ROSmodellen

Introduktion og brugervejledning

Beredskabsstyrelsens model for risiko- og sårbarhedsanalyse

2006

Beredskabsstyrelsen

Indholdsfortegnelse

Denne introduktion og brugervejledning kan med fordel læses sideløbende med en første gennemlæsning af selve ROS-modellen. Det anbefales at benytte den elektroniske version eller papirudgaver printet ud i farver.

Vejledningen og ROS-modellen kan, sammen med de supplerende produkter *Scenariebanken* og *ROS*[60], findes på www.brs.dk/fagomraade/tilsyn/csb/ROS.htm. Materialet erstatter de tidligere versioner fra 2005.

Civil Sektors Beredskab kontoret bistår gerne interesserede parter direkte med træning i brug af ROS-modellen. På samme vis opfordres potentielle brugere til at dele deres erfaringer med kontoret [csb@brs.dk].

Introduktion til Beredskabsstyrelsens model for risiko- og sårbarhedsanalyse

Hvorfor bør myndigheder udarbejde risiko- og sårbarhedsanalyser?

Større forstyrrelser, ulykker og katastrofer vil aldrig helt kunne undgås, men de kan modvirkes ved hjælp af rettidig og helhedsorienteret beredskabsplanlægning. Herved forbedres mulighederne for at opretholde og videreføre samfundets kritiske funktioner. Risiko- og sårbarhedsanalyser er et vigtigt indledende trin i dette planlægningsarbejde.

Sektoransvaret i beredskabslovens § 24, stk. 1

Alle sektoransvarlige myndigheder har ansvar for at udarbejde relevant beredskabsplanlægning, jf. beredskabslovens § 24, stk. 1:

"De enkelte ministre skal hver inden for deres område planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af ulykker og katastrofer, herunder krigshandlinger, samt for at kunne yde støtte til forsvaret."

Risiko- og sårbarhedsanalysers formål og udbytte

Det overordnede formål med risiko- og sårbarhedsanalyser er at skabe grundlag for en målrettet og prioriteret beredskabsplanlægning. I denne sammenhæng kan analyserne give udbytte på en række områder:

- **et værktøj til at skabe overblik**

  Risiko- og sårbarhedsanalyser øger deltagernes viden og overblik. Et sådant overblik gør det nemmere at sætte individuelle trusler, risici og sårbarheder i forhold til hinanden og fokusere på faktorer, som kan påvirke organisationen eller ansvarsområdet kraftigst, herunder opretholdelsen og videreførelsen af kritiske funktioner.

- **et prioriteringsværktøj**

  Risiko- og sårbarhedsanalyser giver grundlag for at opstille prioriterede forslag til nye eller supplerende risiko- og sårbarhedsreducerede tiltag. På samme vis kan analyserne afdække overflødige foranstaltninger eller identificere mere effektive alternativer.

- **et værktøj til beslutningsstøtte**

  Risiko- og sårbarhedsanalyser bidrager til at give organisationens ledelse et solidt grundlag for at træffe beslutninger om beredskabsplanlægning. Hvis analyserne gennemføres regelmæssigt, kan de samtidig bidrage til, at beredskabsmæssige hensyn løbende integreres i organisationens øvrige planlægningsopgaver.

- **et koordinerings-værktøj** Risiko- og sårbarhedsanalyser kan bl.a. lægge op til, at organisationen forholder sig til afhængigheder og afledte konsekvenser. Analyserne kan dermed afdække risici og sårbarheder på tværs af samfundets sektorer, organisationer og kritiske funktioner. Viden om disse tværgående forhold kan bruges til at koordinere indsatsen i krydsfeltet mellem flere beredskabsansvarlige aktører.
- **et øvelsesværktøj** De anvendte trusselsscenarier kan danne grundlag for forskellige former for kompetenceudvikling, f.eks. krisestyringsøvelser.
- **et kommunikationsværktøj** Resultaterne af risiko- og sårbarhedsanalyser kan bruges til at kommunikere begrundelser for anbefalede eller iværksatte tiltag – både internt og eksternt. Herved øges tilliden blandt de ansatte og i det omgivende samfund til, at organisationen har et effektivt beredskab.

Introduktion

Principper i ROS-modellen

Beredskabsstyrelsen har udviklet denne generelt anvendelige model for risiko- og sårbarhedsanalyse (ROS-modellen) for at fremme, at danske myndigheder lægger risiko- og sårbarhedsvurderinger til grund for beredskabsmæssige prioriteringer.

Hensigten med modellen

Den primære hensigt med ROS-modellen er at stille et redskab til rådighed for myndigheder på det statslige niveau. Modellen kan dog i princippet anvendes af alle aktører med beredskabsansvar eller –opgaver; både offentlige og private organisationer. Potentielle brugere er velkomne til at anvende modellen i sin helhed, ændre dele af den til specifikke behov, eller blot bruge den som inspiration ved udvikling af alternative modeller.

Modellen lægger op til risiko- og sårbarhedsanalyser gennemført med et overordnet sigte frem for på detailniveau. Modellen skal derfor ikke erstatte andre, mere specialiserede analyseredskaber, som allerede er i brug. Den er derimod beregnet til organisationer, der ønsker et overordnet redskab til risiko- og sårbarhedsanalyse i forbindelse med deres beredskabsplanlægning.

Samfundets kritiske funktioner

Modellen er lagt an på at vurdere trusler, risici og sårbarheder i forhold til de funktioner, som er særlig kritiske for, at samfundet kan fungere effektivt, også under ulykker og katastrofer. Begrebet ”kritiske funktioner” betegner ***de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets funktionsdygtighed***, og derfor skal kunne opretholdes og videreføres under større ulykker eller katastrofer. Det kan være el-forsyning, fastnet-telefoni, hospitalsbehandling m.v.

Kvalitativ metode

ROS-modellen er hovedsageligt baseret på brug af kvalitative frem for kvantitative data. Det betyder, at arbejdet ikke vil være en rent objektiv proces. Man er nødt til at erkende, at risiko og sårbarhed i denne sammenhæng ofte er noget der ”opleves”, og at vurderingerne påvirkes af analysedeltagernes erfaringer, kompetencer og holdninger. Normative betragtninger kan således ikke undgås. Det er derfor væsentligt at fokusere på saglighed og gennemsigtighed, samt at man løbende sørger for at beskrive de overvejelser, som ligger til grund for vurderingerne undervejs i forløbet.

Indeksmetoden

Alle vurderinger foretages ved brug af indeksmetoden, hvor man angiver niveauet for sandsynlighed, konsekvenser og sårbarheder på en skala fra 1 til 5, hvor ”1” er bedst og ”5” er værst.

Introduktion

Tilrettelæggelse af analysen

Tilrettelæggelse af analysen

Tilrettelæggelse af en risiko- og sårbarhedsanalyse har stor betydning for det videre forløb. Tidsforbruget vil bl.a. afhænge af det valgte analyseniveau, detaljeringsgraden og de tilgængelige ressourcer. Skemaet i Bilag C kan eventuelt benyttes som udkast til individuelle aktivitets- og tidsplaner.

Ledelsens opbakning

Erfaringer fra arbejde med risiko- og sårbarhedsanalyser viser, at ledelsesforankring er væsentligt for et godt forløb. Det bør derfor sikres, at organisationens ledelse bakker op om projektet før analysearbejdet påbegyndes, og at ledelsen løbende inddrages i processen, f.eks. via en styregruppe.

Håndtering af følsomme oplysninger

Risiko- og sårbarhedsanalyser vil ofte indebære, at man inddrager følsomme oplysninger, eller at analyseresultaterne bør beskyttes. Man bør derfor allerede ved tilrettelæggelsen af analysen tage højde for eventuelle spørgsmål om fortrolighed og dokumentsikkerhed.

Team-baseret analysearbejde

ROS-modellen er designet med henblik på teambaseret analysearbejde, og deltagerne i den praktiske del af analysearbejdet er de vigtigste garanter for et troværdigt resultat. Det er derfor væsentligt at overveje, hvordan man vil sammensætte deltagerkredsen.

Antallet af deltagere afhænger bl.a. af ressourcer og ambitionsniveau, og det anbefales at nedsætte bredt funderede arbejdsgrupper, så man kan sikre både detailkendskab til området og tværgående faglighed. Man kan endvidere involvere eksterne eksperter og interessenter, blot man er opmærksom på, at en bred inddragelse også øger kompleksiteten i analysearbejdet.

Diskussion af metodik og definitioner

Før analysearbejdet påbegyndes er det vigtigt, at arbejdsgruppen diskuterer modellens metodik og begrebsapparat grundigt igennem (se Bilag D). Hvad der på overfladen kan forekomme at være rent teoretiske forskelle på begreber såsom ”trussel”, ”risiko” og ”’sårbarhed”, kan i praksis få stor betydning for analysens konklusioner og dermed også for arbejdsgruppens forslag til konkrete beredskabstiltag.

Introduktion

Det praktiske arbejde med ROS-modellen

Arbejd med modellen på pc og projektor

ROS-modellen består af fire skabeloner udarbejdet i Microsoft Word. Det er nemmest at arbejde elektronisk med skabelonerne. Det er ikke hensigtsmæssigt at bruge papirudgaver, fordi man så ikke kan anvende de rullemenuer m.v., der er indlagt i de elektroniske skabeloner. Arbejdet med at identificere og vurdere trusler, risici og sårbarheder sker i praksis ved, at man udfylder åbne tekstfelter og foretager valg vha. de foruddefinerede rullemenuer, afkrydsningsfelter m.v., der findes i skabelonerne.

Da arbejdet bør foregå teambaseret, kan det være en fordel at benytte projektor, så alle deltagerne kan se skabelonerne samtidigt.

Lås op for at tilpasse modellen

Skabelonerne skal være låste ved udfyldelsen. Det sikrer, at man kun kan skrive i de felter som er beregnet hertil, ligesom rullemenuer m.v. kun fungerer i denne tilstand. Det er muligt at ændre i originalteksten, hvis man ønsker at tilpasse modellen. Beskyttelsen af skabelonerne fjernes ved at højreklikke på menuen "Filer", vælge værktøjslinjen "Formularer" og derefter klikke på "hængelås-ikonet".

Overførsel af data mellem modellens dele

Skabelonerne indeholder ikke funktioner til automatisk overførsel af data mellem dokumenterne, så man må i visse tilfælde manuelt kopiere data i modellens skabeloner ved hjælp af "klip" og "sæt ind" funktionerne.

Introduktion

ROS-modellens opbygning

Modellens fire dele

ROS-modellen er opdelt i fire dele:

Del 1 – Udgangspunktet for analysen

Del 2 – Identifikation af trusler

Del 3 – Analyse af hvert enkelt trusselsscenarie

Del 4 – Risiko- og sårbarhedsprofil

Til støtte for analysen er der udarbejdet en skabelon til hver del i Microsoft Word. Under analysen skal der udfyldes ét dokument for del 1 og ét dokument for del 4, mens der i del 2 og del 3 skal udfyldes et dokument for hvert trusselsscenarie, der indgår i analysen.

Formål med del 1

I del 1 skal man identificere deltagerne i analysearbejdet, organisationens beredskabsansvar og de kritiske funktioner, som skal indgå i den konkrete risiko- og sårbarhedsanalyse (analysens objekt). Hvis man ønsker at foretage separate analyser for separate kritiske funktioner, eller for underliggende organisationer, kan det overvejes at bruge modellen flere gange blandt forskellige arbejdsgrupper.

Formål med del 2

ROS-modellen tager udgangspunkt i scenariebaserede analyser af ekstraordinære hændelser, som kan skade kritiske funktioner og resultere i tab af liv, velfærd, ejendom eller andre værdier. I del 2 skal man derfor opstille ét eller flere realistiske scenarier, som er repræsentative for det aktuelle trusselsbillede. Hvert scenarie skal efterfølgende analyseres i modellens del 3.

Hensigten med opstilling af scenarier er at få indsnævret feltet af potentielle trusler, så man kan fokusere på de områder, hvor indledende drøftelser peger på væsentlige risici og sårbarheder. Man skal således ikke udarbejde en ”totalliste” over alle tænkelige trusler.

Formål med del 3

I del 3 skal der foretages separate risiko- og sårbarhedsvurderinger for hvert af de scenarier, man har opstillet i del 2.

Indledningsvis skal man angive hvilke kritiske funktioner, der skal opretholdes og videreføres såfremt den pågældende type hændelse indtræffer. Derefter skal man vurdere henholdsvis sandsynligheden for at hændelsestypen vil kunne indtræffe, samt de konsekvenser dette ville medføre. Man når derved frem til et samlet risikoniveau. Endelig skal man vurdere de sårbarheder, der knytter sig til organisationens evne til at imødegå og håndtere den pågældende hændelsestype.

Formål med del 4

I del 4 skal man sammenstille analyseresultaterne fra de forskellige scenarieanalyser (del 3). Resultatet er en risiko- og sårbarhedsprofil, som giver et samlet overblik over hvilke hændelsestyper, der udgør den største fare.

I risikomatrixen placeres hver enkelt scenarie på baggrund af vurderingerne af sandsynlighed og konsekvenser. Det giver en overskuelig grafisk fremstilling af risikoniveau, hvor man kan sammenligne de forskellige scenarier med hinanden.

Sårbarhedsoversigten viser hvor relativt robust eller sårbart organisationens beredskab er i forhold til at imødegå og håndtere de hændelser scenarierne beskriver. Det sker på baggrund af vurderingerne af organisationens forskellige forberedelser, kapaciteter til indsats og afhjælpning samt kapaciteter til reetablering.

Trin for trin vejledning i modellens fire dele

Del 1: Udgangspunkt for analysen

Identificer og beskriv de kritiske funktioner (pkt. 3-4)

Som medlemmer af arbejdsgruppen skal I indledningsvis udfylde baggrundsoplysninger om jer selv (navn, stilling, ansættelsessted). Herefter skal I identificere og kort beskrive den eller de kritiske funktioner, som jeres organisation har beredskabsansvar for, og som risiko- og sårbarhedsanalysen skal omfatte.

"Kritiske funktioner" betegner ***de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets funktionsdygtighed***, og derfor skal kunne opretholdes og videreføres under større ulykker eller katastrofer. Det kan f.eks. være el-forsyning, fastnet-telefoni, hospitalsbehandling m.v. Til støtte for identifikationen er der i Bilag A opstillet en oversigt over samfundets kritiske funktioner.

Beredskabsansvar for kritiske funktioner følger af sektoransvarsprincippet, hvor den organisation, der har ansvaret for en funktion i det daglige, også har ansvaret i tilfælde af større ulykker og katastrofer. Vær opmærksom på, at jeres organisation også har overordnet beredskabsansvar for kritiske funktioner som er udliciteret.

Under udvælgelsen er det dog vigtigt, at I nøje overvejer hvilke funktioner, der reelt kan betegnes som 'kritiske' frem for blot 'vigtige'. Analyseopgaven kan let blive alt for omfattende, hvis I forsøger at vurdere mange funktioner på en gang.

Trin for trin

Del 2: Identifikation af trusler

Skabelon til trusselsscenarier

Modellens del 2 indeholder en skabelon til at opstille trusselsscenarier. Skabelonen angiver en række forhold, som I bør belyse for at få en dækkende beskrivelse af det konkrete scenarie. Scenariebeskrivelsen sikrer samtidig, at alle deltagere i analysen har et fælles udgangspunkt for den efterfølgende analyse.

Det er imidlertid vigtigt, at I gennemfører vurderingerne af sandsynlighed, konsekvenser og sårbarheder i modellens del 3 ud fra det pågældende scenaries overordnede tema (hændelsestypen) - ikke ud fra meget præcise detaljer i scenariebeskrivelsen såsom datoer, klokkeslæt, hændelsens udbredelse i antal km^2 m.v.

Del 2 indeholder kun én skabelon, som I skal kopiere i det antal, I har behov for. Skabelonen skal låses op før kopiering og låses igen, før den udfyldes (se tilpasning af modellen side 7).

Hvor mange trusselsscenarier?

I beslutter selv, hvor mange trusselsscenarier der skal anvendes, men af hensyn til arbejdsbyrden bør antallet ikke være for stort. Et godt formuleret scenarie sætter fokus på problemer, der også forekommer ved lignende hændelsesforløb.

Katalog over trusler

Vejledningens Bilag B indeholder et katalog over trusselskategorier, trusselstyper og eksempler, som I kan bruge til inspiration, når scenarierne skal opstilles.

Scenariebanken

Som udgangspunkt anbefales det, at I opstiller scenarier på egen hånd. Alternativt - eller som supplement hertil - kan I benytte Beredskabsstyrelsens scenariebank, se www.brs.dk/fagomraade/tilsyn/csb/ROS.htm

Scenariebanken indeholder en række foruddefinerede eksempler, som kan anvendes i deres eksisterende form eller justeres til jeres organisations konkrete kontekst og behov.

Ved tilpasning af ordlyden i Scenariebankens eksempler benyttes samme fremgangsmåde som ved tilpasning af ROS-modellens skabeloner, se side 7.

Anbefalinger vedrørende opstilling af trusselsscenarier

Et scenarie bør beskrive et sammenhængende hændelsesforløb, hvor konsekvenserne kan blive så alvorlige, at det kræver ekstraordinære beredskabsmæssige tiltag.

Alvorlige samfundsmæssige konsekvenser kan være:

- mange omkomne, kvæstede, syge og/eller udsatte personer
- meget stort pres på eller nedbrud i dele af samfundets kritiske funktioner

- store skader på miljøet
- massive tab af materielle eller finansielle værdier
- omfattende angst, utryghed, vrede eller harme i befolkningen og politiske implikationer.

Ekstraordinære beredskabsmæssige tiltag er typisk karakteriseret ved:

- anvendelse af faciliteter, ressourcer og kapaciteter i meget stort omfang
- inddragelse af infrastrukturberedskaber, krisestyringsorganisationer og andre aktører, som ikke er en del af det daglige beredskab.

- **Realistisk**

Scenariet bør være realistisk. Realismen kan bl.a. sikres ved at basere scenariet på hændelser (eller "næsten-hændelser"), som er observeret inden for egen sektor; i Danmark eller i udlandet. Alternativt kan scenariet baseres på en tænkt hændelse, som det frygtes vil kunne forekomme inden for overskuelig fremtid.

Idealet er at skitsere et hændelsesforløb, som ville medføre en væsentlig negativ påvirkning ("breaking point") af de kritiske funktioner, I har udpeget under afgrænsningen i modellens del 1. I bør således undgå at opstille scenarier for de absolut værst tænkelige, og dermed mest usandsynlige katastrofer ("worst case"). Omvendt må der heller ikke være tale om hyppige eller dagligdags hændelser.

Eksempler kunne være særligt alvorlige industriulykker, forureningsuheld, ekstreme vejrfænomener, sygdomsepidemier, forsyningssvigt, eller ondsindede menneskelige handlinger såsom kriminel sabotage eller terrorangreb.

- **Tilpas detaljeret**

Scenariet bør være beskrevet så detaljeret, som det er nødvendigt for at kunne analysere de tilknyttede risici og sårbarheder. Scenariet bør således indeholde beskrivelser af hvilken trusselskategori, der er tale om, samt detaljer om truslens karakter, omfang, varighed m.v. Overvej i denne sammenhæng, om det er mest hensigtsmæssigt at opstille specifikke eller generelle scenarier (fx "Brev med miltbrandsporer til X-styrelse" vs. "Terrorhandlinger mod offentlige myndigheder").

Trin for trin

Del 3: Analyse af trusselsscenarier

Opbygning af del 3

Skabelonen til del 3 indeholder fem afsnit: A, B, C, D og E. Hele del 3 skal udfyldes for hvert af de trusselsscenarier, som I har opstillet i del 2.

- I afsnit A anføres de kritiske funktioner i relation til det valgte scenarie (pkt. 1)
- I afsnit B vurderes sandsynligheden (pkt. 2)
- I afsnit C vurderes konsekvenserne (pkt. 3 – 7)
- I afsnit D fastsættes risikoniveauet ud fra vurderingerne i afsnit B og C (pkt. 8)
- I afsnit E vurderes sårbarhederne (pkt. 9 – 15)

Angivelse af niveauer

Alle vurderinger af niveauet for sandsynlighed, konsekvenser og sårbarheder i del 3 foretages ved brug af indeksmetoden, hvor man angiver på en skala fra 1 til 5, hvor ”1” er bedst og ”5” er værst. I skabelonen er skalaerne indbygget som rullemenuer.

Afsnit A

Kritiske funktioner

(pkt. 1)

Under pkt. 1 skal I mere præcist anføre, de kritiske funktioner jeres organisation har beredskabsansvar for at opretholde og videreføre i tilfælde af den hændelsestype, som scenariet beskriver. I bedes her fokusere på særligt væsentlige driftsopgaver og opgaver vedrørende krisehåndtering i relation til hændelsestypen.

Afsnit B

Vurdering af sandsynlighed

(pkt. 2)

Under pkt. 2 skal I vurdere sandsynligheden for, at hændelsestypen vil kunne indtræffe. Erfaringerne med ROS-modellen viser, at brugerne ofte vil finde det vanskeligt at vurdere sandsynligheden. Det er imidlertid vigtigt, at I forsøger, da sandsynlighedsvurderingen sammen med de efterfølgende konsekvensvurderinger skal anvendes til at fastsætte risikoniveauet for scenariet (pkt. 8).

Hyppighed eller plausibilitet?

Til støtte for sandsynlighedsvurderingen kan I basere jer på overvejelser om ”hyppighed”, dvs. hvor ofte hændelsen forventes at indtræffe, med udgangspunkt i egne eller andres erfaringer, historiske eller statistiske data m.v. For hændelser som aldrig eller kun sjældent er indtruffet, må der i stedet blot anvendes kvalificerede gæt på, hvor ”plausible” de er. Her kan I med fordel inddrage betragtninger om hændelsens bagvedliggende årsager og betingelser m.v.

Indeks til vurdering af sandsynlighed

1 = Meget usandsynlig

2 = Overvejende usandsynlig

3 = Sandsynlig

4 = Overvejende sandsynlig

5 = Meget sandsynlig

Afsnit C

Vurdering af konsekvenser

(pkt. 3 – 7)

Under pkt. 3 – 7 skal I vurdere de mulige konsekvenser af hændelsestypen for henholdsvis jeres egen organisation/ansvarsområde og for samfundet generelt. I begge tilfælde anvendes følgende indeks:

1 = Begrænsede

2 = Moderate

3 = Alvorlige

4 = Meget alvorlige

5 = Kritiske

Konsekvenser for egen organisation/ ansvarsområde

(pkt. 3 – 4)

Først skal I beskrive og vurdere hændelsestypens direkte konsekvenser for evnen til at opretholde og videreføre de kritiske funktioner, som I anførte i afsnit A (pkt. 1). Det kan eksempelvis vedrøre hændelsens påvirkning af bygninger og installationer, personale, nødvendige leverancer m.v.

I skal herefter fastsætte et samlet niveau for de konsekvenser, som hændelsestypen vil have for egen organisation/ansvarsområde. Niveauet fastsættes ud fra vurderingerne af konsekvenserne for de enkelte dele under pkt. 3 sammenholdt med de enkelte deles vigtighed for jeres organisation/ansvarsområde.

Konsekvenser for samfundet generelt

(pkt. 5 – 6)

Under pkt. 5 skal I beskrive og vurdere de generelle samfundsmæssige konsekvenser af hændelsestypen indenfor fire kategorier:

- Tab af liv og helbred
- Tab af aktiver (materielle, finansielle, miljømæssige m.v.)
- Angst, utryghed, vrede, harme eller politiske implikationer
- Afbrydelse af kritisk infrastruktur (f.eks. energi, transport, kommunikation osv.).

I skal i den forbindelse både se på de direkte konsekvenser og på de afledte konsekvenser, som kan opstå i samfundet pga. afhængigheder mellem organisationer, sektorer, kritiske funktioner m.v. Derefter skal I under pkt. 6 ud fra en samlet vurdering af ovenstående, fastsætte et samlet niveau for de samfundsmæssige konsekvenser.

Samlet vurdering af konsekvenser

(pkt. 7)

Under pkt. 7 fastsætter I hændelsestypens samlede konsekvenser ved at angive det højeste konsekvensniveau fra pkt. 4 og pkt. 6. Det bliver dermed det højeste konsekvensniveau, der slår igennem i det overordnede risikoniveau (pkt. 8).

Afsnit D

Trusselsscenariets risikoniveau

(pkt. 8)

Risikovurderingsfasen afsluttes med, at I fastsætter det overordnede risikoniveau for den analyserede hændelsestype. I gør dette ved at gange talværdien fra vurderingen af sandsynlighed fra pkt. 2 med talværdien fra den samlede vurdering af konsekvenser fra pkt. 7.

Afsnit E

Vurdering af sårbarheder

(pkt. 9 – 15)

I afsnit E skal I vurdere, hvor relativt robust eller sårbart jeres organisations beredskab er ud fra tre parametre:

- Forberedelser før hændelsen indtræffer (pkt. 9 – 11)
- Kapaciteter til indsats og afhjælpning under selve hændelsen (pkt. 12 – 13)
- Kapaciteter til reetablering efter hændelsen (pkt. 14 – 15)

Disse tre parametre bliver forklaret nærmere på side 16 – 17.

Af hensyn til analysens omfang skal I ikke kortlægge alle de tiltag, foranstaltninger og ressourcer, som jeres organisation kan trække på. I skal udelukkende koncentrere jer om de kapaciteter, som er relevante i forhold til den konkrete hændelsestype scenariet beskriver, og for de specifikke kritiske funktioner, som I identificerede i afsnit A.

Indeks til vurdering af sårbarheder

	Forberedelser Kapaciteter til indsats og afhjælpning Kapaciteter til reetablering		Overordnet sårbarhedsniveau
1	Tilstrækkelige	≈	Meget lav sårbarhed (robust)
2	Overvejende tilstrækkelige, få mangler	≈	Lav sårbarhed
3	Nogle alvorlige mangler	≈	Middel sårbarhed
4	Mange alvorlige mangler	≈	Høj sårbarhed
5	Helt utilstrækkelige	≈	Meget høj sårbarhed

Forberedelser:

(pkt. 9 – 11)

Under pkt. 9 – 10 skal I beskrive, hvordan jeres organisation har forberedt sig på at kunne håndtere hændelsestypen. Fokus er på de tiltag og foranstaltninger, som er mest relevante for organisationens "modstandskraft" før hændelsen er indtruffet.

Under pkt. 9 anfører I eksisterende forberedelser af planlægningsmæssig eller lignende art. Det kan f.eks. dreje sig om nedskrevne beredskabsplaner, krisekommunikationsplaner, erfaringsopsamlinger fra tidligere hændelser, afholdte beredskabsøvelser og uddannelsesaktiviteter, indgåede kontrakter og samarbejdsaftaler m.v.

Under pkt. 10 beskriver I de mere håndgribelige foranstaltninger, som enten kan forebygge at hændelsen indtræffer eller begrænse skaderne. De forebyggende eller skadesbegrænsende foranstaltninger kan f.eks. involvere fysisk adgangskontrol til bygninger, kameraovervågning, nødstrømsanlæg, redundante it-systemer m.v.

Overvej her især, om der er gennemført foranstaltninger, der sikrer de enkelte dele, som bidrager til at opretholde jeres organisations kritiske funktioner, herunder:

- Væsentlige bygninger, anlæg og andre fysiske installationer
- Medarbejdere og ledelse
- It-systemer
- Energiforsyning
- Tilgang af nødvendige materialer/varer/tjenesteydelser
- Transport/distribution
- Information og kommunikation.

Endelig skal I under pkt. 11 vurdere, hvor virkningsfulde de forberedelser I har beskrevet samlet set er i forhold til den pågældende hændelsestype.

Kapaciteter til indsats og afhjælpning

(pkt. 12 – 13)

Under punkt 12 skal I beskrive jeres organisations eksisterende kapacitet til akut indsats og afhjælpning, såfremt hændelsestypen indtræffer. Fokus begrænser sig til de af jeres kapaciteter, som er mest relevante, mens hændelsen forløber. Det kan bl.a. dreje sig om ledelse, personale, materiel, organisering, logistik, lagre, finansiering m.v. Under pkt. 13 vurderer I efterfølgende, hvor effektive de beskrevne kapaciteter samlet set er for jeres organisations evne til at håndtere hændelsestypen.

Kapaciteter til re-etablering

(pkt. 14 – 15)

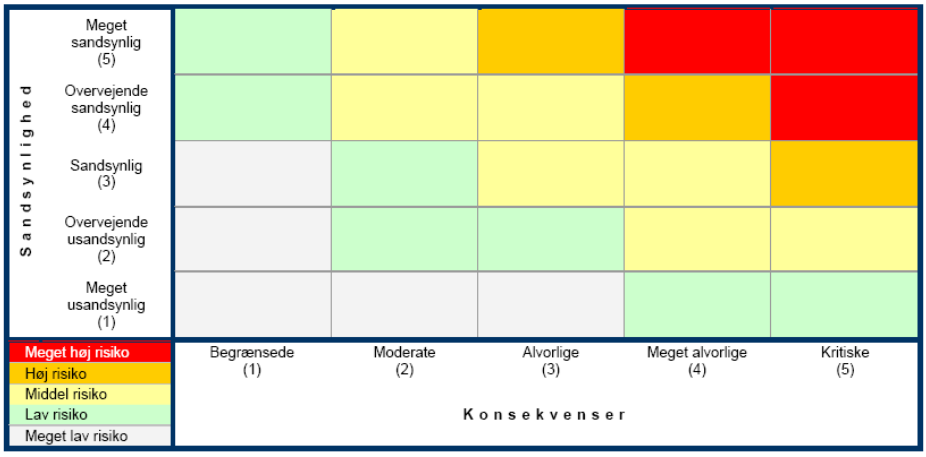
Under de sidste punkter i del 3 skal I først beskrive, og derefter samlet set vurdere, de kapaciteter jeres organisation råder over til reetablering på længere sigt. Fokus er her på de af jeres eksisterende kapaciteter, som er mest relevante for evnen til hurtigt at kunne vende tilbage til en normaltilstand efter hændelsestypen er indtruffet. Ligesom kapaciteterne til akut indsats og afhjælpning, kan kapaciteterne til reetablering omfatte faktorer såsom ledelse, personale, materiel, organisering, logistik, lagre, finansiering m.v.

Trin for trin

Del 4: Risiko- og sårbarhedsprofil

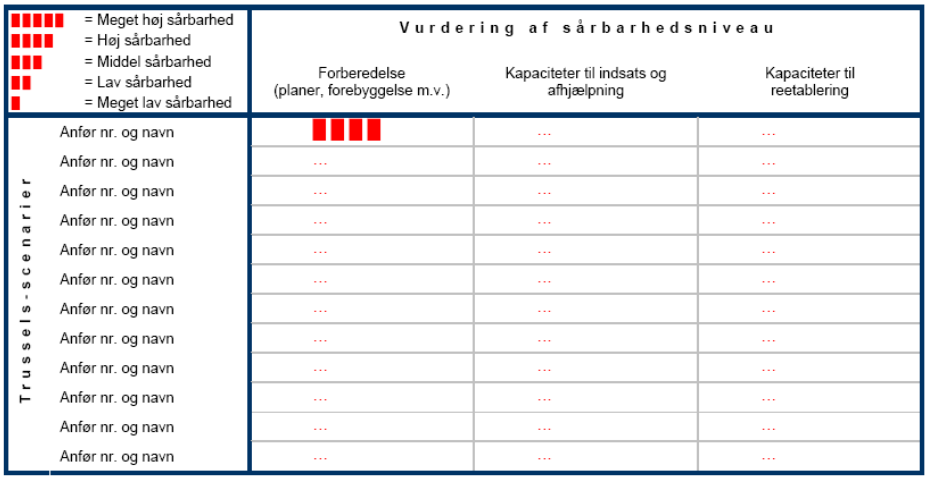
Risikomatrix

I risikomatrixen skal I placere hvert enkelt trusselsscenarie på baggrund af dets samlede risikoniveau (del 3 pkt. 8). Det fremmer overblikket, hvis I skriver både titler og numre på scenarierne i matrixen.



Sårbarhedsoversigt

I sårbarhedsoversigten skal I for hvert scenarie angive sårbarhedsniveauerne for henholdsvis forberedelser (del 3 pkt. 11), kapaciteter til indsats og afhjælpning (del 3 pkt.13) samt kapaciteter til reetablering (del 3 pkt. 15).



Sammenlagt giver profilen en overskuelig grafisk fremstilling over hvilke trussels-scenarier, der er forbundet med de største risici og sårbarheder, og som I bør overveje at iværksætte nye eller supplerende tiltag imod. Risiko- og sårbarheds-profilen kan dog ikke stå alene. Den bør som minimum ledsages af et notat, der beskriver de vigtigste forhold analysen har afdækket (se side 21).

Gennemgå og revurder resultaterne

Risici og sårbarheder indgår i vekselvirkning med hinanden, og vurderinger heraf bør ideelt set ikke holdes adskilt. Både sandsynlighed og konsekvenser af en given trussel påvirkes af hvor sårbart eller robust det system, som truslen retter sig imod, er. Under arbejdet med del 4 anbefales I derfor at se tilbage på analyseresultaterne i del 3, og om nødvendigt foretage justeringer ud fra ændrede antagelser. Dette gælder i særlig grad de valgte talværdier i rullemenuerne, som er styrende for de enkelte scenariers placering i risiko- og sårbarhedsprofilen, og dermed for sammenligningsgrundlaget.

Introduktion

Opfølgning på analysen

Forslag til risiko- og sårbarhedsreducerende tiltag

Brug af ROS-modellen bør ideelt set resultere i prioriterede anbefalinger til risiko- og sårbarhedsreducerende tiltag. Da det hverken er praktisk eller økonomisk muligt at imødegå alle trusler, er opgaven at udvælge de potentielt mest effektive tiltag over for de væsentligste risici og sårbarheder, som analysen har kortlagt.

Risikoreducerende tiltag retter sig primært mod selve truslerne og omfatter både forebyggende tiltag, som forhindrer eller reducerer sandsynligheden for at en specifik hændelse indtræffer, og skadesbegrænsende tiltag, som kan reducere konsekvenserne såfremt hændelsen alligevel indtræffer.

Sårbarhedsreducerede tiltag retter sig primært mod interne karakteristika ved et givet system, og omfatter foranstaltninger som kan styrke dets generelle evne til at modstå trusler og fungere optimalt. Disse tiltag kan forbedre kapaciteterne til at planlægge for uønskede hændelser; forebygge eller reducere skader og tab; og sikre en hurtig indsats, afhjælpning og genoprettelse af kritiske funktioner.

For langt de fleste trusler vil der både kunne iværksættes risikoreducerende og sårbarhedsreducerende tiltag, og grænsen mellem de to typer er i praksis flydende. Eksempler kan være forøget overvågning af trusselsbilledet, investeringer i nyt materiel, uddannelses- og øvelsesaktiviteter, ajourføring af beredskabsplaner, beredskabsrelevante krav ved udlicitering, oplæg til ny lovgivning m.v.

Prioritering af tiltag

Der kan med fordel i første omgang udarbejdes en 'bruttoliste' over mulige tiltag. Herudfra kan der så efterfølgende opstilles en prioriteret 'nettoliste' med de mest anbefalelsesværdige og gennemførlige tiltag. I forhold til hvert tiltag kan det være hensigtsmæssigt at overveje spørgsmål såsom:

- Hvad er rationalet bag tiltaget?
- Hvilke konkrete opgaver ligger der i tiltaget?
- Hvad er tidsrammen for tiltaget?
- Hvad er succeskriterierne for tiltaget?
- Er der synergieffekter i forhold til andre tiltag?
- Hvad er de økonomiske konsekvenser af tiltaget?
- Er der en tydelig sammenhæng mellem omkostninger og effekt?

Konklusionsrapport og beslutningsoplæg

Efter at de anbefalede tiltag er blevet formuleret og prioriteret, bør resultaterne af den samlede analyseproces sammenfattes i en konklusionsrapport. Heri bør det også skitseres, hvor de største usikkerheder, afgrænsninger og forenklinger i analysen er forekommet, og hvor der derfor kan være behov for mere detaljerede undersøgelser. Rapporten bør så vidt muligt udarbejdes i et standardformat, således at den kan bruges ved kvalitetssikring og til brug for fremtidige analyser.

I forlængelse af konklusionsrapporten bør der afslutningsvist udarbejdes et kort beslutningsoplæg til organisationens ledelse, hvor de centrale konklusioner og anbefalinger samles. Herefter er det op til ledelsen at sikre at analyseresultaterne integreres i den videre beredskabsplanlægning, og om de foreslåede tiltag implementeres. Ledelsen kan f.eks. gøre dette via en handlingsplan som skitserer:

- Hvilke tiltag skal implementeres, hvor og hvornår (opgaver)?
- Ud fra hvilke anbefalinger (rationale)?
- Hvem skal implementere tiltagene (ansvar)?
- Hvor mange midler skal bruges (ressourcer)?

Opdatering af analysen

En risiko- og sårbarhedsanalyse kan være enkeltstående og situationsbetinget, men den bør ideelt set gennemføres med faste intervaller, når trusselsbilledet forandrer sig væsentligt, eller når indtrufne hændelser eller større organisatoriske ændringer tilsiger det. Ansvaret for opdatering kan med fordel forankres i én organisatorisk enhed. Ajourføringen bør endvidere tilrettelægges, så den ikke afbryder de daglige processer, men finder sted som et naturligt element i organisationens beredskabsplanlægning.

Bilag A. Oversigt over samfundets kritiske funktioner

”Samfundets kritiske funktioner” betegner de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets funktionsdygtighed, og derfor skal kunne opretholdes og videreføres under større ulykker eller katastrofer.

Sektorer	Kritiske funktioner	Sektorer	Kritiske funktioner
Energi	▫ Elforsyning ▫ Gasforsyning ▫ Olie- og benzinforsyning	**Beredskaber**	▫ Alarmering og varsling ▫ Politiopgaver ▫ Brandslukning ▫ Redning (land/sø/luft/) ▫ Evakuering, modtagelse, indkvartering og forplejning ▫ Præhospital indsats ▫ Kemisk beredskab ▫ Biologisk beredskab ▫ Radiologisk beredskab ▫ Nukleart beredskab ▫ Ammunitionsrydning ▫ Stormflodsberedskab ▫ Miljøberedskab ▫ Militær hjælp til civile myndigheder
Kommunikation og it	▫ Fastnet-telefoni ▫ Mobil-telefoni ▫ Databehandling og datatransmission ▫ Informationsnetværk ▫ Internetadgang ▫ Tv- satellit- og radiotransmission ▫ Navigation ▫ Post- og kurérservice		
Transport	▫ Afvikling, overvågning og kontrol af persontrafik og godstransport (vej, bane, luft, sø) ▫ Overvågning og kontrol af infrastruktur (broer, tunneller, lufthavne, stationer, havne m.v.)		
Finans og økonomi	▫ Betalingsformidling og pengeoverførsler ▫ Bank- og forsikringsvirksomhed ▫ Værdipapirhandel ▫ Centralbankfunktioner	**Sundhed**	▫ Primær sundhedsbehandling ▫ Hospitalsbehandling ▫ Omsorg for udsatte personer ▫ Overvågning af smitsomme sygdomme ▫ Lægemiddelberedskab ▫ Lægemiddelproduktion
Fødevarer	▫ Fødevareforsyning ▫ Overvågning af fødevaresikkerhed ▫ Overvågning af smitsomme husdyrsygdomme	**Offentlig forvaltning**	▫ Krisestyringskapacitet ▫ Opretholdelse af Folketingets, regeringens og centraladministrationens, domstolenes samt kommunernes myndighedsudøvelse
Vand	▫ Drikkevandsforsyning ▫ Transport og rensning af spildevand	**National sikkerhed**	▫ Bevogtning og overvågning af nøglepunkter og grænser ▫ Militært forsvar og suverænitetshåndhævelse ▫ Efterretningsopgaver ▫ Kontraterror ▫ Personbeskyttelse
Farlige stoffer	▫ Kontrol med produktion, opbevaring og transport af farlige stoffer (kemiske, biologiske, radiologiske og nukleare)		

Bilag B. Katalog over trusler

Trusselskategorier/ -typer	*Eksempler*
Ekstreme naturfænomener	
Atmosfæriske trusler	Orkan, snestorm, isvinter, islag, tæt tåge, skybrud, isstorm, saltstorm, lynnedslag
Geologiske trusler	Jordskred, erosion
Oceanografiske trusler	Stormflod, oversvømmelse, havis
Naturkatastrofer i udlandet	Jordskælv, vulkanudbrud, tsunami, cyklon, tornado, orkan
Terrorisme	
Terrorhandlinger mod myndigheders/aktørers aktiver eller ansatte	Konventionelle våben, CBRN-våben (kemiske, biologiske, radiologiske og nukleare), cyber-terror
Terrorhandlinger i Danmark	Konventionelle våben, CBRN-våben, cyber-terror
Terrorhandlinger i udlandet	Konventionelle våben, CBRN-våben, cyber-terror
Transportulykker (havari, brand, eksplosion)	
Sø	Passagerskibe, bulk-, container og tankskibe, militære fartøjer
Luft	Passagerfly, fragtfly, militærfly
Bane	Passagertog, godstog
Vej	Biler, busser, lastbiler
Uheld med eller udslip af farlige/forurenende stoffer	
Kemiske stoffer	Kemikalier, gas, olie og olieprodukter, benzin, toksiner
Biologiske stoffer	Bakterier, virus, toksiner
Radiologiske og nukleare stoffer	Radioaktiv bestråling
Eksplosiver	Sprængstoffer, fyrværkeri, ammunition
Brande og eksplosioner	
Bygninger/områder med mange mennesker	Høje bygninger, storcentre, teatre, biografer, diskoteker, haller, stadions, konferencecentre, hoteller, plejehjem, hospitaler, fængsler, institutioner, festivaler, markeder, stævner
Industri (produktion, distribution, lager m.v.)	"Seveso-virksomheder", miljø/brandfarlige virksomheder, oplag af brandfarlige/eksplosive stoffer
Infrastruktur	Banegårde, lufthavne, tunneller, havne
Natur	Skov, hede, mark
Kulturværdier	Slotte, museer, fredede bygninger, kirker, gamle bykvarterer
Sygdomme og epidemier	
Menneskelige sygdomme	Bakterier, virus, giftstoffer
Husdyrsygdomme	Bakterier, virus, giftstoffer

Trusselskategorier/ -typer	*Eksempler*
Plantesygdomme	Bakterier, virus, giftstoffer
Ødelæggelse, afbrud eller andet svigt af samfundets kritiske funktioner	
Energi	Elforsyning, gasforsyning, olie- og benzinforsyning
Kommunikation og it	Fastnet-telefoni, mobil-telefoni, databehandling og datatransmission, informationsnetværk, internetadgang, tv- satellit- og radiotransmission, navigation, post- og kurérservice
Transport	Afvikling, overvågning og kontrol af persontrafik og godstransport (vej, bane, luft, sø). Overvågning og kontrol af infrastruktur (broer, tunneller, lufthavne, stationer, havne m.v.)
Finans og økonomi	Betalingsformidling og pengeoverførsler, bank- og forsikringsvirksomhed, værdipapirhandel, centralbankfunktioner
Fødevarer	Fødevareforsyning, overvågning af fødevaresikkerhed, overvågning af smitsomme husdyrsygdomme
Vand	Drikkevandsforsyning, transport og rensning af spildevand
Farlige stoffer	Kontrol med produktion, opbevaring, transport og af farlige stoffer (kemiske, biologiske, radiologiske og nukleare)
Beredskaber	Alarmering og varsling, politiopgaver, brandslukning, redning (land/sø/luft), evakuering (inkl. modtagelse, indkvartering og forplejning), præhospital indsats, kemisk beredskab, biologisk beredskab, radiologisk beredskab, nukleart beredskab, ammunitionsrydning, stormflodsberedskab, miljøberedskab, militær hjælp til civile myndigheder
Sundhed	Primær sundhedsbehandling, hospitalsbehandling, omsorg for udsatte personer, overvågning af smitsomme sygdomme, lægemiddelberedskab, lægemiddelproduktion
Offentlig forvaltning	Krisestyringskapacitet, opretholdelse af folketingets, regeringens og centraladministrationens, domstolenes samt kommunernes myndighedsudøvelse
National sikkerhed	Bevogtning og overvågning af nøglepunkter og grænser, militært forsvar og suverænitetshåndhævelse, efterretningsopgaver, kontraterror, personbeskyttelse
Andre trusler	
Kriminalitet	It-angreb, hærværk/sabotage, industrispionage, kidnapning/afpresning, mord/overfald
Uroligheder	Optøjer/nedbrud af offentlig orden, omfattende demonstrationer, pludselige massive befolkningsbevægelser, større strejker/blokader
Udslip af farlige stoffer i Danmarks nærområde	Ulykker på atomkraftværker eller kemiske udslip
Sammenstyrtninger	Store bygninger, stadions, trafikanlæg
Nedstyrtninger	Satellitter, meteorer

Bilag C. Forslag til aktivitets- og tidsplan

Fase I: Forberedelse af analysen	**Termin**
Overvej analysens mål, niveau, afgrænsning og succeskriterier.	
Nedsæt den eller de arbejdsgrupper som skal stå for analysearbejdet samt eventuelt en styregruppe.	
Afhold et indledende møde vedrørende modellens indhold, begrebsapparat, metode m.v.	
Fastsæt en møderække, og påbegynd indsamling af relevant information til brug for analysen. Konsulter eventuelt eksterne eksperter og interessenter.	
Fase II: Udførelse af analysen ved hjælp af ROS-modellen	**Termin**
Udfyld modellens del 1: Baggrundsoplysninger, afgrænsning af kritiske funktioner, beredskabsansvar og analysefokus.	
Udfyld modellens del 2: Opstil et passende antal trusselsscenarier.	
Udfyld modellens del 3: Udfør risiko- og sårbarhedsvurderinger for hvert scenarie.	
Udfyld modellens del 4: Opstil risiko- og sårbarhedsprofilen. Diskuter resultaterne og gå om nødvendigt tilbage til del 3 og foretag justeringer ud fra ændrede antagelser.	
Fase III: Opfølgning på analysen	**Termin**
Identificer en ”bruttoliste” over mulige risiko- og sårbarhedsreducerende tiltag. Udarbejd derefter en prioriteret ”nettoliste”, hvor antallet begrænses til de umiddelbart mest effektive og realistisk gennemførlige tiltag.	
Udarbejd en konklusionsrapport ud fra den samlede analyse og nettolisten over anbefalede tiltag. Identificer samtidig hvor de største usikkerheder i analysen befinder sig, og dokumenter arbejdsprocessen som kvalitetssikring. Suppler eventuelt med drøftelser af ”tolerancekriterier” for acceptable risici og sårbarheder samt foreløbige økonomiske beregninger for de anbefalede tiltag.	
Udarbejd et kort beslutningsoplæg omhandlende de vigtigste trusler, risici, sårbarheder og forslag til modforanstaltninger. Fokuser eksklusivt på hvad ledelsen bedes træffe beslutning om, hvornår og ud fra hvilket rationale. Suppler eventuelt med et udkast til handlingsplan indeholdende konkrete opgaver, ansvarlige enheder/personer, tidsrammer, budgetter m.v.	

Bilag D. Modellens centrale begreber

Risiko- og sårbarhedsanalyse er en systematisk metode til at identificere og vurdere trusler, risici og sårbarheder med henblik på at skabe et overblik og beslutningsgrundlag vedr. mulige modforanstaltninger. Principielt kan man tale om enten risikoanalyse eller sårbarhedsanalyse. En risikoanalyse vurderer traditionelt ydre truslers sandsynlighed og deres mulige konsekvenser, mens en sårbarhedsanalyse typisk vurderer et systems interne styrker og svagheder. I praksis inddrager den ene type analyse dog uundgåeligt elementer fra den anden. Et system kan kun beskrives som sårbart, hvis der er trusler rettet mod det, mens en trussel kun repræsenterer en risiko, hvis der er sårbarheder, som truslen kan udnytte.

Samfundets kritiske funktioner består af de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets funktionsdygtighed, og derfor skal kunne opretholdes og videreføres under større ulykker eller katastrofer. I bilag A findes en oversigt med 11 overordnede sektorer og et større antal delmængder af kritiske funktioner.

Trussel refererer til en potentiel uønsket hændelse eller anden negativ påvirkning. Trusler kan være naturskabte, menneskeskabte eller teknologiske. De kan være tilsigtede eller tilfældige; varslede eller uvarslede. Et trusselsscenarie er et tænkt hændelsesforløb, hvori én eller flere trusler udspiller sig. Trusselsidentifikation stiller spørgsmål vedrørende en given trussels karakteristika, årsag, kilde og mål, men ikke vedrørende truslens sandsynlighed og konsekvenser. Det gøres i den efterfølgende risikovurdering.

Risiko er kombinationen af sandsynligheden for og de mulige konsekvenser af, at trusler virkeliggøres. Et risikoniveau udtrykker således den fare som en specifik trussel repræsenterer for et givet system. Både sandsynlighed og mulige konsekvenser påvirkes imidlertid også af sårbarheder inden for det system, truslen retter sig mod. Risikovurdering bør derfor ideelt set ikke foretages isoleret, men bør ske ved at indregne den relative grad af sårbarhed/robusthed i vurderingerne af sandsynlighed og mulige konsekvenser.

Sandsynlighed og konsekvenser kan vurderes enten kvantitativt eller kvalitativt. Konsekvensvurdering refererer til omfanget, udbredelsen og varigheden af tab og skader på liv, velfærd, kritiske funktioner, ejendom, miljø eller andre værdier. Sandsynlighedsvurdering kan foretages ved hjælp af indikationer på hyppighed (frekvens) eller ”plausibilitet” (kvalificerede gæt). Det sidste vil især være tilfældet, hvad angår menneskeskabte trusler, som er svære eller direkte umulige at forudsige med nogen særlig nøjagtighed.

Sårbarhed (og dets modpart robusthed) udtrykker et givet systems generelle evne til at fungere og opnå sine mål, når det udsættes for trusler. Et system er sårbart, når det mangler eller har reduceret kapacitet til at planlægge imod, forhindre, begrænse, afhjælpe eller overleve en realiseret trussel. Sårbarhedsvurdering sker ved at sætte trusler i forhold til eksisterende modforanstaltninger, kapaciteter og den foretrukne grad af beskyttelse.

Bilag E. Modellens udvikling og metodik

Oprindelsen til ROS-modellen er National Sårbarhedsudredning fra 2004, som anbefalede at der blev udviklet en generelt anvendelig model for risiko- og sårbarhedsanalyse til brug for myndighedernes beredskabsplanlægning.

Under forberedelserne til udviklingen af ROS-modellen hentede Beredskabsstyrelsens kontor Civil Sektors Beredskab inspiration i den omfattende internationale 'risk management' litteratur. Et af de primære resultater af denne research var ønsket om at udvikle et elektronisk værktøj, eftersom skrevne guidelines og vejledninger kan være svære at operationalisere i praksis.

For at sikre at potentielle brugerbehov blev tilgodeset, nedsatte kontoret i 2005 en fokusgruppe med deltagelse fra Energistyrelsen, Energinet.dk, IT- og Telestyrelsen og Politiets Efterretningstjeneste.

Den første version af ROS-modellen blev offentliggjort i november 2005. Efterfølgende justeringer er bl.a. blevet foretaget på baggrund af et ekspertseminar afholdt med samarbejdspartnere fra Storbritannien, Tyskland, Sverige, Norge og Finland; erfaringer fra en ROS-workshop med beredskabsansvarlige aktører på Bornholm; samt feedback fra en række andre aktuelle eller potentielle brugere af modellen. På den baggrund blev den gældende 2. version af ROS-modellen udgivet i efteråret 2006.

Modellens metodik er primært baseret på 'Preliminary Hazard Analysis' (PrHA)[1]. Fordelene er bl.a. at PrHA:

- Kan anvendes i forbindelse med overordnede analyser af de fleste typer organisationer, funktioner m.v.
- Ikke kræver at brugerne har forudgående metodisk kendskab til risiko- og sårbarhedsanalyser.
- Hovedsageligt baserer sig på struktureret brainstorming og kvalitative ekspertvurderinger, og derfor kan gennemføres, selvom brugerne ikke har detaljerede tekniske eller statistiske informationer.
- Kan udføres af en relativt lille gruppe personer ved hjælp af projektmøder og eventuelt inspektioner.
- Kan gennemføres med udgangspunkt i checklister.

Derudover er ROS-modellen kendetegnet ved en 'all-hazards approach'. Det vil sige, at modellen i princippet kan tage højde for alle typer af trusler og farer, uanset karakter, årsag, tid og sted. Hermed tilsigter modellen samtidigt et helhedsorienteret fokus på både forebyggelse, kapacitetsopbygning og konsekvenshåndtering.

Det bør endvidere fremhæves, at ROS-modellen tilstræber analyseresultater, der kan indgå i overordnede beredskabsplaner, selvom modellen selv baserer sig på analyse af konkrete trusselsscenarier. Hermed tilstræber modellen en tilgang, hvor scenarieplanlægning ('contingency planning') komplementerer den mere generelle planlægning for videreførelse af samfundets kritiske funktioner ('continuity planning').

[1] For yderligere information om PrHA og alternative metoder relateret til risiko- og sårbarhedsanalyser kan der eksempelvis henvises til: http://www.uscg.mil/hq/gm/risk/e%2Dguidelines/rbdm/html/vol3/00/v3-00.htm