enn grenseverdiene i vedlegg I del 1 eller del 2, herunder foretak som ikke sysselsetter arbeidstaker (§ 3)

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
IKT-sikkerhet	Personopplysningsloven			
	Ekonomi-loven			
	Helseregisterloven			
	Pasientjournalloven			
	Arkivloven			
	Sikkerhetsloven (2019)	Se Forsvar over		
	Forvaltningsloven			
	Personopplysningsforskriften			
	eForvaltningsforskriften			
	Forskrift om objektsikkerhet			
	Forskrift om informasjonssikkerhet			
	Arkivforskrifta			
Natur og miljø	Forurensningsloven			
	Brann- og eksplosjonsvernloven			
	Folkehelseloven			
	Forskrift om inngrep på åpent hav og i Norges økonomiske sone i tilfelle av havforurensning eller fare for forurensning av olje eller andre stoffer som følge av en sjøulykke			
	Vedtekter for Meteorologisk institutt			
	Forskrift om flyværtjeneste			
Forsyningsikkerhet	Næringsberedskapsloven			
	Beredskapsloven			
	Lov om militære rekvisisjoner			
	Sivilbeskyttelsesloven (2020)	Se Styring og kriseledelse over		
	Petroleumsloven			
	Lov om beredskapslagring av petroleumsprodukter			

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Naturgassloven			
	Næringsberedskapsloven			
	Forskrift om beredskapslagring av petroleumsprodukter			
Vann og avløp	Folkehelseloven			
	Lov om kommunale vass- og avløpsanlegg			
	Sivilbeskyttelsesloven (2020)	Se Styring og kriseledelse over		
	Helseberedskapsloven (2001)	Se Helse og omsorg over		
	Forurensningsloven			
	Plan- og bygningsloven (2013)	Kommuner		Kommunal planstrategi, kommuneplan og reguleringsplan (§ 3-3) sikre at drikkevannshensynet ivaretas
		Fylkestinget		Regional planstrategi, regionale planer og regional planbestemmelse (§ 3-4) sikre at drikkevannshensynet ivaretas
		Planmyndighet	Risiko- og sårbarhetsanalyse for planområdet § 4-3	
	Drikkevannsforskriften (2016)	Vannverkseiere		Driftsplaner og beredskapsplaner for å levere tilstrekkelig mengder drikkevann til enhver tid
		Vannverkseiere av vannforsyningssystemer med produsert vann per døgn på minst 10 m³ drikkevann, eller som forsyner en eller flere		Plan for beredskapsøvelser (§ 11)

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
		sårbare abonnenter		
		Kommuner		Ta drikkevannshensyn når arealdelen av kommuneplanen og reguleringsplaner utarbeides (§ 26)
		Fylkeskommuner		Ta drikkevannshensyn når regionale planer utarbeides, samt ivareta drikkevannshensyn i regionale vannforvaltningsplanene etter vannforskriften (§ 27)
	Forskrift om begrensning av forurensning			
	Forskrift om miljørettet helsevern			
Finansielle tjenester	Sentralbankloven			
	Betalingssystemloven			
	Finanstilsynsloven			
	Verdipapirhandelloven			
	Finansforetakloven			
	Verdipapirregisterloven			
Kraftforsyning	Energiloven (2018)	Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for effektiv sikring og beredskap		Vedtak om beredskapstiltak kan blant annet omfatte krav til organisering, planlegging, forebygging, sikkerhets- eller sikringstiltak, utførelse, gjennomføring, gjenopprettingsevne, ledelse eller drift.
	El-tilsynsloven			

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Sivilbeskyttelsesloven (2020)	<i>Se Styring og kriseledelse over</i>		
	Energilovforskriften			
	Systemansvarforskriften			
	Rasjoneringsforskriften			
	Kraftberedskapsforskriften (2019)	Virksomheter omfattet av forskriften (KBO-enheter) ⁵²	Risikovurdering knyttet til ekstraordinære forhold (§ 2-3). Risikovurdering av digitale informasjonssystemer (§ 6-9)	Beredskapsplan for å håndtere og begrense virkningene av ekstraordinære situasjoner (§1-5). Oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang (§ 2-4). Informasjonsplan (§ 2-8)
	Forskrift om elektriske forsyningsanlegg			
Elektroniske kommunikasjonsnett og -tjenester	Ekomloven			
	Sikkerhetsloven (2019)	<i>Se Forsvar over</i>		
	Ekomforskriften			
	Klassifiseringsforskriften			
	Forskrift om prioritet i mobilnett			
Transport	Veglova (2020)	Statens vegvesen, fylkeskommune og kommune	Loven pålegger ingen krav om analyser eller planer, men stadfester at ansvarlige aktører har et selvstendig ansvar for samfunnstrygghet og beredskap for henholdsvis riksvei, fylkesvei og kommunal vei (§ 10)	
	Vegtrafikkloven			
	Luftfartsloven			
	Jernbaneloven			

⁵² De virksomheter som er KBO (kraftforsyningens beredskapsorganisasjon)-enheter etter § 2-1 annet ledd bokstav a eller som er blitt KBO-enheter etter § 2-1 annet ledd bokstav b (Kraftberedskapsforskriften, 2019, § 1-3)

Funksjon	Sentrale lover og forskrifter	Ansvarlig aktør	Påkrevde analyser	Påkrevde planer
	Sjøloven			
	Havne- og farvannsloven			
	Losloven			
	Forurensningsloven			
	Næringsberedskapsloven			
	Forskrift for sivil transportberedskap			
Satellittbaserte tjenester	Ekomloven			
	Sikkerhetsloven (2019)	Se Forsvar over		
	EØS-avtalen, vedlegg XIV			
	Forskrift om etablering, drift og bruk av jordstasjon for satellitt			
	Forskrift om objektsikkerhet			



Teknologi for et bedre samfunn

www.sintef.no