Kunnskapsdepartementet

Styringsdokument

Styringsdokument for arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren

Oktober 2016

Innholdsfortegnelse

Forord

Det norske samfunnet oppleves som trygt for de fleste av oss. Likevel inntreffer det fra tid til annen hendelser som rokker ved denne tryggheten. Det kan være store ulykker, ekstremvær og flom, klimaproblemer, eller tilsiktede handlinger fra mennesker. De store teknologiske endringene gir oss også noen utfordringer. Denne virkeligheten utfordrer aktører på ulike nivå til planlegging og iverksetting av tiltak og økt beredskap.

Samfunnssikkerhet berører oss alle. Kunnskapsdepartementet har det overordnede ansvaret for samfunnssikkerhet og beredskap i kunnskapssektoren. For at vi skal lykkes med å forvalte dette ansvaret må alle i kunnskapssektoren være seg sitt ansvar bevisst. Alle nivåer og aktører i sektoren må gjøre de nødvendige tiltak for å forebygge at det inntreffer uønskede hendelser og minske konsekvensene av de hendelsene som likevel inntreffer.

For å bidra til en systematisk og god oppfølging av arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren, utviklet Kunnskapsdepartementet i 2011 et overordnet styringsdokument for dette arbeidet. Styringsdokumentet foreligger nå i revidert versjon.

Styringsdokumentet er revidert i tråd med utvikling på feltet etter 2011. Det gjelder blant annet instruksen for departementenes arbeid med samfunnssikkerhet og beredskap som ble nedfelt i en kongelig resolusjon 15. juni 2012, stortingsmeldingen om samfunnssikkerhet fra 2012 og Nasjonal strategi for informasjonssikkerhet.

Departementet utredet i 2015 departementets sektoransvar for samfunnssikkerhet og beredskap, og det ble utarbeidet en risiko- og sårbarhetsanalyse av sektoren. Begge disse ligger til grunn for revisjonen av styringsdokumentet.

Kunnskapssektoren omfatter store deler av befolkningen, og virksomhetene i sektoren er svært forskjellige - både i størrelse, oppgaver, eierskap og tilknytningsform til departementet. Den omfatter blant annet private og kommunale barnehager og skoler, stiftelser, statlige og private universiteter og høyskoler og aksjeselskap. For den enkelte virksomhet vil det derfor variere i hvilken grad styringsdokumentet stiller krav eller kommer med anbefalinger. For alle virksomheter inneholder dokumentet mer veiledning enn tidligere.

Vi har et stort ansvar i kunnskapssektoren. Departementets mål med styringsdokumentet er å legge til rette for at hele sektoren kan nå det felles målet om at drøyt 1,6 mill. barnehagebarn, elever, studenter og ansatte skal være trygge der de oppholder seg store deler av dagen.

Lykke til i dette viktige arbeidet!

Foto: Marte Garmann

Torbjørn Røe Isaksen
kunnskapsminister

1. Overordnet mål

Kunnskapsdepartementet har det overordnede ansvaret for samfunnssikkerhet og beredskap i kunnskapssektoren.

Kunnskapsdepartementets overordnede mål for arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren er å forebygge uønskede hendelser og minske konsekvensene av de hendelsene som likevel oppstår

For å bidra til en systematisk og god oppfølging av arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren, utviklet Kunnskapsdepartementet i 2011 et overordnet styringsdokument for dette arbeidet. Styringsdokumentet som nå er revidert henvender seg til alle nivåer og aktører i kunnskapssektoren og gir en oversikt over ansvarsforhold, grunnleggende tiltak og departementets oppfølging av arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren.

Styringsdokumentet må sees i sammenheng med andre styringsdokumenter i sektoren, herunder statsbudsjettet og tildelingsbrev til virksomhetene.

Krav, føringer og veiledning i styringsdokumentet må sees i sammenheng med styringslinjer, styringsvirkemidler og hjemmelsgrunnlag for de ulike eierskap og tilknytningsformer som gjelder for den enkelte virksomhet i kunnskapssektoren. For departementets underliggende virksomheter innebærer dette i hovedsak krav til arbeidet på feltet, mens det for resten av sektoren i større grad må forstås som sterke anbefalinger.

2. Ansvar og organisering

Kongelig resolusjon av 15.06.2012[1] er departementenes instruks for arbeidet med samfunnssikkerhet og beredskap, og Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentrale krisehåndtering. Instruksen slår fast at det departementet som har ansvar for en sektor til daglig, også har ansvaret for samfunnssikkerhet og beredskap i sektoren. Sektoransvaret er grunnleggende innenfor samfunnssikkerhets- og beredskapsarbeidet i Norge. Dette innebærer blant annet at hvert departement forventes å ha både en grunnleggende oversikt over risiko og sårbarhet, og en god styring med det forebyggende arbeidet i sektoren. I henhold til instruksen har Justis- og beredskapsdepartementet også et generelt samordningsansvar på tvers av sektorene for å sikre et helhetlig og koordinert samfunnssikkerhetsarbeid i sivil sektor. Det enkelte departement rapporterer til Justis- og beredskapsdepartementet. På vegne av Justis- og beredskapsdepartementet gjennomfører Direktoratet for samfunnssikkerhet og beredskap (DSB) jevnlige tilsyn med departementene.

Kunnskapsdepartementets styringsdokument bygger på de fire grunnleggende prinsippene[2] i den nasjonale beredskapstilnærmingen:

Ansvarsprinsippet som betyr at den som har et ansvar i en normalsituasjon også har dette ansvaret i tilfelle ekstraordinære hendelser

Likhetsprinsippet som betyr at den organisasjonen som skal håndtere en krise, er mest mulig lik den daglige organisasjonen

Nærhetsprinsippet som betyr at kriser skal håndteres på lavest mulig nivå

Samvirkeprinsippet som betyr at alle aktører har et selvstendig ansvar for å sikre optimalt samvirke og samarbeid med relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering

Det er krav til at arbeidet med samfunnssikkerhet og beredskap skal være målrettet, systematisk og sporbart og være integrert i departementets planverk, styringssystemer og i styringsdialogen med underliggende virksomheter.[3] Det er departementets fagavdelinger som har ansvaret for samfunnssikkerhets- og beredskapsarbeidet innenfor eget ansvarsområde. Administrasjons- og økonomiavdelingen har et pådriver- og koordineringsansvar for samfunnssikkerhets- og beredskapsarbeidet i departementet og kunnskapssektoren.

[1] Kgl.res av 15.06.2012 fra Justis- og beredskapsdepartementet *"Instruks for departementets arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering"*

[2] Meld. St. 29 (2011-2012 Samfunnssikkerhet 2012)

[3] Prop. 1 S (2014-2015) for Justis- og beredskapsdepartementet.

3. Begrepsbruk og avgrensning

Samfunnssikkerhet kan beskrives som den evne samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger. Samfunnssikkerhetsbegrepet dekker sikkerhet innenfor hele spekteret av utfordringer, fra begrensede hendelser via større krisesituasjoner som representerer omfattende fare for liv, helse, miljø og materielle verdier, til sikkerhetsutfordringer som truer nasjonens selvstendighet eller eksistens.[4]

Samfunnssikkerhet innebefatter vern av samfunnet mot hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller av bevisste handlinger.[5]

Forebygging handler om iverksetting av tiltak for å redusere sannsynligheten for en hendelse og for å redusere konsekvensene av en hendelse dersom den likevel inntreffer.

Begrepet *beredskap* er definert som planlegging og forberedelser av tiltak for å begrense konsekvenser av uønskede hendelser og planer for å håndtere kriser eller andre uønskede hendelser på best mulig måte. Beredskapstiltak er tiltak som det er planlagt eller etablert systemer for, men som først iverksettes når en hendelse er under utvikling eller har inntruffet.[6]

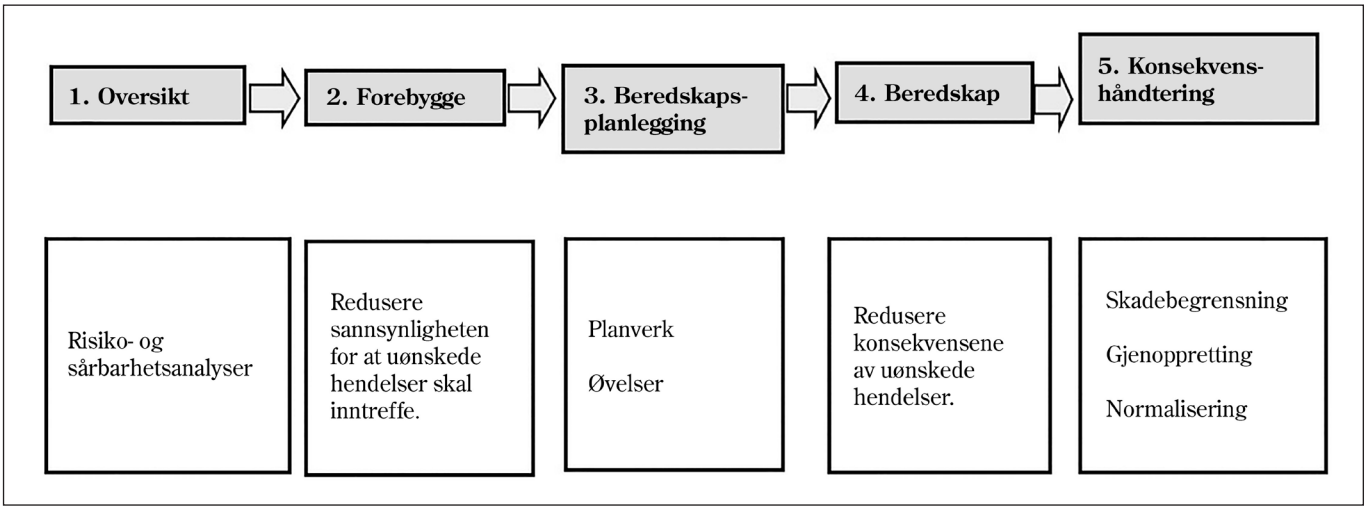
I dette styringsdokumentet brukes samlebegrepet *samfunnssikkerhets- og beredskapsarbeid* om alt forebyggende arbeid, innenfor hele spekteret av utfordringer kunnskapssektoren og den enkelte virksomhet står overfor, og alt arbeid for å begrense eller håndtere kriser eller andre uønskede hendelser på en best mulig måte. Begrepet avgrenses mot arbeidsmiljørelatert HMS-arbeid.

Med *kriser* menes en situasjon som truer eller kan true en organisasjons kjernevirksomhet og/eller troverdighet. Ikke alle hendelser er kriser – det er først når hendelsen krever en annen måte å organisere arbeidet på enn ved en normalsituasjon at man kan snakke om en krise.

Sammenhengen mellom elementene i samfunnssikkerhets- og beredskapsarbeidet kan illustreres som i figuren under:

[4] Innst. S. nr. 9 (2002–2003), St.meld. nr. 17 (2001–2002) Samfunnssikkerhet.
[5] Innst. 426 S (2012–2013), Meld. St. 29 (2011–2012) Samfunnssikkerhet.

[6] DSBs veileder Departementenes systematiske samfunnssikkerhets- og beredskapsarbeid. 2015-versjon 1.0, s.10



4. Styringslinjer i kunnskapssektoren

4.1 Kunnskapsdepartementets sektoransvar

Det følger av Justis- og beredskapsdepartementets instruks at departementene har ansvar for samfunnssikkerhet og beredskap innenfor egen sektor. Det er imidlertid opp til det enkelte departement å avgrense ansvaret og virkemidlene i styringen av sin sektor.

Kunnskapssektoren omfatter store deler av befolkningen og er preget av stort mangfold. Barnehagetilsatte, lærere, vitenskapelig personale og andre i sektoren utgjør om lag 300 000 tilsatte. Totalt omfatter kunnskapssektoren om lag 1,6 mill. barn og voksne. Obligatorisk tiårig grunnskole og høy dekningsgrad i barnehage og videregående opplæring gjør at en svært stor andel av årskullene fra ett til 19 år oppholder seg i barnehage eller skole mange timer daglig. Både barnehager, grunnskoler, videregående skoler og lærebedrifter har et ansvar for at barn og unge er trygge der de er. Dette handler både om personlig trygghet med tanke på liv og helse, og om sikkerhet for at f. eks. personopplysninger om enkeltindivider ikke kommer på avveie. Dette er en utfordring med tanke på beredskap både for den enkelte barnehage- og skoleeier, og for den enkelte barnehage og skole. Tilsvarende vil det være store ansamlinger av studenter og ansatte ved universiteter og høyskoler. Videre forvaltes det betydelige verdier som historiske bygninger, forskningsdata og samlinger ved universiteter, høyskoler og universitetsmuseene ved universitetene i Oslo, Bergen, Trondheim, Tromsø og Stavanger.

Meteorologisk institutt har en særskilt rolle som forvalter av kritisk infrastruktur. Meteorologiske tjenester utgjør en kritisk allmenn innsatsfaktor ved at det leveres nødvendig meteorologisk informasjon til befolkningen og andre virksomheter med kritisk samfunnsfunksjon.

Virksomhetene og institusjonene i kunnskapssektoren har ulike eierskap og tilknytningsformer. Det er blant annet kommunale og private barnehager, kommunale, fylkeskommunale og private skoler, fylkeskommunale og private fagskoler, statlige og private universiteter og høyskoler. I tillegg kommer folkehøyskoler, som i stor grad er eid av stiftelser. Kunnskapsdepartementets arbeid med samfunnssikkerhet og beredskap i kunnskapssektoren må derfor sees i sammenheng med øvrige styringslinjer og virkemidler som departementet har til rådighet.

Kunnskapsdepartementet har definert nærmere hvordan beredskapen ved virksomheter med ulike tilknytingsformer skal følges opp. Departementet har det overordnede ansvar for samfunnssikkerhet og beredskap i alle de underliggende statlige virksomhetene, barnehagesektoren, det meste av opplæringssektoren og mange private virksomheter i UH-, fagskole- og samskipnadssektoren. Det er kommunene som har det operative ansvaret for samfunnssikkerhet og beredskap i skoler og barnehager, og fylkeskommunene har tilsvarende for videregående skoler.

4.2 Avgrensning av departementets sektoransvar

Virksomheter som departementet kun i begrenset grad er involvert i, for eksempel ved å gi delvis støtte til drift eller andre aktiviteter til private virksomheter, er vurdert å være innenfor sektoren som sådan, men utenfor departementets ansvar i forhold til samfunnssikkerhet og beredskap. For enkelte virksomhetstyper og aktiviteter er det særlig krevende å avgrense sektoransvaret. Det gjelder først og fremst statlig eide aksjeselskaper, der styret har en betydelig rolle, og virksomheter og aktivitet i utlandet.

Aksjeselskaper

Hvert aksjeselskap må vurderes særskilt med hensyn til om de er innenfor eller utenfor sektoransvaret. Kunnskapsdepartementet forvalter p.t. eierskapet i UNINETT, Simula Research Laboratory, CESSDA, Norsk samfunnsvitenskapelig datatjeneste og Universitetet på Svalbard. I tillegg har de statlige universitetene og høyskolene ulikt eierskap i om lag 100 selskaper.

Forvaltningen av aksjeselskap ligger til styret. Styret skal sørge for forsvarlig organisering av virksomheten og føre tilsyn med den daglige ledelse og selskapets virksomhet for øvrig. Gjennom eierstyring i generalforsamlingen utøver departementet som aksjeeier den øverste myndighet i selskapet. Imidlertid er det et generelt utgangspunkt at generalforsamlingen ikke bør gripe inn i styrets daglige ledelse av selskapet.

Rammene for eierstyring er ikke til hinder for at staten som eier tar opp forhold som selskapene bør vurdere i tilknytning til sin virksomhet og utvikling. De synspunkter staten gir uttrykk for i slike sammenhenger er å betrakte som innspill til selskapets administrasjon og styre. Styret har ansvar for å forvalte selskapets eierandeler til beste for eierne, og må foreta de konkrete avveininger og beslutninger. I aksjeselskaper som eies av departementets underliggende virksomheter med minst 51 prosent, må institusjonene vurdere å tilrettelegge for arbeidet med samfunnssikkerhet og beredskap. Statens andel av eierskapet, hvor mye offentlig tilskudd de får, i hvilken grad de utøver oppgaver på vegne av staten, og om aksjeselskapenes virksomhet omfatter ansvar for studenter og ansatte ved statlige institusjoner, vil være relevante kriterier å vurdere dette etter.

Virksomheter i utlandet

Det er et betydelig antall norske borgere i utlandet som er i en opplæringssituasjon, arbeider med forskning eller er engasjert i annen aktivitet som er knyttet til kunnskapssektoren. Utenriksdepartementet har hovedansvaret for håndtering av sivile kriser i utlandet. Utenriksdepartementet gir råd og tips på sine landsider og utsteder offisielle reiseråd. Ansvars- og nærhetsprinsippet tilsier at den enkelte virksomhet har ansvar for å etablere egne forebyggende tiltak og for beredskapsplanlegging som skal ivareta elever og studenters sikkerhet i utlandet.

4.3 Krav til beredskap

Barnehagesektoren

Barnehageeier har ansvaret for at virksomheten drives i samsvar med gjeldende lover og regelverk. Kommunene eier ca. halvparten av barnehagene, og har således en rolle både som barnehageeier og barnehagemyndighet. Myndighetsoppgavene omfatter alle barnehagene i kommunen, både kommunale og ikke-kommunale. Som sektormyndighet må Kunnskapsdepartementet sikre at det påligger krav til departementets institusjoner i kommunene, slik at alle relevante aktører blir ansvarliggjort og bidrar inn i det helhetlige arbeidet. Slike krav påligger barnehager fra mai 2015. I forskrift om miljørettet helsevern i barnehager og skoler[7] er det presisert i rundskriv I-6/2015 at barnehageeier ved leder av virksomheten plikter å vurdere risiko for alvorlige tilsiktede hendelser, og planlegge beredskap ved virksomheten i henhold til dette risikobildet. Tilsyn med barnehagenes krav til samfunnssikkerhet og beredskap føres av kommunen. Fylkesmannen skal føre tilsyn med at kommunen utfører de oppgaver den er pålagt.

Grunnopplæringssektoren

Skoleeier har ansvaret for at virksomheten drives i samsvar med gjeldende lover og regelverk. Kommunene eier de offentlige grunnskolene og fylkeskommunene eier de videregående skolene. I tillegg kommer private skoleeiere både på grunnskolenivå og videregående nivå.

Fylkesmannen utøver tilsyn, kontrollerer lovligheten av vedtak og behandler klagesaker knyttet til grunnopplæringen. Kunnskapsdepartementet har det overordnede ansvar for utvikling av kvalitet og for styring av opplæringssektoren. Utdanningsdirektoratet er delegert en rekke oppgaver på grunnopplærings- og barnehageområdet.

I forskrift om miljørettet helsevern i barnehager og skoler[8] er det presisert i rundskriv I-6/2015 at skoleeier ved leder av virksomheten plikter å vurdere risiko for alvorlige tilsiktede hendelser, og planlegge beredskap ved virksomheten i henhold til dette risikobildet. Tilsyn med skolenes krav til samfunnssikkerhet og beredskap føres av kommune og for videregående skoler av fylkeskommunen. Fylkesmannen skal føre tilsyn med at kommunen utfører de oppgaver den er pålagt.

Høyere utdanning

De statlige høyere utdanningsinstitusjonene er virksomheter med egne styrer med særskilte fullmakter direkte underlagt Kunnskapsdepartementet. Dette medfører at Kunnskapsdepartementet har et særskilt ansvar for beredskapen ved disse institusjonene. For de private høyskolene er det ikke en direkte styringslinje, men det er en dialog med disse virksomhetene og departementet oppfordrer institusjonene til å arbeide med samfunnssikkerhet og beredskap.

Fagskoleutdanning

Fagskolene er enten private eller underlagt fylkeskommunene (en fagskole er direkte underlagt departementet). Her er det ulike styringslinjer. Den statlige følger den samme styringslinjen som for høyere utdanning. De fylkeskommunale følger samme styringslinje som videregående opplæring, mens det ikke er en styring av

[7] Forskrift om miljørettet helsevern i barnehager og skoler mv. (Helse og omsorgsdepartementet) trådt i kraft 1.1.1996.

[8] Forskrift om miljørettet helsevern i barnehager og skoler mv. (Helse og omsorgsdepartementet) trådt i kraft 1.1.1996.

de private fagskolene utover de krav som følger av tilskuddsbrev. Departementet har derimot et overordnet tilsynsansvar for fagskolene.

Studentsamskipnader

Studentsamskipnader forvalter studentvelferden på vegne av staten, men er private og ikke en del av staten. Departementet har ingen direkte styring og har ikke stilt krav i tilskuddsbrev til arbeidet med samfunnssikkerhet og beredskap, men er i dialog med samskipnadene og oppfordrer disse til å arbeide med samfunnssikkerhet og beredskap.

Folkehøyskoler

Folkehøyskoler er enten i privat eie eller fylkeskommunale. Folkehøyskolelovens regulering er ikke detaljert og gir få rettigheter og plikter, sammenlignet med offentlige skoler eller friskoler. Dette har sammenheng med folkehøyskolenes særlige funksjon, altså at det ikke gis opplæring som resulterer i vitnemål eller tilsvarende dokumentasjon på oppnådd kompetanse.

Kunnskapsdepartementet stiller ikke direkte krav til folkehøyskolenes arbeid med samfunnssikkerhet og beredskap, men anbefaler at det tas utgangspunkt i veiledningen om beredskapsarbeid som er tilgjengelig på Utdanningsdirektoratets nettsider.

Underliggende virksomheter

I tillegg til de høyere utdanningsinstitusjonene har Kunnskapsdepartementet ansvaret for noen større statlige virksomheter som Utdanningsdirektoratet, Statens lånekasse for utdanning, Norges forskningsråd, Meteorologisk institutt og VOX. Kunnskapsdepartementet har særskilt ansvar for beredskapen i disse virksomhetene.

Utdanningsdirektoratets veiledningsmateriell

Utdanningsdirektoratet har sammen med Politidirektoratet utarbeidet en veiledning i beredskapsplanlegging Alvorlige hendelser i barnehager og utdanningsinstitusjoner

Veilederen skal følges opp av politiet gjennom et opplæringsprogram som blir gjennomført av lokalt politi, og retter seg mot eiere av barnehager og utdanningsinstitusjoner. På nettsiden til Utdanningsdirektoratet ligger også annet veiledningsmateriell som gir praktiske råd i beredskapsarbeidet.

4.4 Departementets oppfølging av underliggende virksomheter

Kunnskapsdepartementet bruker den ordinære styringsdialogen med virksomhetene til å følge opp spørsmål knyttet til samfunnssikkerhet og beredskap. Dette innebærer at departementet bruker tildelingsbrev, etatsstyringsmøter og egne tilsyn til å ta opp disse spørsmålene med virksomhetene.

Tildelingsbrev

Målsettinger og resultatoppfølging for samfunnssikkerhets- og beredskapsarbeidet er integrert i eksisterende styringsdokumenter, budsjettproposisjonen (Prp. nr. 1 S) og tildelingsbrevene til underliggende virksomheter. På denne måten skal mål og tiltak for samfunnssikkerhets- og beredskapsarbeidet fanges opp gjennom ordinær virksomhetsstyring og dermed også bli en integrert del av den ordinære resultatoppfølgingen og -rapporteringen.

Tildelingsbrevene skal inneholde en standardtekst om samfunnssikkerhet og beredskap som er felles for alle Kunnskapsdepartementets underliggende virksomheter. For enkelte virksomheter kan det i tillegg benyttes en virksomhetsspesifikk tekst.

Rapportering

På bakgrunn av krav i tildelingsbrevene rapporterer alle virksomheter i sine årsrapporter, med beskrivelse av samfunnssikkerhets- og beredskapsarbeidet ut i fra kravene. Vesentlige avvik skal rapportertes særskilt til Kunnskapsdepartementet. Spørsmål om samfunnssikkerhet og beredskap kan også tas opp i den vanlige styringsdialogen med departementet eller ved egne tilsyn.

Enkelte virksomheter vil være gjenstand for særskilt rapportering og egne tilsyn fra Kunnskapsdepartementet som fast ordning.

Tilsyn

Departementet gjennomfører regelmessige tilsyn med underliggende virksomheters beredskapsarbeid, jf. krav til oversikt over risiko og sårbarhet i egen sektor i tidligere nevnte kgl.res. av 15.06.2012. Tilsynsrapporten inneholder en konkret vurdering og eventuelle oppfølgingspunkter.

4.5 Risiko- og sårbarhetsanalyse av kunnskapssektoren

En risiko og sårbarhetsanalyse skal gi grunnlag for å utvikle strategier, for å prioritere og utvikle forebyggende og beredskapsmessige tiltak og for øvelser. I 2015 gjennomførte Kunnskapsdepartementet en risiko og sårbarhetsanalyse for kunnskapssektoren. En kortversjon av risiko og sårbarhetsanalysen av kunnskapssektoren (sektor-ROS) er tilgjengelig på Regjeringen.no. Arbeidet med sektoranalysen følger av krav i instruksen fra Justis- og beredskapsdepartementet. Det er avgjørende for departementene å ha oversikt over risiko og sårbarhet i egen sektor for å kunne vurdere og iverksette tiltak for å redusere risikoen og sårbarheten. Kunnskapssektoren er, som beskrevet over, stor og svært sammensatt. Den store ansamlingen av mennesker på avgrensede områder i kunnskapssektoren utgjør en samfunnssikkerhets- og beredskapsmessig utfordring i forhold til ulike scenarioer, som smittefare, ulykker, vold og terror.

Analysen tar for seg alvorlige farer og trusler som kan ramme kunnskapssektoren og gir anbefalinger til hva som kan gjøres for å redusere den risiko som foreligger. En del av Sektor-ROS er scenariobasert og har tatt utgangspunkt i Nasjonalt risikobilde 2014. Analysen viser at kunnskapssektoren kan bli rammet av svært ulike typer hendelser. De har blitt delt inn i kategoriene naturhendelser, store ulykker og tilsiktede handlinger. Dette skyldes blant annet at departementet har virksomheter over hele landet og at virksomhetene er så forskjellige.

Den scenariobaserte delen av analysen viser at ingen hendelser anses å ha høy risiko, men flere anses å ha middels risiko.

5. Fylkesmannen

Det er to ulike styringslinjer som krysser hverandre i arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren. En styringslinje, ofte omtalt som "beredskapslinjen", går fra Justis- og beredskapsdepartementet via DSB til Fylkesmannen og videre til kommunene. Kunnskapsdepartementets styringslinje for barnehage- og opplæringssektoren går via Utdanningsdirektoratet til Fylkesmannen og videre til kommunen.

Fylkesmannen skal bidra til å styrke samfunnssikkerheten og krisehåndteringsevnen på regionalt og lokalt nivå. Fylkesmannen skal utarbeide risiko- og sårbarhetsanalyse for fylket som skal legges til grunn for beredskapsplanleggingen, slik at forebyggende og beredskapsmessige tiltak gjenspeiler de risikoscenarioer som beskrives i ROS-analysen. Embetene skal ha en organisasjon som kan ivareta Fylkesmannens oppgaver innenfor krisehåndtering.

Fylkesmannen har et særlig ansvar for tilsyn, oppfølging og veiledning av kommunene. Fylkesmannen må påse at kommunenes arbeid med samfunnssikkerhet og beredskap i tilstrekkelig grad omfatter barnehager, skoler og eventuelle andre utdanningsinstitusjoner som er lokalisert i den aktuelle kommunen.

6. Kommunen

Kommunene har en nøkkelrolle i arbeidet med samfunnssikkerhet og beredskap. Oversikt over samfunnssikkerhetsarbeidet i landets kommuner er derfor et viktig verktøy for lokale, regionale og sentrale myndigheter.

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret trådte i kraft i 2010. Loven stiller blant annet krav om gjennomføring av helhetlige ROS-analyser, beredskapsplaner og øvelser. Formålet med kommunal beredskapsplikt er trygge og robuste lokalsamfunn. Dette oppnås gjennom systematisk og helhetlig samfunnssikkerhetsarbeid på tvers av sektorer i kommunen. Den helhetlige risiko- og sårbarhetsanalysen er en helt sentral del av dette arbeidet ved å skape oversikt og bevissthet om risiko og sårbarhet i kommunen. Dette danner grunnlag for kommunens langsiktige mål, strategier og tiltak i arbeidet med samfunnssikkerhet og beredskap. (Kommuneundersøkelsen 2014)

Det fremgår av lovens §§ 14 og 15, at kommunen plikter å kartlegge hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kommunen. Resultatet av dette arbeidet skal vurderes og sammenstilles i en helhetlig ROS-analyse. ROS-analysen skal legges til grunn for kommunens arbeid med samfunnssikkerhet og beredskap. Med utgangspunkt i ROS-analysen skal kommunen utarbeide en beredskapsplan som skal inneholde en oversikt over hvilke tiltak kommunen har forberedt for å håndtere uønskede hendelser. Beredskapsplanen skal være oppdatert og revideres minimum én gang per år. Kommunen skal sørge for at planen blir jevnlig øvet.

Resultatene fra kommuneundersøkelsen i 2016 viser at stadig flere kommuner jobber bedre med samfunnssikkerhet og beredskap, men at det fortsatt er en vei å gå før alle kommuner oppfyller alle krav i gjeldene lov og forskrift. Undersøkelsen viser at 48 prosent av kommunene har en helhetlig ROS som i hovedsak tilfredsstiller kommunal beredskapsplikt, og 41 prosent har en overordnet beredskapsplan som oppfyller krav i forskrift om kommunal beredskapsplikt. Videre har 77 prosent øvet sin beredskapsplan og 66 prosent har en plan for oppfølging av arbeidet med samfunnssikkerhet og beredskap.

Kunnskapsdepartementet viser til lovbestemmelsene og forutsetter at kommunenes ROS-analyser, beredskapsplaner og øvelser omfatter barnehager, skoler og eventuelle andre utdanningsinstitusjoner som er lokalisert i den aktuelle kommunen.

7. Grunnleggende tiltak

Kravene i instruksen tilsier at departementene skal ha oversikt over risiko og sårbarhet i egen sektor. For at departementet skal innfri disse kravene og det overordnede målet om å forebygge uønskede hendelser og minske konsekvensene dersom de skulle oppstå, er det viktig at virksomhetene i sektoren jobber systematisk og helhetlig med samfunnssikkerhet og beredskap.

De fire grunnleggende elementene i arbeid med samfunnssikkerhet og beredskap er:

Risiko- og sårbarhetsanalyser (ROS-analyser), forebyggende tiltak, beredskapsplaner og øvelser. Departementets krav og forventninger til sektoren er også knyttet til disse grunnleggende tiltakene, at arbeidet forankres i virksomhetens ledelse og gis nødvendig prioritet.

Det er viktig at det på alle virksomhetsnivåer i kunnskapssektoren:

- Utarbeides virksomhetstilpasset risiko- og sårbarhetsanalyser, samt delanalyser knyttet til særskilte utfordringer i den enkelte virksomhet.
- Utarbeides krise- og beredskapsplaner som sikrer en god krisehåndtering og som styrker organisasjonens krisehåndteringsevne.
- Gjennomføres øvelser for å teste egen beredskap, og for å sette ansatte i stand til å takle utfordringer ved kriser.

7.1 Risiko- og sårbarhetsanalyser

Målet med risiko- og sårbarhetsanalyser er å identifisere uønskede hendelser som kan inntreffe, vurdere risikoen knyttet til hendelsene og utarbeide forebyggende og skadereduserende tiltak. Risikoen ved en hendelse beregnes ofte ut fra en sammenstilling av sannsynlighet og konsekvens. I noen sammenhenger kan imidlertid risiko best beskrives gjennom å vurdere de tre komponentene verdi, trussel og sårbarhet. Trusselen beregnes da på grunnlag av vurderinger av trusselaktørens kapasitet, evne og vilje til å påføre skade. Denne modellen er altså mer tilpasset tilsiktede uønskede handlinger og sannsynlighetsvurderingen er mer implisitt.

Arbeidet med ROS-analyser må tilpasses virksomhetens størrelse og egenart. Det er stor variasjon i kunnskapssektoren, fra små barnehager og skoler til store universitet og høyskoler. Det er derfor viktig at virksomhetene tar utgangspunkt i egen situasjon og tilpasser analysen til hva som er relevant for denne. Dette er også sammenfallende med et grunnleggende krav om at samfunnssikkerhets- og beredskapsarbeidet skal være effektivt og målrettet. ROS-analysene skal være nyttige verktøy i det konkrete arbeidet med samfunnssikkerhet og beredskap.

For de større virksomhetene skal analysene fokusere på risiko knyttet til *samfunnssikkerhet*, ikke HMS eller risikovurdering i forhold til måloppnåelse. Oversikt over risiko innen HMS, jf Internkontrollforskriften, bør ivaretas i en egen HMS-ROS.

Kunnskapsdepartementet anbefaler at virksomhetene tar utgangspunkt i Nasjonalt Risikobilde utarbeidet av Direktoratet for samfunnssikkerhet og beredskap (DSB) når de skal gjøre sine ROS-analyser. I arbeidet med Nasjonalt risikobilde analyserer DSB svært alvorlige hendelser samfunnet bør kunne forebygge og håndtere konsekvensene av. NRB tar utgangspunkt i større kriser som rammer samfunnet som helhet, og som derfor potensielt vil kunne ramme Kunnskapsdepartementets virksomheter.

Det er viktig at ROS-analysen følges opp med konkrete tiltak overfor hendelser som vurderes til å inneha middels og høy risiko. Dette må synliggjøres gjennom utarbeidelse av en egen oppfølgingsplan for disse hendelsene. En slik oppfølgingsplan skal beskrive hva som er gjort, og hva som planlegges utført for å redusere risikoen for at hendelsene kan oppstå og hvilke skadereduserende tiltak som er gjennomført.

ROS-analyser må jevnlig revideres, minst annet hvert år, for at man skal ha et mest mulig oppdatert bilde av risiko- og sårbarhet. Dette vil sikre at analysen fanger opp eventuelle endringer i organisasjonen, oppgaver og trusselbilde.

Departementet har utarbeidet en veiledning som kan være til hjelp i arbeidet med ROS-analyser

Departementet understreker i tilknytning til veilederen at dette er et fagfeltet i stadig utvikling og at metoder og begrepsbruk endrer seg.

7.2 Kriseplanverk

En krise kan oppstå som en plutselig hendelse, som en eskalerende hendelse som gradvis går fra normal håndtering til krisehåndtering eller som en varslet krise. Krisesituasjoner krever ofte svært raske beslutninger

og iverksettelse av tiltak på en raskere og mer effektiv måte enn i en normal situasjon. Det er derfor viktig å ha utarbeidet planverk som raskt kan tas i bruk for å håndtere ulike typer kriser. Planverket skal utarbeides på grunnlag av ROS-analysen.

Planverket må være lett tilgjengelig for de ansatte og bør bl.a. beskrive ansvarsforhold, organisering og rutiner for varsling, informasjon og håndtering av ulike hendelser. Planverket må jevnlig gjennomgås med tanke på revisjon. Dette er særlig aktuelt i forbindelse med evaluering av krisehåndteringen ved faktiske hendelser og øvelser.

7.3 Øvelser

En viktig forutsetning for å lykkes i håndtering av kriser er at involverte medarbeidere i organisasjonen kjenner kriseplanverket og sin rolle og sine oppgaver i en krisesituasjon. Øvelser skal bidra til at planverket og roller er kjent i organisasjonen og være en test på om planverket fungerer.

Ved valg av øvelsesscenario bør virksomhetene ta utgangspunkt i ROS-analysen. Øvelser kan gjennomføres lokalt enten som en skrivebordsøvelse eller som en spilløvelse, hvor det utføres handlinger mot en spillstab som fyller aktuelle roller. Fullskalaøvelse er den mest ressurskrevende måten å øve på. Her øver man mot reelle instanser. Denne øvingsformen ligner mest på en reell situasjon.

Virksomhetene bør vurdere øvelser sammen med eksterne aktører/samarbeidspartnere som kommunen, politiet og andre beredskapsetater. Slike øvelser kan variere i omfang fra å teste varslingsrutiner, til fullskala realistiske øvelser. Tematikk og omfang bør variere.

Departementet vil sterkt anbefale at det som et minimum planlegges og gjennomføres én øvelse per år, men det er ikke nødvendig at hele organisasjonen øves hver gang. Se også punkt 6.4 om skoleskyting. Barnehager bør også øve på evakuering med tanke på ulike hendelser og situasjoner.

Mål og hensikt med øvelsen må defineres og i etterkant må øvelsen evalueres. Øvelser er nødvendige for en kontinuerlig vurdering og evaluering av virksomhetens kriseorganisasjon og kriseplanverk. Evalueringen skal bidra til å avdekke eventuelle forbedringspunkter, slik at nødvendige forbedringstiltak blir identifisert og fulgt opp.

DSB holder på å utarbeide en veileder i planlegging, gjennomføring, evaluering og oppfølging av øvelser som det vil lenkes til når denne er klar.

For virksomheter som kan ha nytte av det, er veiledningen departementet bruker i forbindelse med interne øvelser lagt ved styringsdokumentet.

7.4 Skoleskyting

Nasjonalt risikobilde 2015 beskriver skoleskyting som ett scenario det norske samfunnet bør planlegge for; DSBs delrapport om skoleskyting i Nordland. Scenarioet er lagt til en videregående skole på et tettsted i Nordland.

Risikoanalysen for skoleskyting er basert på informasjon fra forskning, granskingsrapporter og medieomtale av skoleskytinger i andre land. Representanter fra departementer, direktorater og lokale myndigheter har bidratt i arbeidet. Analysen tar for seg bakgrunn, drivkrefter og kontekst for skoleskyting og konkluderer med forutsetningene for skoleskyting er til stede også i Norge.

Rapporten peker på at systematisk arbeid med et inkluderende læringsmiljø, forebygging mot mobbing, gode psykososiale tjenester og samarbeid om lokale beredskapsplaner, er med på å redusere risikoen for skoleskyting her i landet.

Rapporten peker på fem viktige tiltak som kan forebygge skoleskyting:

- Forebygge utenforskap
- Koordinering av instansene som er involvert i forebyggende arbeid og oppfølging av den enkelte elev (skolen, skolehelsetjenesten, kommunehelsetjenesten, politiet, barnevernet m.fl.)
- Skolene må ha en beredskapsplan for skoleskyting, og den må øves
- Lærere, skolehelsetjeneste og andre relevante aktører må ha nødvendig kunnskap om skoleskyting og den typiske gjerningsmannen
- Bygningsmessige tiltak (talevarslingsanlegg, rømningsmuligheter)

Kunnskapsdepartementet legger til grunn at kommunen og skoleledelsen regelmessig vurderer om egne beredskapsplaner både på kommunalt nivå og skolens nivå i tilstrekkelig grad dekker alvorlige hendelser som skoleskyting. Videre vil departementet påpeke at øvelser er en helt sentral del av dette beredskapsarbeidet. Øvelser må gjennomføres på en måte som ivaretar skolens behov for å være forberedt på en alvorlig hendelse, men uten å virke skremmende på elevene.

Departementet forventer at høyere utdanningsinstitusjoner regelmessig vurderer egne beredskapsplaner og gjennomfører øvelser knyttet til alvorlige hendelser.

7.5 Pandemi

Pandemi er et scenario som i Nasjonalt risikobilde vurderes å ha høy sannsynlighet og store samfunnsmessige konsekvenser. Den nasjonale pandemiplanen[9] fastslår at *«Alle departementer og sektorer må planlegge for å forebygge smittespredning og sykdom og opprettholde viktige samfunnsfunksjoner».*

Barnehage- og skolebarn samt ansatte i barnehager/ skoler er utsatte grupper ved en eventuell pandemi. Erfaringsmessig blir barn lett smittet, og i barnehager/ skoler/ SFO er mange barn samlet. Myndigheten til å stenge institusjonene ligger iht. smittevernloven hos den enkelte kommune (gjelder også private barnehager/skoler). Helsemyndighetene kan fatte vedtak om stenging av slike institusjoner for hele eller deler av landet. Behovet for omfattende stenging må nøye avveies mot de store samfunnsmessige ringvirkningene dersom mange friske arbeidstakere må være hjemme med friske barn på grunn av stengte barnehager, skoler eller SFO.

Skole- og barnehageeier skal påse at virksomheten har etablert et system for best mulig å forebygge sykdom og har ansvar for at de ansatte gis relevant og tilstrekkelig opplæring i dette. Leder i skole og barnehage er ansvarlig for at elever og barn vernes mot eventuelle helseskader og iverksetter de tiltak som er nødvendig (forskrift om miljørettet helsevern i barnehager og skoler). Stenging på grunn av sykdom blant personalet bør søkes unngått gjennom planlegging av gode vikarordninger.

En alvorlig pandemi er én av de største utfordringene for samfunnssikkerheten.

Kunnskapsdepartementet forutsetter at alle underliggende virksomheter og kommunene gjennomgår og oppdaterer pandemiplanene med jevne mellomrom, slik at man er forberedt dersom et pandemiutbrudd skulle inntreffe. Kunnskapsdepartementets pandemiplan

[9] Nasjonal beredskapsplan for pandemisk influensa, Helse- og omsorgsdepartementet 2006

7.6 Nasjonalt beredskapssystem og terror

Det er utarbeidet et sikkerhetsgradert Sivilt beredskapssystem (SBS), som sammen med Beredskapssystem for Forsvaret (BFF) utgjør Nasjonalt beredskapssystem (NBS). Kunnskapsdepartementet er en del av NBS og har med bakgrunn i SBS utarbeidet Kunnskapsdepartementets beredskapsplan (KDBP). Denne inneholder en rekke tiltak knyttet til sektorovergripende kriser i fredstid forårsaket av alvorlige tilsiktede hendelser, væpnet konflikt, eller trusler om slike og sikkerhetspolitiske kriser. Planverket inneholder tiltak som omfatter Meteorologisk institutt, UiO og UNINETT. De fleste av Kunnskapsdepartementets underliggende virksomheter berøres av dette planverket på en eller annen måte og skal utarbeide tiltak blant annet innen egenbeskyttelse etter nærmere føringer fra departementet.

Alle virksomheter har et ansvar for å sikre egen aktivitet mot terrorhandlinger. Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Politidirektoratet (POD) har i den forbindelse utgitt en veileder for offentlige og private virksomheter Terrorsikring: Veileder i sikkerhets- og beredskapstiltak mot tilsiktede uønskede handlinger

Formålet med veilederen er å gi virksomhetene et hjelpemiddel til å utarbeide tidsbegrensede sikkerhetstiltak for å møte en terrortrussel. Behovet for å iverksette slike tiltak kan oppstå ved endringer i risikobildet knyttet til mulige terrorhandlinger – herunder endringer i trusselsituasjonen, verdisituasjonen eller sårbarheten. Tiltakene er ment å håndtere *ekstraordinære situasjoner* som går utover hva som kan håndteres gjennom virksomhetens ordinære sikkerhetsopplegg.

Det er stor variasjon når det gjelder de ulike virksomhetenes sikkerhetsbehov, noen er mer utsatte enn andre avhengig av virksomhetens formål, driftsform og lokalisering. Derfor vil også anbefalte sikkerhetstiltak variere.

Regjeringen har utarbeidet en nasjonal veileder for forebygging av ekstremisme og voldelig radikalisering og en handlingsplan mot radikalisering og voldelig ekstremisme. Målet er å fange opp personer i risikosonen så tidlig som mulig og møte dem med tiltak som virker. Flere sektorer bidrar i oppfølgingen av tiltakene. Kunnskapsdepartementet har særlig ansvar for tiltak knyttet til forebygging av hatretorikk og for å øke kunnskapen om hvordan vi kan motvirke uønskede opplevelser på internett.

8. Informasjonssikkerhet

De store teknologiske endringene gir oss noen utfordringer. Vi ser at sentrale tjenester for samfunnet, som for eksempel betaling og telefoni, utfordres av internasjonale aktører som leverer tjenester i Norge uten at norske myndigheter har rettslig kontrollmulighet over dem. Dessuten er vår evne til å holde informasjon konfidensiell utfordret, og dermed også personvernet. I tillegg utsettes mange virksomheter for reelle trusler knyttet til at det utstyret de bruker kan angripes, og som et resultat bli delvis styrt av uvedkommende. Det foreligger således et betydelig teknologisk press som kan utfordre sentrale samfunnsverdier.[10]

Informasjonssikkerhet er en integrert del av arbeidet med samfunnssikkerhet og beredskap. De digitale tjenestene er blitt kritiske for at samfunnet skal fungere som normalt. Kunnskapsdepartementet forventer at arbeidet med informasjonssikkerhet gis høy prioritet i kunnskapssektoren. Med informasjonssikkerhet menes her beskyttelse mot brudd på *konfidensialitet , integritet eller tilgjengelighet*[11] av den informasjonen som blir behandlet i et system, samt beskyttelse av informasjonssystemer og nett i seg selv. Utvalget som har sett på digital sårbarhet trekker også frem *sporbarhet* som et fjerde sikkerhetsmål.[12]

Nasjonal strategi for informasjonssikkerhet[13], Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017 og andre føringer gitt av Justis- og beredskapsdepartementet, Kommunal- og regionaldepartementet, og Nasjonal sikkerhetsmyndighet utgjør et viktig grunnlag for Kunnskapsdepartementets arbeid med informasjonssikkerhet.

Krav til informasjonssikkerhet er en integrert del av flere lover og forskrifter, som for eksempel personopplysningsloven med forskrifter, esignaturloven med forskrifter, lov om elektronisk kommunikasjon (ekomloven) med forskrifter, e-forvaltningsloven, forvaltningsloven, offentlighetsloven med forskrifter og sikkerhetsloven med forskrifter.

Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier, og handler ikke bare om tekniske løsninger, men like mye om fordeling av ansvar, oppfølging av rutiner og planverk og bevisstgjøring av den enkelte bruker.

Informasjonssikkerhet er ikke minst viktig i forhold til elektronisk kommunikasjon med andre virksomheter og publikum. Tap av informasjon og bortfall av IKT-tjenester kan få store konsekvenser for en virksomhet, en sektor eller for samfunnet som helhet. Det er derfor svært viktig at risiko og sårbarhet forebygges kontinuerlig.

Også innenfor informasjonssikkerhet gjelder de fire grunnleggende beredskapsprinsippene: ansvars-, nærhets-, likhets- og samvirkeprinsippet. Det er følgelig den enkelte virksomhet ved ledelsen som har ansvaret for å etablere og opprettholde tilfredsstillende informasjonssikkerhet. Iverksetting og oppfølging av tiltak skal inngå som en integrert del av den interne styringen i enhver virksomhet. Departementet har et overordnet ansvar for å ivareta sikring av sektorens IKT-infrastruktur, og at det forebyggende arbeidet med informasjonssikkerhet i sektoren er tilfredsstillende.

I 2015 kom en egen Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017 (KMD). Denne, og tiltaksområdene den beskriver, er det viktig at virksomhetene i sektoren følger opp. Tiltaksområdene er innenfor styring og kontroll, sikkerhet i digitale tjenester, digital beredskap, sikkerhet i nasjonale felleskomponenter, kunnskap, kompetanse og kultur. I tillegg til de fire grunnleggende prinsippene i den nasjonale beredskapstilnærmingen, bygger arbeidet med informasjonssikkerhet i statsforvaltningen på forutsetningene risikostyring og innebygget informasjonssikkerhet. Risikostyring er kjernen i arbeidet med informasjonssikkerhet. Virksomhetene i statsforvaltningen skal ha god risikoforståelse og arbeide systematisk med risikovurderinger. Risikostyring skal gjøre virksomhetene i stand til å ta informerte valg og gjøre prioriteringer ved innføring av sikkerhetstiltak. Innebygd informasjonssikkerhet innebærer at informasjonssikkerhet skal være en del av ethvert digitaliseringsprosjekt i statsforvaltningen fra starten, og i hele systemets livssyklus. Informasjonssikkerhet skal også være en naturlig del av virksomhetsstyringen, og et tema som alle ansatte i statsforvaltningen – ut fra sin rolle – skal ha et kjennskap til.

De vanligste dataangrepene fra Internett skjer via e-poster og nettsider. En del angrep kommer også fra infiserte USB-minnepinner. NSM har utarbeidet dokumen-

[10] NOU 2015:13 Digital sårbarhet – sikkert samfunn, kap. 1, s.15.
[11] FAD, Justis- og beredskapsdepartementet, FD og SD. (2012). Nasjonal strategi for informasjonssikkerhet. Oslo:FAD
[12] NOU 2015:13. Digital sårbarhet – sikkert samfunn, kap 5. s. 35.
[13] Vedtatt av regjeringen i 2012.

tet Ti viktige tiltak mot dataangrep hvor de fire første vil stoppe 80-90 prosent av alle kjente dataangrep. Departementet forutsetter at virksomhetene gjennomgår og oppdaterer sine rutiner i henhold til disse tiltakene.

Det vises også til Nasjonal sikkerhetsmyndighets rapport Helhetlig IKT-risikobilde 2015. Rapporten tar for seg de viktigste risikoene knyttet opp mot bruk av IKT i det norske samfunnet.

8.1 Styringssystem for informasjonssikkerhet

Kunnskapsdepartementet stiller krav til at underliggende virksomheter skal ha et helhetlig styringssystem for informasjonssikkerhet (ISMS/SSIS), også kalt ledelsessystem. Styringssystemet består av alle aktiviteter en virksomhet samlet gjør av planlagte og systematiske tiltak for styring, kontroll og oppfølging av informasjonssikkerhet og skal i staten være basert på anerkjente standarder som ISO 27001:2013 (iht. Difis referansekatalog). Styringssystem for informasjonssikkerhet bør være en integrert del av virksomhetenes helhetlige styringssystem, internkontroll, kvalitetssystem eller tilsvarende betegnelse på samlet og helhetlig intern kontroll.

Departementet viser til UNINETTs veiledning til styringssystem for informasjonssikkerhet i UH-sektoren.

Difi har utarbeidet et praktisk rettet veiledningsmateriell for internkontroll av informasjonssikkerhet. Veiledningen er basert på anerkjente standarder for styringssystemer for informasjonssikkerhet, og skal gi lederne og fagansvarlige i forvaltningen bedre styring og kontroll med informasjonssikkerheten. Begrepet internkontroll brukes her i stedet for betegnelsen styringssystem, men dette refererer til det samme.

8.2 Skytjenester

Skytjenester blir en stadig viktigere del av vår IKT-hverdag, både privat og i jobbsammenheng. Skytjenester er en felles betegnelse på alt fra dataprosessering og datalagring, til programvare som er tilgjengelige fra eksterne serverparker tilknyttet internett.

Utvalget som har sett på digital sårbarhet mener de vurderingene en må gjøre når det gjelder sikkerhet ved bruk av skytjenester, ligner vurderingene en må gjøre om en skal sette ut andre tjenester til eksterne leverandører. I praksis betyr dette å forholde seg til de formelle avtalene med leverandøren om hvordan data vil bli lagret eller behandlet. Når skytjenestene åpner for lagring og behandling av data i utlandet, reiser det seg imidlertid særlige juridiske problemstillinger knyttet til at tjenestene ikke reguleres av norske lover.

Utvalget påpeker at risikoen ved å bruke skytjenester vil variere avhengig av hvor sensitive data en skal lagre eller behandle, og hvordan skytenesteleverandøren har implementert sine spesifikke skytjenester. Hvor omfattende vurderinger av leverandøren må være, vil avhenge av verdien av den informasjonen det er snakk om, og hvor alvorlige konsekvensene kan bli dersom noe går galt.

Det vil antagelig ofte være slik at en bedrift eller virksomhet vil kunne legge noe av sin informasjon ut i skyen, mens annen informasjon beholdes lokalt/internt. Det kan finnes opplysningstyper som av konkurransehensyn eller sensitivitetshensyn ikke bør legges i en skytjeneste, selv om det er lovlig å legge dem der[14]

[14] NOU 2015:13 Digital sårbarhet – sikkert samfunn, kp. 23, s. 306.

9. Kritisk infrastruktur og kritiske samfunnsfunksjoner

Departementet skal gjøre vurderinger av hva som er kritiske og viktige samfunnsfunksjoner innenfor sektoransvaret. Kritiske samfunnsfunksjoner er definert gjennom Meld. St. 21 (2012–2013) Terrorberedskap og Prop. 1 S (2013–2014).

Funksjonene er utledet av DSBs rapport *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner. Modell for overordnet risikostyring* (KIKS) (2012). KIKS-modellen skal sikre at oppfølgingen av sikkerheten i kritiske samfunnsfunksjoner blir ivaretatt, gjennom blant annet å tydeliggjøre hva som inngår i begrepene *kritisk infrastruktur og kritiske samfunnsfunksjoner* og å etablere en overbygning for den sektorvise risikostyringen av disse.

Kritisk infrastruktur[15] defineres her som de anlegg og systemer som er helt nødvendige for å opprettholde samfunnskristiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse. *Kritisk samfunnsfunksjon* er knyttet opp mot samfunnets grunnleggende behov som er definert som trygghet for den enkelte og basale fysiske behov som vann, mat, varme og lignende.

Begrepet **basiskapabilitet** brukes om den funksjonsevnen det norske samfunnet må planlegge å opprettholde, nærmest uansett hvilke påkjenninger det utsettes for. **Basisleveranser** er en konkretisering av hvilke vare- og tjenestetyper som vil være nødvendig for å opprettholde samfunnets grunnleggende funksjonsevne. Begrepet **innsatsfaktor** brukes om leveransene virksomhetene er avhengig av for å kunne produsere og levere slik at samfunnets og befolkningens behov kan ivaretas. Innsatsfaktorene er i prinsippet erstattbare eller dublerbare.

Det enkelte departement skal i samarbeid med underliggende virksomheter, ved hjelp av blant annet KIKS-modellen, identifisere kritisk infrastruktur i egen sektor og følge opp nødvendig tiltak, og koordinering med andre departement.

[15] Alle begreper og definisjoner under punkt 9.er hentet fra DSBs rapport sikkerhet i Kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring. KIKS-prosjektet 1. delrapport. 2012.

Innenfor Kunnskapsdepartementets ansvarsområde finnes det aktører og virksomheter innen IKT-området som faller inn under kategorien kritisk infrastruktur. Departementet følger opp disse spesielt, bl.a. i forbindelse med forskrift om objektsikkerhet av 01.01.11.

9.1 Installasjoner omfattet av ekomloven

NIX (Norwegian Internett eXchange) er viktige samtrafikkpunkter for norsk internettrafikk. Dette er knutepunkter hvor også private aktører som Telenor og andre internettilbydere er påkoblet. Hensikten med disse NIX-ene er å koble sammen deler av internettet i Norge. Disse samtrafikkpunktene eies av UNINETT, men driftes av USIT ved Universitetet i Oslo. UNINETT har ansvaret for NIX-ene og er ansvarlig for disse ved tilsyn fra Nasjonal kommunikasjonsmyndighet. Dette følges opp av Kunnskapsdepartementet gjennom den løpende dialogen om de tjenestene som UNINETT leverer til UH-sektoren. Universitetet i Oslo vurderer NIX som viktig, men ikke kritisk for Internett i Norge.

Selv om NIX ikke vurderes til å være et skjermingsverdig objekt etter forskrift om objektsikkerhet, er ekomtjenester likefullt en kritisk allmenn innsatsfaktor iht. KIKS-modellen. NIX vurderes derfor til å være en kritisk infrastruktur.

UNINETT Norid AS, som er et datterselskap av UNINETT AS, driver .no-domenet og vedlikeholder den sentrale databasen for alle norske domenenavn. De har ansvaret for utvikling av regelverket for .no etter brukernes ønsker og innenfor rammene av den norske domeneforskriften. UNINETT Norid har Nasjonal kommunikasjonsmyndighet (Nkom) som tilsynsorgan. Samferdselsdepartementet og Nkom følger opp UNINETT Norid hva gjelder objektforskriftens krav om utvelgelse og klassifisering av eventuelle skjermingsverdige objekter.

Tilgjengeligheten til .no-domenet går inn under ekomtjenestene som kritisk allmenn innsatsfaktor og navnetjenesten vurderes derfor som en kritisk infrastruktur på samme måte som NIX.

Ansvarsforhold

Det er Nasjonal kommunikasjonsmyndighet (Nkom) som har ansvar for oppfølging av Norid og NIX, og fører tilsyn med disse. Kunnskapsdepartementet har imidlertid et ansvar som eier for å følge opp avvik og pålegg fra Nkom som krever tiltak fra eier.

9.2 Forskningsnettet

UNINETT AS, som eies av Kunnskapsdepartementet, utvikler og driver det norske forskningsnettet, som forbinder mer enn 200 norske utdannings- og forskningsinstitusjoner og over 300 000 brukere, og knytter dem opp mot internasjonale forskningsnett.

Meteorologisk institutt er avhengig av forskningsnettet for å drifte dataløsningene og er også avhengig av tungregningskapasiteten som er koblet opp i forskningsnettet. Dette gjelder også en rekke andre viktige tjenesteleverandører i universitets- og høyskolesektoren der i blant Statens strålevern og Folkehelseinstituttet. Forskningsnettet er iht. KIKS-modellen en kritisk infrastruktur for å opprettholde basiskapabiliteten *«evnen til å betjene virksomheter med kritisk samfunnsfunksjon og befolkningen med nødvendig meteorologisk informasjon»* og flere andre basiskapabiliteter gjennom leveransene fra universitets- og høyskolesektoren.

9.3 Meteorologisk institutt

DSB har i KIKS-prosjektet definert *«meteorologiske tjenester»* som en kritisk allmenn innsatsfaktor og *«evnen til å betjene virksomheter med kritisk samfunnsfunksjon og befolkningen med nødvendig meteorologisk informasjon»* som en basiskapabilitet.

For å kunne ivareta basiskapabiliteten, har DSB definert følgende fire fundamentale kapabiliteter:

a. Evne til å samle inn, behandle og tilgjengeliggjøre meteorologiske data.
b. Evne til å utarbeide og distribuere varsler av betydning for liv og sikkerhet.
c. Evne til å ivareta behov for spesielle meteorologiske beregninger og tjenester i forbindelse med søk- og redningsoperasjoner, kritiske operasjoner og sikkerhetstruende hendelser.
d. Evne til å levere tilstrekkelig flymeteorologisk informasjon av god kvalitet, slik at sivil og militær luftfart kan opprettholdes.

Meteorologisk institutt gjennomfører jevnlige ROS-vurderinger av infrastrukturen for å avdekke sårbarheter og iverksette risikoreduserende tiltak. Deler av infrastrukturen er omfattet av Sikkerhetslovens forskrift om objektsikkerhet og således undergitt særskilte sikkerhetskrav.

9.4 Krav til oppfølging fra virksomheter som ivaretar kritisk infrastruktur

Alle virksomheter som ivaretar samfunnskritisk IKT-infrastruktur har et spesielt ansvar for beskyttelsestiltak som sikrer opprettholdelse av drift og basisleveranser. Det må vektlegges tiltak for å sikre robusthet og rask gjenoppretting etter brudd.

Virksomheter som ivaretar kritisk IKT-infrastruktur har et særlig ansvar for å gjennomføre regelmessige risiko- og sårbarhetsanalyser, jf. kapittel 6. Gjennomføringen av analysen må inngå i et fastlagt styringssystem for risikohåndtering i virksomheten og må være forankret hos ledelsen.

10. Nyttige lenker

Nedenfor følger en liste over aktuelle offentlige virksomheter med oppgaver eller tilbud innenfor samfunnssikkerhet og beredskap. Listen er ikke uttømmende.

- Veiledning i beredskapsplanlegging utarbeidet av Utdanningsdirektoratet og Politidirektoratet
- Justis- og beredskapsdepartementet (generelt om samfunnssikkerhet)
- Direktoratet for samfunnssikkerhet og beredskap (DSB) - publikasjoner, rapporter, veiledere
- Nasjonalt risikobilde (DSB)
- Delrapport om skoleskyting i Nordland - Nasjonal risikobilde 2015
- Helsedirektoratet - publikasjoner, rapporter, veiledere
- Veileder til forskrift om miljorettet helsevern i barnehager og skoler
- Nasjonal sikkerhetsmyndighet (NSM) - publikasjoner, veiledere, kurs og konferanser
- Statens strålevern - fagmyndighet innen strålevern og atomsikkerhet
- Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap (NUSB) - kurs og utdanningstilbud bl.a. innenfor ROS-analyse og krisekommunikasjon
- Norsk Senter for Informasjonssikring (NorSIS) - veiledere, seminarer/konferanser om internkontroll og informasjonssikkerhet
- Kommunal informasjonssikkerhet (KINS) - seminarer/konferanser om informasjonssikkerhet
- Datatilsynet - veiledere om internkontroll og informasjonssikkerhet
- Direktoratet for forvaltning og IKT (Difi) - veiledere om informasjonssikkerhet
- Norsk brannvernforening (uavhengig stiftelse) - informasjon, opplæring og rådgivning

Veiledning i risiko- og sårbarhetsanalyse

Vedlegg til Styringsdokument for arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren

1. Innledning

Målet for risiko og sårbarhetsanalysen (ROS-analysen) er å etablere en oppdatert oversikt over risiko, et risikobilde av eget ansvarsområde, vurdere virksomhetens sårbarhet og foreslå hvordan risiko og sårbarhet bør håndteres gjennom eventuelle nye risikoreduserende tiltak. Hensikten er å bidra til tilfredsstillende sikkerhet for virksomheten og dens brukere gjennom målrettet forebygging og beredskap. ROS-analysen skal ligge til grunn for kriseplanverket og valg av øvelsesscenarioer.

En ROS-analyse kan utføres på ulike måter. ROS-analysen gir ikke fasitsvar for hva som vil skje i framtiden, men skal gi grunnlag for gode vurderinger og beslutninger i dag. Kunnskapsdepartementet har inntrykk av at det er noe usikkerhet mht. hvordan den enkelte virksomhet kan lage en god og hensiktsmessig ROS-analyse. Dette vedlegget til Styringsdokumentet er tenkt som en hjelp i arbeidet.

I instruksen om departementenes arbeid med samfunnssikkerhet (forskrift 15. juni 2012 nr. 535), stilles det krav til at departementene skal ha *oversikt* over risiko og sårbarhet i egen sektor. Dette forutsetter etter Kunnskapsdepartementets syn at virksomhetene i sektoren må klargjøre hvilket ansvar de har overfor sine brukere for å kunne vurdere om samfunnssikkerheten er tilstrekkelig ivaretatt. Instruksen forutsetter bl.a. at departementene legger Nasjonalt risikobilde (NRB) utarbeidet av Direktoratet for samfunnssikkerhet og beredskap (DSB) til grunn for sine ROS-analyser.

Kunnskapsdepartementet anbefaler derfor at virksomhetene tar utgangspunkt i NRB i sine ROS-analyser. NRB omhandler katastrofer som store naturhendelser, ulykker og tilsiktede hendelser som rammer samfunnet som helhet, og som derfor også vil kunne ramme virksomheter i kunnskapssektoren. Kunnskapsdepartementet anbefaler også at man ser på mer lokale og virksomhetsspesifikke hendelser som kan ramme virksomheten. Se for øvrig delmålene for ROS-analysen under. Det viktige er at man gjør bevisste og begrunnede valg av hvilke hendelser man velger å analysere eller å utelate.

2. Mål

Få oversikt over risiko og sårbarhet innenfor eget ansvarsområde. Dette krever en kartlegging både av hva og hvem man har ansvar for, og av hvilken risiko og sårbarhet som eksisterer.

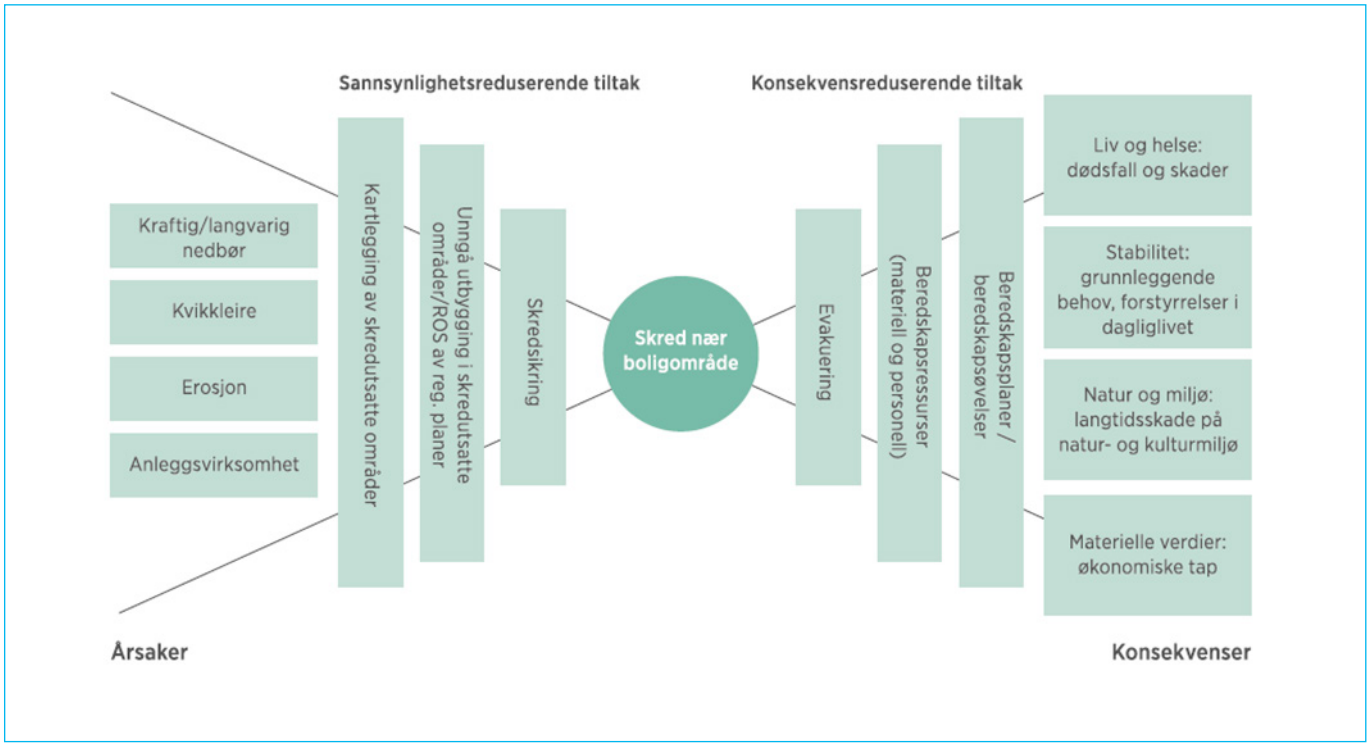
3. Spørsmål som skal besvares i ROS-analysen

ROS-analysen skal gi svar på:

- Hvilke verdier ønsker vi å beskytte? (konsekvensområder)
- Hvilke farer og trusler står vi overfor - hva kan gå galt? (uønskede hendelser)
- Hvorfor og hvordan kan det gå galt? (årsaker til hendelsene, hendelseskjeder)
- Hvilke hendelser er mest alvorlige for oss? (risikovurdering)
- Hva har vi gjort og hva kan vi gjøre for å forhindre at uønskede endelser inntreffer? ? (forebyggende tiltak)
- Hva har vi gjort og hva kan vi gjøre for å begrense konsekvensene dersom hendelsen likevel inntreffer? (skadebegrensende tiltak)

I midten av figuren under er en uønsket hendelse. Til venstre for denne vises mulige årsaker som kan føre til at den uønskede hendelsen inntreffer. Her er det også listet tiltak for å hindre at den uønskede hendelsen inntreffer (sannsynlighetsreduserende tiltak). Til høyre for den uønskede hendelsen vises mulige konsekvenser for ulike verdier som liv og helse, stabilitet, miljø og materielle verdier. Her finner vi også tiltak for å redusere konsekvensene (konsekvensreduserende tiltak).

Figur 3.1 Modell for ROS-analyse



Eksempel på et sløyfediagram med utgangspunkt i den uønskede hendelsen "skred nær boligområde". (Fra DSBs Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen s 16).

4. Organisering og avgrensning

Arbeidet med ROS-analysen bør organiseres slik at kartleggingen av hendelser dekker hele bredden i virksomheten. Dette vil sikre at flest mulig relevante hendelser fanges opp. ROS-analysen er rettet mot samfunnssikkerhet og beredskap (SoB) dvs hendelser med konsekvenser for brukerne/befolkningen. I kartleggingsfasen kan det komme opp uønskede hendelser som faller innunder kategorien HMS-hendelser og hendelser relatert til mål- og resultatstyring. Disse bør holdes utenfor denne analysen og kan dekkes i egne risikoanalyser.

I noen tilfeller kan det være vanskelig å trekke et skarpt skille mellom en uønsket hendelse i samfunnssikkerhets- og beredskapsmessig forstand og en HMS-hendelse, men en tommelfingerregel kan være at en hendelse i samfunnssikkerhets- og beredskapsmessig forstand kan utgjøre en krise for virksomheten og medføre nedsettelse av krisestab og aktivisering av tiltak i beredskapsplanverk. En HMS-hendelse kan derfor i verste fall også utgjøre en hendelse i samfunnssikkerhets- og beredskapsmessig forstand.

For mindre virksomheter omfattet av forskrift om miljørettet helsevern i barnehager og skoler, kan det være mer naturlig at HMS-hendelser inkluderes i analysen.

5. Sentrale begreper

Uønsket hendelse: En situasjon som inntreffer og som antas å kunne true en organisasjons samfunnsverdier og å kunne eskalere til en krise. Hendelsene kan være naturskapte, skyldes teknisk eller menneskelig svikt eller være tilsiktede handlinger.

Risiko: Uttrykker den fare uønskede hendelser representerer for mennesker liv og helse og andre verdier som er sentrale for samfunnet som helhet eller for virksomheten. Risiko er et uttrykk for sannsynlighet for- og konsekvensene av en uønsket hendelse.

Sårbarhet/robusthet: Uttrykker virksomhetens evne til å fortsette å fungere som tiltenkt når den utsettes for ekstraordinære påkjenninger.

Krise: En situasjon som truer eller kan true en organisasjons samfunnsverdier og som krever en annen måte å organisere arbeidet på enn ved en normalsituasjon.

Samfunnssikkerhet: Samfunnets evne til å opprettholde viktige samfunnsfunksjoner og ivareta liv og helse under ulike former for kritiske hendelser.

Forebygging: Redusere sannsynligheten for at en uønsket hendelse skal inntreffe.

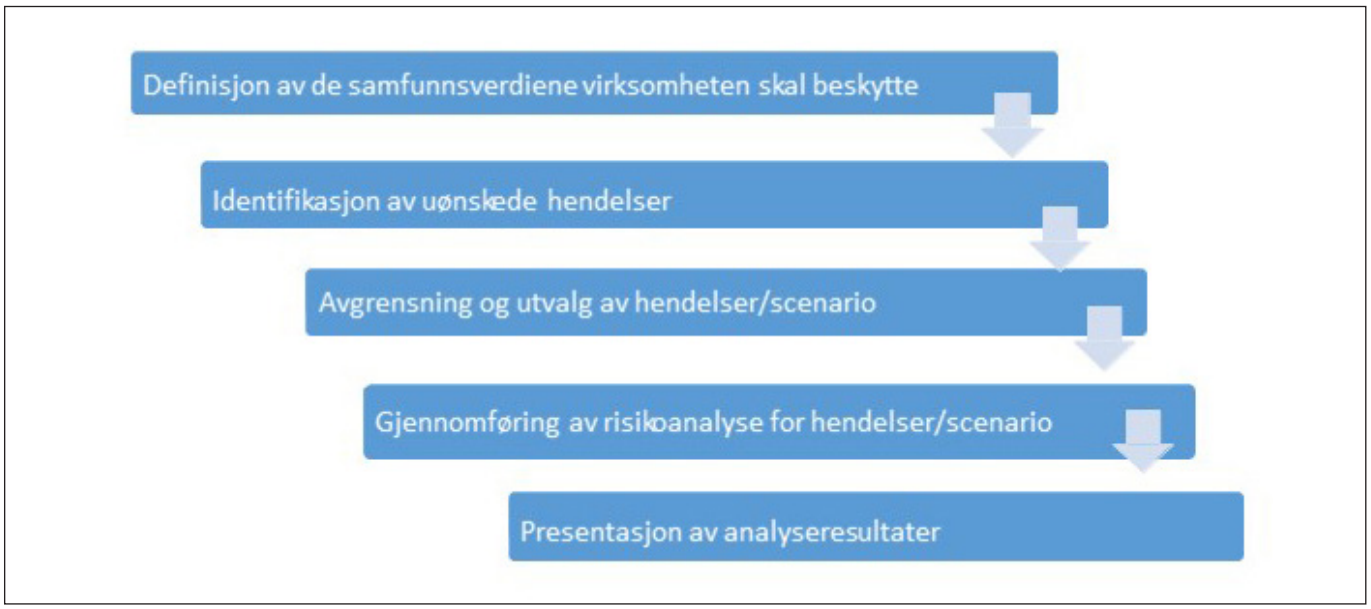
Beredskap: Etablerte tiltak som hindrer at en uønsket hendelse utvikler seg til en krise og får alvorlige konsekvenser.

Risikoreduserende tiltak: Samlebetegnelse for forebyggende og skadebegrensende tiltak for å redusere risiko og sårbarhet.

6. Framgangsmåte for ROS-analyser

Det fins ulike analytiske tilnærminger til ROS-analyser. Risikoanalysen er en systematisk fremgangsmåte som kan benytte både kvalitativ og kvantitativ kunnskap. Noen analyser er kvantitative og formelle, mens andre følger en enklere metodikk. I tillegg til eksisterende skriftlig kunnskap og historikk, foregår en viktig kunnskapsinnhenting og – bearbeiding i gruppeprosesser. Risiko knyttet til de uønskede hendelsene kan presenteres som tall, med ord eller skjematisk, f.eks på en skala fra svært lav til svært høy risiko. Man trenger ikke gjøre tallmessige beregninger dersom det ikke finnes statistisk grunnlag for det. Trinnene i risikoanalysen er de samme uavhengig av omfang og type data som benyttes.

Figur 6.1 Hovedtrinnene i en risikoanalyse (etter modell i dokumentet "Fremgangsmåte for risikoanalyser i Nasjonalt risikobilde" s. 16)



7. Konsekvensområder

Konsekvensområdene er de verdier som virksomheten ønsker å beskytte og verne om. Konsekvensområdene varierer følgelig med type virksomhet. Kunnskapsdepartementet definerer f.eks barn, elever studenter og ansatte som oppholder seg i barnehager og utdanningsinstitusjoner, som den viktigste verdien sektoren skal beskytte. De vanligste konsekvensområdene er:

- samfunnsviktige funksjoner/kritisk infrastruktur
- menneskers liv og helse,
- drift/produksjon/tjenesteyting,
- økonomi/ materielle verdier,
- troverdighet/renommé/omdømme
- miljø

8. Vurdering av konsekvenser og sannsynlighet

Aksept handler om hvilken risiko man er villig til å leve med. Akseptkriterier har å gjøre med hvordan man vurderer **konsekvens** og **sannsynlighet**. Dette kan det være vanskelig å sette klare kriterier for, og konsekvenskriterier og sannsynlighetskriterier kan være til hjelp i vurderingene. **Konsekvenser** kan graderes fra ufarlige til katastrofale, eller fra små til store.

Tabell 8.1 Eksempel på gradering av ulike konsekvenstyper (fra Kunnskapsdepartementets egen ROS-analyse)

Konsekvens-kategorier	Konsekvenstyper (verdier)			
	A. Menneskers liv og helse	**B. Drift, produksjon og tjenesteyting**	**C. Økonomi og materielle verdier**	**D. Troverdighet, renommé og omdømme**
1. Ufarlig	Ingen fysiske eller psykiske skader	Ingen stans	Ingen økonomisk skade	Ingen skade
2. En viss fare	Få eller små fysiske og psykiske skader	Stans i mindre enn 24 timer	Mindre økonomisk tap som kan gjenopprettes	Ubetydelig skade
3. Farlig	Alvorlig fysisk eller psykisk skade	Stans i 1-2 døgn	Betydelig økonomisk tap som kan gjenopprettes	Tap av troverdighet/ renommé/ omdømme
4. Kritisk	1 dødsfall og/eller flere alvorlig fysisk skadet	Stans i 2-7 døgn	Uopprettelig økonomisk tap	Alvorlig tap av troverdighet/ renommé/omdømme
5. Katastrofalt	Flere døde	Stans i mer enn 1 uke	Betydelig og uopprettelig økonomisk tap	Uopprettelig tap av troverdighet/renommé/ omdømme

9. Sannsynlighets-intervaller

En av oppgavene i forbindelse med ROS-analyser er å definere intervaller eller kategorier for sannsynlighet for at hendelser skal inntreffe. Med sannsynlighet menes hvor trolig det er at hendelsen vil inntreffe, gitt den bakgrunnskunnskapen analysegruppa har. Tidsintervall er ofte et godt utgangspunkt for vurdering av sannsynlighet. Tabellen under gir et eksempel på dette. Når det gjelder vurdering av sannsynlighet for tilsiktede hendelser, så brukes oftere en kortere tidshorisont enn for andre typer hendelser. Tidshorisont i PSTs årlige åpne trusselvurderinger er for eksempel ett år. Derfor kan det være vanskelig å sammenlikne sannsynlighet for tilsiktede og utilsiktede hendelser. For en type tilsiktede hendelser som for eksempel terror eller skoleskyting er det likevel mulig å si noe om sannsynlighet på lengre sikt.

Det er verdt å merke seg at NRB vurderer sannsynlighet for hendelser ut fra et nasjonalt perspektiv. Dersom en virksomhet tar utgangspunkt i hendelsene i NRB i sin ROS-analyse, må virksomheten tilpasse sannsynlighets- og konsekvenskategoriene til egen virksomhet.

Tabell 9.1 Eksempel på sannsynlighetskriterier for en ROS-analyse.

Begrep	Definisjon
Lite sannsynlig	Sjeldnere enn en gang hvert 10. år.
Mindre sannsynlig	Mellom en gang hvert 5. år og en gang hvert 10. år.
Sannsynlig	Mellom en gang hvert år og en gang hvert 5. år.
Meget sannsynlig	Mellom en gang i måneden og en gang i året.
Svært sannsynlig	En gang i måneden eller oftere.

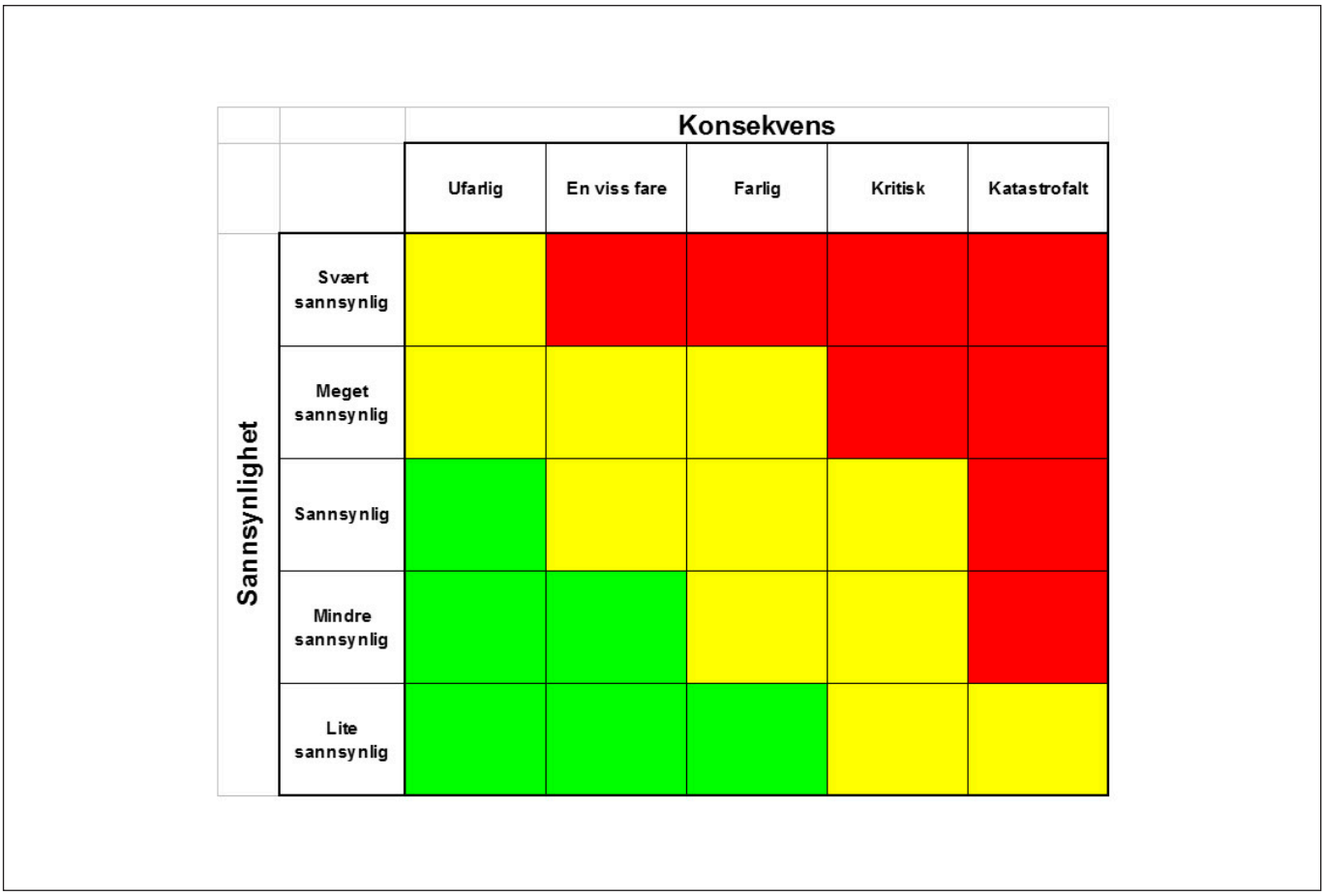
10. Risikovurdering

Risiko ved en hendelse kan framstilles gjennom en sammenstilling av sannsynlighet og konsekvens. Risikovurderingen uttrykker hvilken fare den uønskede hendelsen representerer for verdiene i virksomheten. Risiko kan framstilles i en risikomatrise som den nedenfor. Identifiserte hendelser plasseres inn i matrisen, slik at forskjellen i risiko mellom hendelsene synliggjøres.

Nivåer i risiko:

- **Høy (rød)**
  Risikoreduserende tiltak skal/må iverksettes umiddelbart
- **Middels (gul)**
  Risikoreduserende tiltak skal/må vurderes
- **Lav (grønn)**
  Det er ikke nødvendig å iverksette risikoreduserende tiltak så fremt kravene i lov og forskrifter er oppfylt

Figur 10.1 Risikovurdering



11. Oppfølging og handlingsplan

Det er viktig at risikovurderingen følges opp med en handlingsplan for risikoreduserende tiltak. Hendelser som er vurdert til å ha høy eller middels risiko må følges opp. Handlingsplanen må inneholde vurdering av aktuelle tiltak og ansvarsforhold og tidsfrister for iverksetting av tiltak. Handlingsplanen må forankres hos virksomhetens ledelse.

12. Oppsummering

Som nevnt innledningsvis kan en ROS-analyse utføres på ulike måter. Det finnes ingen fastlagt metodikk som passer for alle virksomheter. Denne veiledningen kan være til hjelp i arbeidet med ROS-analysen, men den enkelte virksomhet må tilpasse metodikken og analysen til egen situasjon og egenart, og hva som er hensiktsmessig sett i lys av risiko og vesentlighet.

Utgitt av:
Kunnskapsdepartementet

Publikasjonskode: F-4428 B