Oslo kommune
Beredskapsetaten

DEL 1 RISIKO- OG SÅRBARHETSANALYSE

Veileder i helhetlig og systematisk arbeid med samfunnssikkerhet og beredskap

Innholdsfortegnelse

Begrep

Begrep	Forklaring
ALARP-prinsippet	As Low As Reasonably Practicable, vil si at risiko som oppstår etter tiltak, skal være så lav som praktisk mulig.
Befolkning	Med befolkning menes de som til enhver tid bor og oppholder seg i kommunen.
Beredskap	Med beredskap forstås tiltak for å forebygge, begrense eller håndtere kriser og andre uønskede hendelser (NOU 2000:24 "Et sårbart samfunn").
Beredskapshendelse	En hendelse som avviker fra det normale i så stor grad at beredskapsressurser må benyttes.
Kritiske samfunnsfunksjon	Kritiske samfunnsfunksjoner er tjenester som samfunnet må opprettholde til enhver tid for å ivareta befolkningens sikkerhet og trygghet. Dette er leveranser som dekker befolkningens grunnleggende behov. Mat, vann, varme og helsetjenester er eksempel på slike behov. Disse tjenestene må være robuste mot mange ulike typer hendelser. Svikt i kritiske samfunnsfunksjoner kan forsterke konsekvensene av en hendelse, og skape følgehendelser som igjen får nye konsekvenser.
Konsekvenser	Konsekvenser uttrykker vi i form av tap av samfunnsverdier. Samfunnsverdier er uttrykk for de verdiene vi ønsker å beskytte, f.eks. liv og helse, natur- og kulturverdier, materielle verdier.
Risiko	Risiko kombinerer sannsynlighet og konsekvens etter en hendelse som kan ha verdier for oss mennesker. Verdiene kan være liv og helse, miljø eller andre økonomiske verdier.
Risikoeier	En risikoeier er ansvarlig for å identifisere, vurdere og håndtere – risikoer innen eget ansvarsområde. De er ansvarlig for utføring av arbeidet og de mål som skal nås.
Risikoområde	Risikoområde betegner et felles område som gir utspring til ulike risikoer. Eksempelvis kan det innen ekom være risikoer for data-, telefon-, radio- og satellitt-trafikk, eller mer spesifikke risikoer innunder funksjonaliteter.
Sannsynlighet	Sannsynlighet brukes som mål på hvor trolig vi mener det er at en bestemt hendelse vil inntreffe, gitt vår bakgrunnskunnskap. Sannsynlighet kan angis på ulike måter. Ofte bruker vi å angi den som en prosentstørrelse innenfor et tidsrom, f.eks. 1% sannsynlighet for at hendelsen skal inntreffe i løpet av et år.
Samfunnssikkerhet	Samfunnssikkerhet handler om samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare (St.meld.nr. 5 (2020-2021).
Samfunnsverdier	Samfunnsverdier er uttrykk for de verdiene vi ønsker å beskytte, i Kommunalt risikobilde benyttes samfunnsverdiene liv og helse, natur og miljø, økonomi, samfunnsstabilitet og styringsevne og kontroll.
Statusrapport	En rapport som gir et samlet bilde av konsekvensene hendelsen har for virksomheten, hvilke tiltak som er iverksatt, etablert kriseledelse,

	krisekommunikasjon og tiltak som vurderes iverksatt. Rapporten oppdateres jevnlig og distribueres.
Styrbarhet	Styrbarhet benyttes for å beskrive virksomhetens evne til å kontrollerer forutsetninger for og i hendelsen som kan minimere eller avverge konsekvenser.
Sårbarhet	Sårbarhet er et uttrykk for et systems manglende evne til å motstå en uønsket hendelse samt manglende evne til å gjenoppta sin funksjon etter at en hendelse har inntruffet. Sårbarhet er knyttet til mulig tap av samfunnsverdier. Et system kan i denne sammenheng for eksempel være en virksomhet, et tjenesteområde, en tjeneste leveranse eller en digital tjeneste. Det motsatt av sårbarhet er **robusthet**.
Tjenestested	Tjenestested kan være skoler, barnehager, omsorgshjem som ligger under en virksomhet i Oslo kommune, eller som Oslo kommune har ansvar for.
Uønsket hendelse	Hendelser som avviker fra det normale, og som har medført eller kan medføre tap av liv eller skade på helse, miljø, materielle verdier og kritisk infrastruktur (sivilbeskyttelsesloven § 3a).
Usikkerhet	Begrepet usikkerhet benyttes for å beskrive kvaliteten på bakgrunnskunnskapen vurderingene er basert på.
Virksomhet	Kommunal virksomhet eller virksomhet benyttes om alle organisatoriske enheter i kommunen. Byrådsavdelinger, etater, bydeler og kommunale foretak.

1 OM VEILEDEREN

Virksomhetene i Oslo kommune har en sentral rolle i arbeidet med samfunnssikkerhet og beredskap. Kommunens arbeid skal være helhetlig og systematisk, og lovverket understreker den viktige rollen kommunene har som samordner og pådriver på samfunnssikkerhetsområdet.

Grunnlaget for et godt samfunnssikkerhetsarbeid er kunnskap og bevissthet om de risikoer og sårbarheter vi står overfor. Risiko- og sårbarhetsanalysen (ROS-analysen) skal ikke være et mål i seg selv, men et virkemiddel i virksomhetenes arbeid med å redusere risiko for befolkningen og for å opprettholde nødvendig tjenesteproduksjon gjennom forebyggende tiltak, styrket beredskap og bedre evne til å håndtere hendelser.

Denne veilederen viser hvordan virksomhetene kan gjennomføre en ROS-analyse i henhold til beredskapsreglementet i Oslo kommune og kommunal beredskapsplikt. Målgruppen for denne veilederen er virksomheter, og tjenestesteder som er forskjellige med hensyn til størrelse, ressurser og kompetanse – også med hensyn til ulike risikobilder på samfunnssikkerhets-området. Med visse tilpasninger bør likevel veilederen kunne brukes av alle. Av praktiske hensyn bruker denne veilederen begrepet "virksomhet" om kommunale organer som denne veileder er relevant for. Begrepet "virksomhet" viser dermed både til etater, kommunale foretak og bydeler (nivå 1 – se delkapittel 1.3) og til underliggende tjenestesteder (nivå 0 – se delkapittel 1.3).

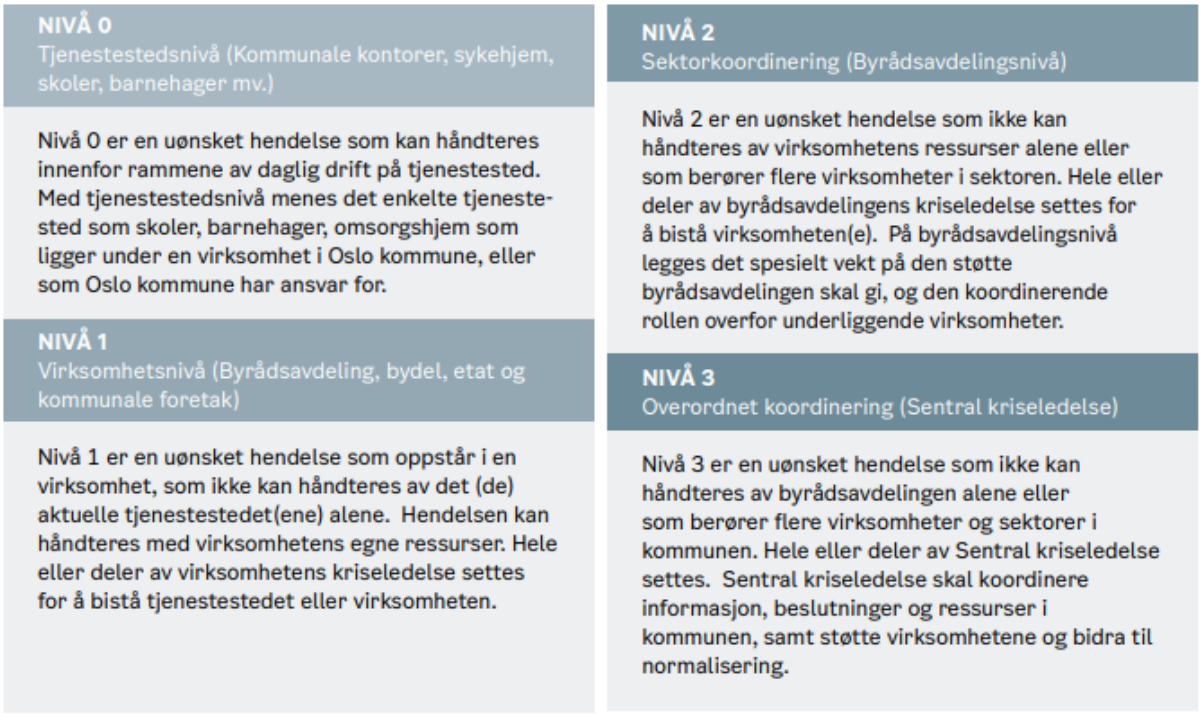
I veilederen vil vi kort nevne litt om krisehåndtering i Oslo. For deretter å se kort på hva en risiko – og sårbarhetsanalyse er og hva slags krav som ligger til grunn for å utarbeide en ROS – analyse. I dette kapitelet vil veilederen også se på hvorfor man bør gjennomfører analyseprosessen, hva den bør inneholde, kommunalt risikobilde og sannsynlighet og konsekvens. Til slutt vil veilederen i dette kapittelet se nærmere på metode, identifisering og vurdering i tillegg til mål og strategi.

Veilederen vil deretter se nærmere på organisering og mandat før den går videre til risiko- og sårbarhetsanalysens forskjellige faser. Disse seks fasene er som følger, bestemmelse av kontekst hvor kunnskap om egen virksomhet og omgivelsene rundt står sterkt. Deretter vil kommunikasjon, risikoidentifisering, risikoanalyse, risikoevaluering og risikohåndtering avslutte dette kapittelet. I de siste kapitlene vil det kort nevnes litt om handlingsplan og avslutningsvis være vedlegg med mal til ROS.

2 KRISEHÅNDTERING I OSLO KOMMUNE

Hver virksomhet har plikt til å etablere kriseledelse og håndtere uønskede hendelser innenfor eget ansvarsområde. Hver virksomhet har et selvstendig ansvar for koordinering av informasjon, beslutninger og ressurser.

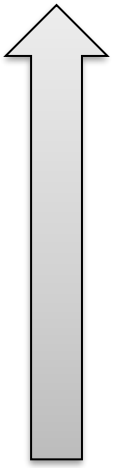
Krisehåndtering i Oslo kommune er organisert på følgende måte:



3 RISIKO- OG SÅRBARHETSANALYSE

En risiko – og sårbarhetsanalyse er en analyseprosess som skal hjelpe kommuner, virksomheter og tjenestesteder til å vurdere risikoen for at uønskede hendelser kan komme til å skje. ROS – analysen skal i tillegg til dette hjelpe til med å finne sannsynligheten for at en negativ hendelse kan skje og hvor store de negative konsekvensene kan komme til å bli. Samtidig er det viktig å understreke at selve analyseprosessen kan ha stor verdi for å styrke kunnskapen og bevisstheten om de utfordringer virksomhetene står overfor og for samfunnssikkerhetsarbeidet generelt. Beredskapsetaten anbefaler derfor at arbeidet med ROS-analyse skjer i egenregi og involverer alle relevante fagmiljøer i virksomhetene i tillegg til viktige eksterne aktører.

Oslo kommune har på overordnet nivå kartlagt hvilke uønskede hendelser som kan inntreffe i kommunen, vurdert sannsynligheten for at disse hendelsene inntreffer, og hvordan de vil kunne påvirke kommunen. Resultatet av dette er presentert i Kommunalt risikobilde 2021 (KRB).

Nivå	Analyser		
Nasjonalt nivå	Analyser av krisescenarioer (AKS) (DSB) Nasjonale trusselvurderinger (NSM, PST, E-tjenesten, politiet, Økokrim)		Risiko aggregeres fra laveste til høyeste nivå.
Regionalt nivå	Fylkesmannens Statsforvalter risiko- og sårbarhetsvurdering («FylkesROS») andre regionale analyser ++		
Kommune	Kommunalt risikobilde (KRB) Overordnet ROS-analyse for Oslo kommune		
Byrådsavdeling	ROS-analyse for sektor		
Virksomhet	ROS-analyse av kommunal virksomhet		
Tjenestested	ROS-analyse av kommunalt tjenestested		

Figur 1: Aggregert risiko i Oslo kommune vil kunne gi et bedre kunnskapsgrunnlag om risiko fra laveste nivå av tjenesteleveranse opp til statlig nivå for analyse av krisescenarioer. Denne veilederen tar for seg de tre laveste nivåene.

3.1 Krav til overordnet Risiko- og sårbarhetsanalyse

Kommunalt risikobilde (heretter kalt KRB) er Oslo kommunes overordnede risiko- og sårbarhetsanalyse (ROS-analyse).

Lov 25.06.2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (Sivilbeskyttelsesloven) stiller krav om at alle kommuner skal ha en egen ROS-analyse.

KRB gir en samlet oversikt over risiko og sårbarheter som befolkningen og kommunen kan bli utsatt for. Formålet er å benytte denne kunnskapen som et grunnlag til å jobbe systematisk og helhetlig med samfunnssikkerhet på tvers av sektorer i kommunen, for å redusere risiko for tap av samfunnsverdier.

I Oslo kommune er ansvaret for å utarbeide denne analysen lagt til Beredskapsetaten, men selve analysen vedtas av byrådet. Analysen skal ligge til grunn for kommunens arbeid med samfunnssikkerhet og beredskap på overordnet nivå og som en del av grunnlaget i de kommunale virksomhetenes egne ROS-analyser[1].

Innføring av kommunal beredskapsplikt iht. sivilbeskyttelsesloven gir en sektovergripende beredskapsplikt med det formål å komplettere eksisterende beredskapsplikter. Det skal bidra til at kommunen vurderer samfunnssikkerhet i et mer helhetlig perspektiv.

3.2 Hvorfor utarbeide en risiko- og sårbarhetsanalyse?

Ingen vet når en alvorlig uønsket hendelse kan inntreffe eller hva denne hendelsen vil bringe med seg av utfordringer for opprettholdelse av kommunal tjenesteproduksjon. Det som kan sies med

[1] Byrådsvedtak 1108/17

sikkerhet er at hendelser vil inntreffe, og at samfunnet vil bli utfordret. Å erkjenne dette er en viktig forutsetning for et godt samfunnssikkerhetsarbeid.

Virksomhetenes risiko- og sårbarhetsanalyse bør:

- Gi oversikt over uønskede hendelser som kan utfordre virksomheten
- Skape bevissthet om risiko og sårbarhet virksomheten står ovenfor.
- Fange opp risiko og sårbarhet på tvers av sektorer internt i virksomheten og med eksterne.
- Gi kunnskap om tiltak for å redusere risiko og sårbarhet for virksomhetens tjenesteproduksjon.
- Identifisere tiltak som er vesentlige for virksomhetens evne til å håndtere risiko.
- Gi grunnlag for mål, prioriteringer og nødvendige beslutninger i virksomhetens arbeid med samfunnssikkerhet og beredskap.
- Gi innspill til andre risiko- og sårbarhetsanalyser internt i kommunen og på overordnet nivå i kommunen (Kommunalt risikobilde).

3.3 HVA INNEHOLDER EN RISIKO- OG SÅRBARHETSANALYSE?

En risiko – og sårbarhetsanalyse består av tre hoveddeler. En innledende del, en analysedel og en oppsummerende del.

En risikoanalyse er et dokument som analyserer en mengde forskjellige typer av hendelser som er uønsket, som kan oppstå hvor som helst og som kan komme til å utfordre kommune, virksomhet eller et tjenestesteds evne til krisehåndtering.

3.4 KOMMUNALT RISIKOBILDE

Kommunalt risikobilde 2021 (KRB) danner grunnlaget for lokale risiko- og sårbarhetsanalyser i alle byrådsavdelinger, bydeler, etater, virksomheter og tjenestesteder2. Formålet med KRB er å gi en samlet oversikt over risiko og sårbarheter i kommunen for å etablere en felles forståelse av risikobildet. KRB skal samtidig innfri krav gitt i sivilbeskyttelsesloven (2010) og forskrift om kommunal beredskapsplikt (2011).

3.5 SANNSYNLIGHET OG KONSEKVENS

I risikoanalysen er det sannsynligheten for at noe kan komme til å skje, konsekvensen av det som har skjedd og usikkerheten for om det kan komme til å skje som måles.

En risiko – og sårbarhetsanalyse starter ofte med en oppsummering og en konklusjon på de risiko som er analysert og hva man har kommet frem til. Dette er for å gjøre det enklere og lettere å vekke leserens interesse i tillegg til at det gir et godt overblikk over hovedinnholdet.

Etter dette bør det følge en introduksjon som innbefatter beskrivelse av bakgrunnen for at analysen skal gjennomføres, formålet, forutsetningene og eventuelle avgrensninger.

[2] Byrådsvedtak 1108/17

Så kommer vi til den fasen som heter mandat. Et mandat er en plan som anslår arbeidets handlingsrom og setter opp mål i tillegg til rammene for arbeidet.

Deretter bør man komme med en beskrivelse av virksomhet eller tjenestested. Her bør man ha med et godt informasjonsgrunnlag og en beskrivelse på hvem som har deltatt, i tillegg til ulike interessenters involvering.

3.6 METODE

Så kommer vi til metodedelen. Dette må med for å kunne vise at valgt metode egner seg til å besvare spørsmålene knyttet til risikoanalysen, både med tanke på validitet og reliabilitet. Det forklarer leseren hva du har gjort i undersøkelsen, hvilke valg du har gjort, på hvilken måte du har samlet inn data og hva slags rammer som er satt.

3.7 IDENTIFISERING OG VURDERING

Identifisering av uønskede hendelser er viktig for å kunne komme fram til hva slags hendelser som kan oppstå i virksomheten eller tjenestested. Uønskede hendelser kan være ulykker hvor en hendelse fører til personskade eller død, alvorlige hendelser kan være noe som kunne ført til en ulykke mens hendelser kan være alle andre typer hendelser. Enhver virksomhet eller tjenestested kan ha forskjellige typer av hendelser som vil være spesifikt, det vil derfor ikke gis et eksempel på dette. Flere eksempler på uønskede hendelser gis i KRB 2021.

I delen som heter risiko og sårbarhetsvurdering skal man identifisere risikoene i systemet, med andre ord hva som eventuelt kan gå galt og vurdere konsekvensene og sannsynligheten av disse.

Det neste trinnet i analysen er å identifisere tiltak som kan hindre eller minimere skadene som kan oppstå ved en eventuell hendelse eller ulykke. Det er funnet risikoer, som kan skade virksomheten og disse er såpass betydelige at virksomheten bør iverksette risikoreduserende tiltak.

Oppbyggingen av en risiko- og sårbarhetsanalyse er et stort stykke arbeid, og vi kommer nå fram til et punkt som kan kalles fremstilling av risiko- og sårbarheter. I denne delen av analysen skal alle diagrammer og matriser legges frem. Matrisene gir en god visuell fremstilling av identifiserte konsekvenser og sannsynligheter og viser den vurderte risiko til de analyserte scenarioer som er funnet mest alvorlig.

3.8 MÅL OG STRATEGI

Risikohåndtering er analysens forslag til mål og strategi i tillegg til en plan for videre oppfølging. Det skal iverksettes spesifikke tiltak som kan redusere konsekvensene av en hendelse. Dette punktet er viktig å ha med da analysen uten dette vil være å anse som ufullstendig.

Helt til slutt har vi to punkter som vel så viktig som de andre, men ofte kan virke vanskelige å få fullført. Det ene er referanser, som betyr og gi nøyaktig informasjon om hvilke kilder, opplysningsverk, kart eller andre kilder, som er benyttet underveis i analysen. Referanser skal vises til underveis i analysen og i en referanseliste på slutten av dokumentet.

Det siste punktet vil typisk kunne inneholde vedlegg i form av analyseskjemaer, matriser, kart mv.

4 ORGANISERING

En ROS krever en bred gjennomgang i hele virksomheten for å identifisere og analysere alle risikoer virksomheten er utsatt for. Det er viktig med en tverrfaglig sammensetning og helhetlig tilnærming for å belyse flest mulig områder som er nødvendig å frembringe i analysen.

ROS arbeidet bør organiseres som et prosjekt der prosjekteier er leder av virksomheten, og har det overordnede ansvaret for samfunnssikkerhet og beredskapsarbeidet i virksomheten.[3]

Prosjektet kan bestå av prosjektleder og prosjektgruppe, men organiseres og dimensjoneres etter hva som er mest hensiktsmessig for virksomheten utfra størrelse og ansvarsområde.

Prosjektgruppen kan etableres som en fast gruppe, mindre grupper per risikoområde eller man kan trekke inn personer innenfor fagområder som analyseres. Det er hensiktsmessig at et medlem i prosjektet har kompetanse i, og erfaring fra risiko- og sårbarhetsanalyser og forståelse for fagfeltene samfunnssikkerhet og beredskap.

Risiko- og sårbarhetsanalyser er en læringsprosess for prosjektets medlemmer og virksomheten. Det er derfor virksomhetens egeninteresse at det benyttes internt ansatte til gjennomføringen. Noen risikoområder vil være sammenfallende med andre virksomheters risikoer og det kan være hensiktsmessig med hensyn til effektivitet og kompetanse at det samarbeides med dem innenfor noen analyser.

For tjenestesteder vil det være naturlig at eier av lokal ROS er tjenestestedets leder. Gjennomføring av analyser vil være avhengig av tjenestestedets omfang og ansvar. Gjennomføring av analyser bør derfor organiseres slik det er mest hensiktsmessig.

Ulike løsninger som kan benyttes:

- Gruppetilnærming
- Utpeke individuelt ansvarlige for analyser
- Tjenestestedsleder utfører analyser eller kvalitetssikrer analyser som er utført

Flere tjenestesteder vil ha like arbeids og ansvarsoppgaver, og det kan være hensiktsmessig med hensyn til effektivitet og kompetanse at det kan samarbeides innenfor noen analyser.

Oppsummering av delkapittel

- ROS forankres hos virksomhetsleder/tjenesteleder
- Virksomheter drar fordel av prosjekttilnærming
- Mandat utarbeides skriftlig
- ROS er en læringsprosess som gir avkastning til egen virksomhet
- Dimensjoner prosess til hensiktsmessig omfang for virksomheten/tjenestestedet

[3] Instruks for virksomhetsstyring

4.1 Mandat

Utarbeiding av mandat må inkludere formålet til ROS. Formålet til ROS er beskrevet i forskrift om kommunal beredskapsplikt, men virksomheten/tjenesteområdet har mulighet til å utdype formålet, eventuelt legge til. Mandat innebærer også en avklaring av hvilke avgrensninger ROS-analysen skal gjøre, for eksempel knyttet til geografisk nedslagsfelt, detaljnivå eller utelukking av hendelser med ekstremt høy eller veldig lav risiko. Det kan også være andre avgrensninger som må gjøres, avhengig av virksomhetens/tjenesteområdets fagfelt.

Mandat, formål og avgrensning bør også forankres, slik at alle interessenter er omforent om hva som blir sluttproduktet.

5 Gjennomføring av risiko- og sårbarhetsanalysen

KRB-metoden baserer seg konseptuelt på rammeverket i ISO 31000, ved at metodikken er delt inn i forskjellige faser, som er hovedelementer i risikostyringsprosessen:

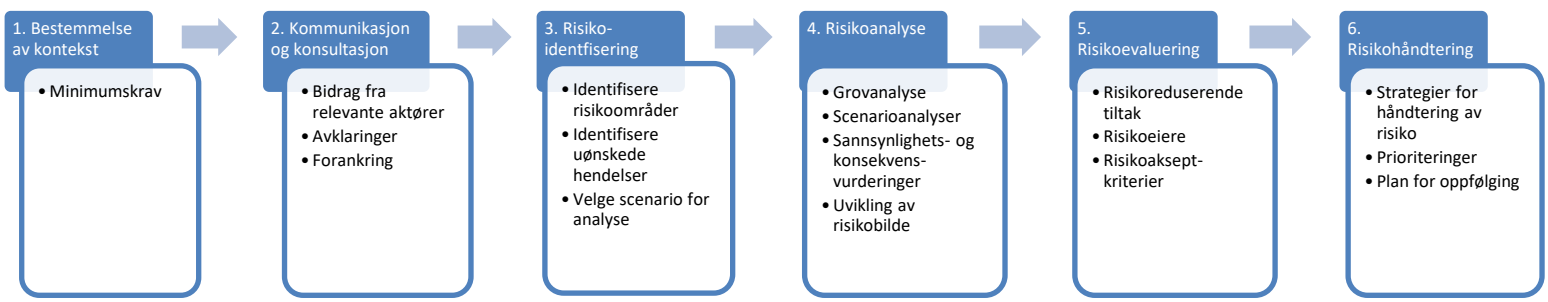
1. Bestemmelse av kontekst
2. Kommunikasjon og konsultasjon
3. Risikoidentifisering
4. Risikoanalyse
5. Risikoevaluering
6. Risikohåndtering

Risikoevaluering og risikohåndtering krever vurderinger om beslutning av tiltak som ligger til beslutningsprosessen i etterkant av analysen som er en del av handlingsplanen (Kapittel 3). Risikohåndtering kan kreve mer detaljerte vurderinger av tiltakenes risikoreduserende effekter og kostnader før beslutninger kan tas hos den enkelte risikoeier.

Risikoanalyser for virksomheter skal behandle risikoer som utfordrer virksomhetens kontroll og styringsevne eller evne til å opprettholde tjenesteproduksjon. Risikoer som forstås som dagligdagse hendelser og håndteres av grunnberedskapen i virksomheten er ikke tiltenkt å inkluderes i virksomhetens risikoanalyse.

Risikoområder og analyse

KRB benytter risikoområder til å samle lignende hendelsestyper. Som et eksempel vil du i KRB finne risikoområdet *Ekstremvær og nedbør.* I risikoområdet vil du finne tre ulike scenarioanalyser for henholdsvis *Stormflo indre Oslofjord, Urban flom* og *Kvikkleireskred.* Strukturen gir dermed leseren informasjon om hva som er risiko og sårbarhet for et risikoområde, med en underliggende scenarioanalyse om hvordan risiko og sårbarheter kan påvirke kommunen.



Figur 2: Visuell illustrasjon av trinnene i risikostyringsprosessen (utgangspunkt ifra KRB).

Virksomhetene er ikke låst til denne strukturen, men scenarioanalysemetodikken er sentral. Årsak til dette er at scenarioanalyser forsøker å forstå omfang og potensielle muligheter for utvikling av risiko. I KRB-metoden benyttes scenarioanalyser, erfaring og kontekst i kombinasjon med fagkunnskap for å analysere mulige uønskede hendelser som kan oppstå.

Oppsummering delkapittel

- Risiko- og sårbarhetsvurderingen har seks faser.
- Risikoevaluering og Risikohåndtering tilhører handlingsplanen og bør inneholde tiltak med behov for beslutningsmyndighet.
- Scenarioanalyser er nødvendig for alle virksomheter og tjenestesteder.

5.1 Bestemmelse av kontekst

For å forstå risiko er det viktig at forutsetningene for eksponeringen mot risiko blir forstått. Det innebærer kunnskap om seg selv og sine omgivelser. Virksomhetens risiko- og sårbarhetsanalyse skal begynne med beskrivelse av virksomheten og konteksten virksomheten opererer i.

Dette kan inkludere:

- Lover, forskrifter, reglementer, byrådsvedtak og administrative vedtak som styrer virksomheten.
- Organisering.
- Geografiske avgrensinger innen Oslo kommune og/eller bydeler.
- Beredskapskapasiteter i og utenfor virksomheten.
- Samarbeidende aktører og andre aktører innenfor virksomhetens område og ansvar.
- Særskilte aspekter innen virksomhetens fagansvar eller særskilte aktiviteter.

Annen relevant informasjon bør være:

- Fysiske og naturgitte forhold
- Sosiale, demografiske og økonomiske forhold
- Samferdsel (veg, bane, luft, sjø)
- Næringsvirksomhet/industri/turisme
- Kritiske samfunnsfunksjoner og infrastrukturer
- Planer for fremtidig utvikling
- Fremtidig klima

Minimumskrav til analysen for virksomheter:

1. Hvilke årsaker og årsaksforhold kan føre til uønskede hendelser og potensielt farlige situasjoner?
2. Hvordan arbeides det med forebygging og beredskap innenfor forskjellige risikoområder?
3. Hvor robust er virksomheten til å håndtere en alvorlig uønsket hendelse og samtidig opprettholde virksomhetens tjenesteproduksjon?
4. Hvordan kan virksomhetens arbeid med samfunnssikkerhet og beredskap styrkes?
5. Eksisterende og fremtidige risiko- og sårbarhetsfaktorer i virksomheten.

6. Risiko og sårbarhet utenfor virksomhetens geografiske område / lokasjon som kan ha betydning for virksomheten.
7. Hvordan ulike risiko- og sårbarhetsfaktorer kan påvirke hverandre.
8. Særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur.
9. Virksomhetens 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.
10. Behov for befolkningsvarsling og evakuering?

Oppsummering delkapittel

- ROS-analysen begynner med beskrivelse av egen virksomhet og eksterne faktorer som påvirker - konteksten til analysene.
- Analyser må svare ut minimumskrav, enten det er på virksomhetsnivå eller tjenestested.

5.1.1 KOMMUNIKASJON OG KONSULTASJON

Kommunikasjon og konsultasjon innad i virksomheten, med andre kommunale, offentlige og private aktører og risikoeiere er viktig for å oppnå innsikt i og tilgang til ekspertise innen forskjellige risikoområder.

Kommunikasjon er en kontinuerlig og sentral delprosess i analyseprosessen. Innledende kommunikasjon og kommunikasjon underveis med ledelsen vil være avgjørende for å sikre sluttproduktets relevans. Kommunikasjon og samarbeid med ulike fagmiljøer internt og eksternt er viktig for integriteten og objektiviteten til analyser.

5.1.2 RISIKOIDENTIFISERING

Identifisering av risikoområder er et resultat av et sammensatt arbeid. Risikoområder som må analyseres vil avdekkes i løpet av arbeidet med å etablere kontekst, kommunikasjon med fagmiljøer og risikoeiere, i tillegg til undersøkelser av ulike datakilder.

Informasjonskilder som kan ha betydning for risikoidentifisering og analysen kan være:

- Tidligere risiko- og sårbarhetsanalyser for virksomheten og tjenestesteder.
- Evalueringer og rapporter fra tidligere hendelser og kriser i virksomheten i tillegg til historiske data i kommunen.
- KRB 2022.
- Fylkes-ROS og nasjonale risikovurderinger.
- Evalueringer og rapporter fra øvelser og tilsyn.
- Kontakt, samarbeid og avtaler med andre aktører.
- Forskning og rapporter innen virksomhetens fagområder.
- Egen lokalkunnskap, erfaringsdata og kompetanse i virksomheten.
- Kommunale og nasjonale GIS-systemer.
- Avviks- og kvalitetssystemer.

Risiko- og sårbarhetsanalysene skal aggregeres i kommunen mot overordnet ROS, og det er derfor nyttig at virksomhetens kompetanse og erfaring fremkommer tydelig. Dette bidrar til at kommunen blir bedre kjent med seg selv, sine kapasiteter og utfordringer. Dette har betydning

for den overordnede risiko- og sårbarhetsanalysen, samfunnssikkerhets- og beredskapsarbeidet og samvirket i kommunen.

Risiko skal ikke bare aggregeres mot overordnet ROS, men også inneholde overordnede analyser som skal være relevante og hensiktsmessige for kommunens virksomheter og tjenestesteder. Det kan eksempelvis benyttes risikoområder og scenarioer fra KRB, tidligere analyser og andre virksomheters analyser inn mot sin egen identifisering og scenarioer, dimensjonert og tilpasset for virksomheten eller tjenestestedet.

Identifisering av uønskede hendelser – valg av scenario for analyse

De uønskede hendelsene som inkluderes i ROS er hendelser som er større og mer alvorlig enn uønskede hendelser som den daglige driften kan håndtere. Det vil si at hendelser som er alvorlige for et tjenestested ikke nødvendigvis påvirker virksomheten i sin helhet. Virksomheter og tjenestesteder må dermed dimensjonere scenarioene til sine respektive nivåer.
For at en uønsket hendelse skal være alvorlig nok på et overordnet nivå er følgende kriterier benyttet for utvelgelse.

De uønskede hendelsene som inkluderes i ROS er hendelser som:

- vil ramme større grupper av mennesker.
- er større og mer alvorlige enn uønskede hendelser som virksomhetenes/tjenestestedets daglige drift kan håndtere.
- er av en slik art at den utgjør en ekstraordinær påkjenning.
- Berører flere sektorer eller ansvarsområder som krever samvirke.

Oppsummering delkapittel

- Risikoidentifisering er et resultat av arbeidet med å etablere kontekst, kommunikasjon med fagmiljøer og risikoeiere, i tillegg til undersøkelser av ulike kilder.
- Omfattende informasjonskildegrunnlag gir mulighet til å identifisere nye risikoer som ikke har blitt analysert tidligere.
- Benyttelse av risikoområder og scenarioer fra KRB kan tilføre egen erfaring og kompetanse til risikoområdet.
- Tjenestesteder benytter egen erfaring og kompetanse som primærkilde i identifisering og analyser.
- Hendelsene som analyseres må tilpasses hvilket nivå ROS utføres for, og må utfordre den daglige driften i virksomhetene eller tjenestestedene.

5.1.3 RISIKOANALYSE

Risiko

Risiko beskrives i KRB som hvor sannsynlig det er at en uønsket hendelse inntreffer, konsekvenser av denne, gitt usikkerheten. Begrepet usikkerhet benyttes for å beskrive kvaliteten på bakgrunnskunnskapen vurderingene er basert på.

Risiko handler om hva som kan skje i framtiden og er derfor forbundet med usikkerhet. Usikkerheten knytter seg til om en bestemt uønsket hendelse vil inntreffe og hva konsekvensene av denne hendelsen vil bli. Usikkerhet reflekterer blant annet kunnskapsgrunnlaget for analysen, og dette må adresseres eksplisitt i beskrivelsen av analyseresultatene.

Hovedkategorier

Analyser av risikoområder som er valgt kategoriseres innenfor fem hovedkategorier:

1. Store ulykker
2. Naturhendelser
3. Kritisk infrastruktur
4. Helse
5. Tilsiktede handlinger

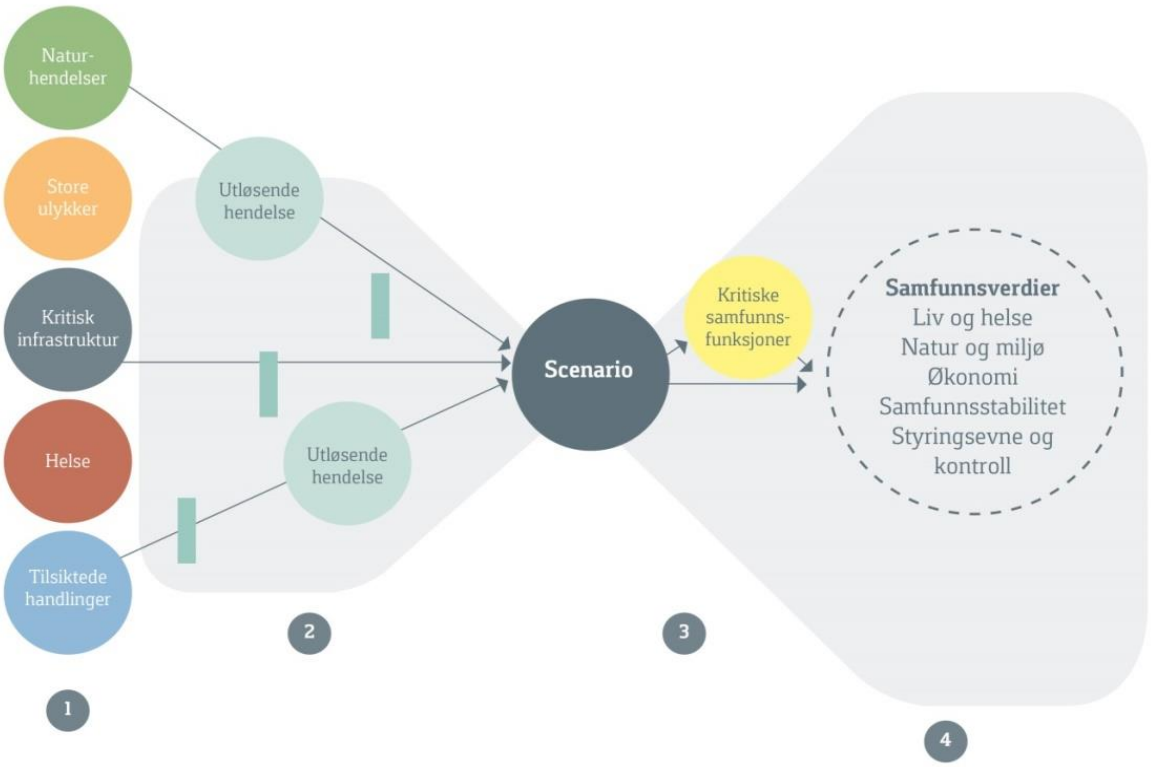
Noen kategorier vil ha flere risikoområder enn andre for noen virksomheter. For å sikre en bred innsikt bør alle kategorier dekkes. KRB 2022 har 17 risikoområder. Virksomheter og tjenestesteder bør tilstrebe 10 eller flere analyser for å sikre at de mest nødvendige risikoområdene blir analysert.

Analyseprosess

Analyser i ROS følger sløyfemodellen. Analyser skal undersøke årsaker innenfor risikoområder som kategoriseres innenfor de fem nevnte hovedkategoriene (1).
Virksomheter har muligheten til å velge om de ønsker å gjennomføre inngangsanalyser. Om inngangsanalyser benyttes vil de være grovanalyser som dekker et risikoområde (1). Grovanalysen undersøker sårbarheter og sannsynlighetsreduserende barrierer, samt årsaker og årsaksforhold som kan føre til farlige hendelser.

Inngangsanalysene (2) beskriver sårbarheter og sannsynlighetsreduserende barrierer risikoområdene representerer, men også årsaker og årsaksforhold som kan føre til uønskede hendelser og potensielt farlige situasjoner. Inngangsanalysene beskriver også arbeidet med forebygging og beredskap innenfor risikoområdene, som konsekvensreduserende tiltak.

Ved konsekvensvurderinger vurderes påkjenninger på kritiske infrastrukturer og deres påkjenninger på samfunnsverdiene (3), og direkte påkjenninger på samfunnsverdier fra hendelsen (4). Sårbarheter som rammes, kan påvirke både sannsynligheten for at hendelsen vil inntreffe og konsekvensene den får. Sårbarheten er i stor grad avhengig av om det finnes tilstrekkelige, pålitelige og effektive barrierer i systemet. Usikkerhetsfaktoren er sentral, både ved sannsynlighetsvurderinger og for konsekvensvurderingene. Usikkerheten er en medvirkende (kunnskaps)faktor for analysenes resultat og er en sentral del i alle analysene.



Sannsynlighet

Sannsynlighet brukes som et uttrykk for hvor trolig det er at en bestemt hendelse vil inntreffe, gitt tilgjengelig kunnskapsgrunnlag. For å kunne angi sannsynligheten for at en gitt hendelse skal skje er kilder som statistikk, andre sentrale analyser som KRB, Sektor-ROS, lokalkunnskap, fagkunnskap og øvrige erfaringer fra hendelser både lokalt, regionalt, nasjonalt og internasjonalt relevant.

For hendelser som skjer sjeldnere, eller som enda ikke har skjedd, er vurderingsgrunnlaget mer usikkert. Her bør sannsynlighetsvurderingene baseres på diskusjon og på fagkunnskapen til de aktørene som involveres.

Sannsynlighetsvurderinger kan baseres på enten beregninger og/eller estimater der hvor datagrunnlaget er godt og har vært tilgjengelig for de respektive scenario.

Kategori	A			B			C			D			E		
Sannsynlighets-vurdering	Svært lav			Lav			Middels			Høy			Svært høy		
Sannsynlighetsverdi	0	10	20	21	30	40	41	50	60	61	70	80	81	90	100

Scenarioanalyser

Et scenario er hverken en prognose eller en forventning om framtiden. Scenariometoden handler om å lage et sett av forskjellige, troverdige og utfordrende fortellinger om framtiden. Fortellingene kan brukes som et bakteppe for strategiarbeid eller iverksettelse av tiltak. Scenarioene som representerer ulike fremtidsbilder åpner et mulighetsrom for hva virksomheten trenger å være forberedt på at kan inntreffe og hva virksomheten potensielt vil måtte håndtere.
Et spesifikt scenario gir et mer konkret analysegrunnlag enn generelle hendelser, som gir for store variasjoner i resultatene til at de kan brukes til analyse. Ved å analysere et scenario er det mulig å kartlegge konkret hvilke samfunnsfunksjoner som berøres. Dette gjør det mulig å utarbeide forebyggende og konsekvensreduserende tiltak. Forståelse for viktige usikkerheter, gjensidige avhengigheter og deres underliggende dynamikk gjennom en scenarioanalyse bidrar til økt innsikt i følgekonsekvenser.

Når man bruker scenarioanalyser vil analysen av sannsynlighet og konsekvenser kun være gyldig for akkurat dette scenarioet, med de forutsetninger som er valgt. Likevel, fordi man ofte analyserer verstefallsscenarioer, vil øvrige scenarioer innen samme hendelsestype kunne være mildere og lettere å håndtere, med færre og mindre alvorlige konsekvenser.

Det kan behandles flere sårbarheter i inngangsanalyser uten at en scenarioanalyse gjennomføres. På denne måten blir ROS-analysen mer utfyllende, og den får dermed en større nytteverdi for virksomhetenes arbeid med samfunnssikkerhet.

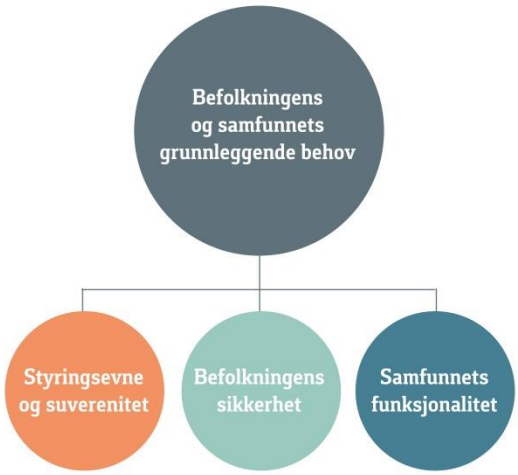
Utvikling av risikobilde

Et konkret risikobilde kan skape både tilslutning og motforestillinger, men bidrar i begge tilfeller til økt bevissthet og diskusjon om risiko. Å diskutere og analysere risiko øker kunnskapsnivået og forståelsen av farer, sårbarheter og usikkerhet. Ved å tenke gjennom hva som kan skje, forstå utviklingen av katastrofale hendelser og hvilke konsekvenser de kan få, blir vi i bedre stand til å møte krisene som måtte komme.

Scenarioanalyser brukes for å bringe frem og skape økt kunnskap og bevissthet om det brede spekteret av følgehendelser og konsekvenser.

Kritiske samfunnsfunksjoner

Kritiske samfunnsfunksjoner er oppgaver som samfunnet må opprettholde for å ivareta befolkningens sikkerhet og trygghet, samt dekke deres grunnleggende behov. Flere virksomheter har ansvar for kritiske samfunnsfunksjoner og det er viktig å prioritere å knytte disse opp mot scenarioanalysene for å vurdere påkjenninger og sammenfall. Utledningen av hvilke samfunns-funksjoner som er kritiske, og hva disse samfunnsfunksjonene består i er hentet fra DSBs definisjon av kritiske samfunnsfunksjoner.



Styringsevne og suverenitet
inkluderer funksjoner knyttet til territoriell og styringsmessig integritet, opprettholdelse av styringsaktiviteter og evne til å møte ekstra ordinære situasjoner.

Befolkningens sikkerhet
inkluderer funksjoner som skal gi vern mot død, fysisk skade eller sykdom, tap av demokratiske rettigheter og personlig integritet, og tap eller skade på livsmiljøet, eiendom eller materielle verdier.

Samfunnets funksjonalitet
inkluderer kontinuitet i forsyninger og infrastrukturbaserte tjenester.

Disse tre kategoriene representerer samlet 14 underliggende samfunnsfunksjoner med tilhørende kapabiliteter.

I scenarioanalysene vurderes påkjenninger for disse 14 samfunnsfunksjonene med tilhørende kapabiliteter. Det er kun de samfunnsfunksjonene som får påkjenninger som synliggjøres i scenarioanalysene og som representerer gjensidige avhengigheter.

Underkategoriene brytes ned til de nivåer som er relevante for kommunen og virksomhetene. Eksempelvis vil utfall av Oslo felles nettverk være en påkjenning for «Elektroniske kommunikasjonstjenester» (og mulig «IKT sikkerhet»), eller brann på helseinstitusjon være påkjenning for «Helse og omsorg».

Styringsevne og suverenitet	Befolkningens sikkerhet	Samfunnets funksjonaliteter
Styring og kriseledelse Forsvar	Lov og orden Helse og omsorg Redningstjenester IKT-sikkerhet Natur og miljø	Forsyningssikkerhet Vann og avløp Finansielle tjenester Kraftforsyning Elektroniske kommunikasjonstjenester Transport Satellittbaserte tjenester

Samfunnsverdier

Konsekvenser av en hendelse vil være alvorlige når de rammer de verdier vi har, materielle og immaterielle. Derfor blir konsekvenser målt mot verdier for å forstå hvor stor konsekvensen er. Verdiene i KRB er satt basert på samfunnsverdier:

- Liv og helse
- Natur og miljø
- Økonomi
- Samfunnsstabilitet
- Styringsevne og kontroll

Det vil bli vedlagt kriteriesetting for vurdering av konsekvenser mot verdiene fra KRB. Kriteriene må dimensjoneres etter virksomhetens eller tjenestestedets behov. Det vil si at i KRB kan ulike påkjenninger vurderes utfra eksempelvis hvor mange virksomheter som er påvirket, men for en virksomhet kan det være hvor mange lokasjoner eller avdelinger som er påvirket.

I noen analyser kan det være verdier som ikke har noen påkjenning og en vurdering er ikke da nødvendig.

Usikkerhet

Usikkerhetsvurderingen må gjøres for alle konsekvenser mot verdier som er vurdert.

Kunnskapsgrunnlaget	**Liten**	**Moderat**	**Stor**
Tilgang på relevante data og erfaringer	1	2	3
Forståelse av hendelsen som analyseres (hvor kjent og utforsket er fenomenet)	1	2	3
Enighet blant ekspertene (som har deltatt i risikoanalysen)	1	2	3
Sensitivitet			
I hvilken grad påvirker endringer i forutsetningene anslagene for sannsynlighet og konsekvenser?	1	2	3
Samlet vurdering av usikkerhet	**Stor**	**Moderat**	**Liten**
Gjennomsnittsverdi	**1,0 – 1,49**	**1,5 – 2,49**	**2,5 – 3,0**

Styrbarhet
Styrbarheten til et scenario betyr hvordan virksomheten kan påvirke utfallet i en hendelse. Hvilke tiltak virksomheten bør iverksette for å redusere sannsynlighet og konsekvens, og hvor effektive de vil være. Styrbarheten til et scenario vil være lav hvis det er lite virksomheten kan gjøre for å kontrollere og påvirke. Styrbarheten er en egen evaluering som skal øke forståelsen for hvilke tiltak som er aktuelle og gir økt innsikt i sensitiviteten til et scenario.
Tjenestesteder trenger ikke vurdere styrbarhet.

Overførbarhet
Overførbarhet er en vurdering av om scenario og vurderinger som er utført er overførbare til andre virksomheter eller sektorer. Årsaken til at man gjør overførbarhetsvurdering er at det forteller leseren av vurderingen om hvor tett knyttet den er til fag, virksomhetsspesifikke anliggender, forståelsen av hendelsen og hvordan den tolkes.

Scenarioer med høy overførbarhet indikerer at risikoen befinner seg flere steder i kommunen og kan bidra i risikoidentifiseringsarbeidet for andre virksomheter og gi innsikt for overordnet ROS hva som er behovet.

Oppsummering delkapittel
- Det er fem hovedkategorier analyser inndeles etter.
- Analyseprosessen tar utgangspunkt i sløyfemodellen.
- Analyser årsaker, sannsynlighetsreduserende barrierer og konsekvensreduserende barrierer.
- Vurder konsekvenser mot kritisk infrastruktur og verdier. Tjenestesteder vurderer ikke kritisk infrastruktur.
- Scenarioanalyser må benyttes.
- Diskusjoner og analyser øker bevissthet om risiko og er en viktig faktor.
- Vurderingskriterier mot verdiene må dimensjoneres etter virksomheten og tjenestestedets behov.
- Virksomheter må vurdere usikkerhet i konsekvensvurderingene, men tjenestesteder må ikke.
- Virksomheter må vurdere styrbarhet og overførbarhet av scenarioanalysene, men ikke tjenestesteder.

5.1.4 RISIKOEVALUERING
Med utgangspunkt i sammenstillingene er det mulig å identifisere hvilke hovedkategorier, herunder tilhørende risikoområder, som utgjør størst risiko. På bakgrunn av resultatene som er funnet vil det være mulig å prioritere områder for sannsynlighetsreduserende eller konsekvensreduserende tiltak.

Risikoreduserende tiltak på detaljnivå kan innebære økonomiske prioriteringer og er et ansvar som tilligger virksomheters mandat og ansvarsområder.

Hva som skal aksepteres av risiko og sårbarhet og hvilke tiltak som skal iverksettes avgjøres i praksis gjennom faglige og byråkratiske beslutningsprosesser styrt av risikoeiere innenfor de ulike risikoområdene.

Akseptkriterier
Bruk av akseptkriterier krever forhåndsdefinering av akseptkriterier. I en analyseprosess kan det oppfattes som formelle beslutningskriterier. Fastsettelse av akseptkriterier før ROS-analyser/risikovurderinger kan bidra til å ALARP-prinsippet (As Low As Reasonably Practicable), som innebærer at alle tiltak for å redusere risiko skal gjennomføres såfremt det ikke er et stort misforhold mellom kostnaden og nytten av tiltaket.
Virksomhetene skal selv vurdere behovet for å iverksette identifiserte risikoreduserende tiltak
Virksomheter som har flere ulike ansvarsområder kan oppleve det problematisk med akseptkriterier, da ikke alle områder kan vurderes innenfor de samme spenn av kriteriene.

ROS-analyser med kvalitative konsekvensvurderinger av scenarioer, gjør at tiltak utarbeides uavhengig av fastsettelse av akseptkriterier. Et annet viktig aspekt ved kvalitative ROS-analyser er at usikkerhet ved fastsettelse av sannsynlighet og konsekvens gjør at det ofte benyttes erfaring og skjønn under prosessen.

Det vil si at kvalitative konsekvensvurderinger er kompetansedrevet fremfor kvantitative kriterier, og tiltak vil dermed gjenspeile faglige vurderinger og behov fremfor kvantitative vurderinger. Kvantitative vurderinger kan gjøre prosessen enklere, men har noen negative sider for en analyse på virksomhetsnivå.

For de fleste tjenestesteder er det hensiktsmessig å benytte akseptkriterier. For virksomheter kan det vurderes hva virksomheten selv finner mest hensiktsmessig.

Alle vurderinger, uavhengig av valg av hvordan konsekvens vurderes, må vurderes etter verdiene som er satt:

- Liv og helse
- Natur og miljø
- Økonomi
- Samfunnsstabilitet
- Styringsevne og kontroll

5.1.5 RISIKOHÅNDTERING
Tiltak i risikohåndteringen omfatter i hovedsak fire alternative måter å håndtere risiko på: unngå risiko, dele risiko, redusere risiko og akseptere risiko. Fokus på å redusere sannsynlighet og/eller konsekvenser står sentralt for vurdering av tiltak. Men også å koble positive og negative sider ved risiko.

Virksomhetene må utarbeide langsiktige mål, strategier, prioritering og plan for oppfølging av samfunnssikkerhets- og beredskapsarbeidet. Risikohåndtering er en naturlig del av dette arbeidet, som fullføres i etterkant av analysearbeidet.

6 HANDLINGSPLAN
Virksomhetene og tjenestestedene står ikke overfor en enkel trussel, risiko eller sårbarhet, men et mangfold av risikobilder, som vil kreve ulike forebyggende og skadereduserende tiltak. Alle

virksomheter og tjenestesteder skal etablere en handlingsplan med tiltak mot risikoer som er identifisert i ROS-analysen.

For tjenestesteder må handlingsplanen utarbeide forebyggende og konsekvensreduserende tiltak, samt en plan for gjennomføring av tiltak.

For virksomheter skal handlingsplanen identifisere nødvendige tiltak for å utvikle kunnskapsgrunnlag, forebygge hendelser, redusere konsekvenser og styrke evne til krisehåndtering. I tiltakene skal det utarbeides langsiktige mål, strategier, prioriteringer og plan for oppfølging av samfunnssikkerhets- og beredskapsarbeidet og inkluderes i den langsiktige virksomhetsstyringen.

§ 3b i forskrift om kommunal beredskapsplikt pålegger også kommunen å gjøre vurdering av om det er risiko- og sårbarhetsforhold i ROS-analysen, som bør integreres i planer og prosesser etter plan- og bygningsloven. Det er viktig for å unngå at arbeidet med risiko- og sårbarhetsanalyser og oppfølgingen av disse ikke blir frikoblet fra kommunens øvrige styringssystem.

Det er de enkelte virksomhetenes analyser og planverk, som skal være styrende for hvordan forebyggende arbeid, beredskap og økt evne til krisehåndtering lokalt skal utvikles basert på overordnede planverk, målsetning og strategi.

7 VEDLEGG MALER

Under følger en foreslått mal til risiko- og sårbarhetsvurderinger i kommunen.

Oslo

Beredskapsetaten

Mal - Risiko- og sårbarhetsanalyse

Dette dokumentet fremstiller en mal for hvordan en ROS-analyse i Oslo kommune kan bygges opp.

[Denne malen viser hvordan en ROS-analyse i Oslo kommune kan bygges opp. Malen bygger på dokumentet «veileder til ROS», utarbeidet av Beredskapsetaten. Hva gjelder oppbygging av ROS-dokumentet henvises det spesielt til kapittel 1.4 i «Veileder til ROS». Hva gjelder teori og metodikk henvises det til «Veileder til ROS» i sin helhet. Det bes om at den enkelte virksomheter tilpasser malen til egen ROS-analyse.]

BEGREPSLISTE

[Se begrepsliste i «Veileder til ROS», og vurder om andre begreper bør forklares, for eksempel virksomhetsinterne begreper og forkortelser]

1.0 OPPSUMMERING OG KONKLUSJON

[Oppsummering av ROS-analysens funn. Dette kan være blant annet kort om analyseobjektet, omfang og avgrensninger, oppsummering av scenarioanalyser og risikobilde]

INNHOLDSFORTEGNELSE

2.0 INNLEDENDE DEL

[Bør inneholde en beskrivelse av bakgrunn for gjennomføring av analysen, formålet, forutsetninger og avgrensninger, i tillegg til en beskrivelse av den aktuelle virksomhet eller tjenestested, samt hvem som har deltatt og interessenters involvering. Denne delen bør også inkludere en beskrivelse av anvendt metode]

2.1 BAKGRUNN FOR AT ANALYSEN GJENNOMFØRES

[Kan si noe om hva som er bakgrunner for at analysen gjennomføres nå, for eksempel nye forhold som har generert behov for en ny ROS]

2.2 FORMÅL

[Kan si noe om hva som er formålet med ROS-analysen. Dette kan være basert på lovkrav eller andre krav, etterlevelse av virksomhetsinterne retningslinjer, eller å dekke noen nye behov]

2.3 Forutsetninger og lovkrav

[Kan si noe konkret om hvilke forutsetninger som ligger til grunn for ROS-analysen, og hvilke pålagte krav, eksterne og/eller interne, som legger føringer for blant annet ROS-analysens omfang, innhold og avgrensning]

2.4 Omfang og avgrensninger

[Kan si noe om hvor bredt ROS-analysen spenner, eller med andre ord hvor bredt nedslagsfeltet til ROS-analysen er. Kan også si noe om hvilke forhold som bevisst utelates fra ROS-analysen. Disse valgene bør begrunnes]

2.5 Mandat

[Kan si noe om hvilket mandat som er utgangspunkt for ROS-analysen, for eksempel knyttet til tidsbruk, gjennomføringsansvarlige eller lignende. Mandat handler også om forankring. Forankringen av ROS-analysen hos virksomheten og eventuell toppledelse bør beskrives]

2.6 Beskrivelse av virksomhet/tjenestested

[I dette punktet kan det følge en beskrivelse av virksomheten/tjenestestedet. Dette kan inneholde en beskrivelse av virksomhetens fagområde og ansvarsområde, konkrete tall og fakta om virksomheten, nedslagsfelt, fysisk og digital eiendom, brukere med mer. Dette kapittelet skal gi en introduksjon til «systemet» som skal risiko- og sårbarhetsanalyseres]

2.7 Deltakere og interessenters involvering

[Kan gi en beskrivelse av hvem som har deltatt i analyseprosessen. Her kan det også gis en beskrivelse av eventuell relevans av ROS-analysen utover virksomhetens eget fagområde/ansvarsområde. Med interessenters involvering sikter det til blant annet eksterne som har bidratt i prosessen]

2.8 Metodisk tilnærming

[Dette delkapittelet bør gi en beskrivelse av hvordan arbeidsgruppen har gått frem rent metodisk i arbeidet med å utarbeide og ferdigstille ROS-analysen. Dette kan innebære en beskrivelse av organisering av arbeidsgruppen, arbeidsmetode og vurderingsprosesser]

3.0 Analysedel

[Inndelingen i kapittel 3 er et forslag, og virksomhetene/tjenestestedene oppfordres til å justere hovedkategoriene etter hva som er hensiktsmessig]

3.1 Identifisering av hovedkategorier

[En beskrivelse av de hovedkategoriene relevante for virksomheten/tjenestestedet. Hovedkategoriene er store ulykker, naturhendelser, kritisk infrastruktur, helse og tilsiktede hendelser]

3.2 Hovedkategori 1

[Beskrivelse av hovedkategori 1, for eksempel store ulykker]

3.2.1 RISIKOOMRÅDE 1

[Beskrivelse av risikoområde 1 innenfor hovedkategori 1]

3.2.1.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.2.2 RISIKOOMRÅDE 2

[Beskrivelse av risikoområde innenfor hovedkategori 1]

3.2.2.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 2 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.2.3 OPPSUMMERING AV HOVEDKATEGORI 1

[En oppsummering av identifisert risiko innenfor hovedkategori 1]

3.3 HOVEDKATEGORI 2

[Beskrivelse av hovedkategori 2, for eksempel naturhendelser]

3.3.1 RISIKOOMRÅDE 1

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.3.1.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.3.2 RISIKOOMRÅDE 2

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.3.2.1 Scenarioanalyse

[Analyse av hendelsen med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.3.3 OPPSUMMERING AV HOVEDKATEGORI 2

[En oppsummering av identifisert risiko innenfor risikoområde 2]

3.4 HOVEDKATEGORI 3

[Beskrivelse av hovedkategori 3, for eksempel kritisk infrastruktur]

3.4.1 RISIKOOMRÅDE 1

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.4.1.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.4.2 RISIKOOMRÅDE 2

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.4.2.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.4.3 OPPSUMMERING AV HOVEDKATEGORI 3

[En oppsummering av identifisert risiko innenfor risikoområde 2]

3.5 HOVEDKATEGORI 4

[Beskrivelse av hovedkategori 4, for eksempel helse]

3.5.1 RISIKOOMRÅDE 1

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.5.1.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.5.2 RISIKOOMRÅDE 2

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.5.2.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.5.3 OPPSUMMERING AV HOVEDKATEGORI 4

[En oppsummering av identifisert risiko innenfor risikoområde 2]

3.6 HOVEDKATEGORI 5

[Beskrivelse av hovedkategori 5, for eksempel tilsiktede handlinger]

3.6.1 RISIKOOMRÅDE 1

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.6.1.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.6.2 RISIKOOMRÅDE 2

[Beskrivelse av risikoområde innenfor hovedkategori 2]

3.6.2.1 Scenarioanalyse

[Analyse av en alvorlig uønsket hendelse innenfor risikoområde 1 med analyse av sannsynlighet, konsekvens, usikkerhet og risikoreduserende tiltak]

3.6.3 OPPSUMMERING AV HOVEDKATEGORI 5

[En oppsummering av identifisert risiko innenfor risikoområde 2]

3.7 FREMSTILLING AV RISIKO- OG SÅRBARHETSBILDE

[Kan inneholde en oppsummering av alle identifiserte risikoer, gjerne visuelt fremstilt i tabeller eller diagrammer. Kan også gi en oversikt over hvilke tiltak som er identifisert, og hvordan de vil påvirke det samlede risikobildet]

4.0 RISIKOHÅNDTERING

[Dette kapittelet har til hensikt å forklare plan og strategi for oppfølging, og eventuelt beskrive hvilke risikoakseptkriterier som er lagt til grunn]

4.1 STRATEGI OG PLAN FOR OPPFØLGING

[Kan si noe om hvordan virksomheten planlegger å følge opp ROS-analysens funn]

4.2 RISIKOAKSEPTKRITERIER

[Kan si noe om de vurderingene som er blitt gjort relatert til å akseptere risiko, eller valg om å redusere den ved å implementere risikoreduserende tiltak]

4.3 PLAN FOR IMPLEMENTERING AV TILTAK

[Kan gi en mer konkret plan for hvordan virksomheten planlegger å implementere de risikoreduserende tiltakene som er identifisert, og som er besluttet å skulle implementeres. Det kan også inkluderes en beskrivelse av tidsperspektivet på dette arbeidet. Dette punktet er også nyttig med tanke på neste gang en ROS-analyse med lignende omfang gjennomføres, for å sikre en kontinuitet og sammenheng i ROS-analysene over tid]

5.0 KILDER OG REFERANSER

[I dette kapittelet fremlegges kilder og referanser til informasjonen som er lagt til grunn i analysen]

6.0 VEDLEGG

[I dette kapittelet vedlegges relevante vedlegg]