ROS-modellen

Introduktion og brugervejledning



Beredskabsstyrelsens model for risiko- og sårbarhedsanalyse

November 2023

# Indledning

## Baggrund og formål

Større forstyrrelser, ulykker og katastrofer vil aldrig helt kunne undgås, men deres konsekvenser kan begrænses og afhjælpes ved hjælp af rettidig og helhedsorienteret beredskabsplanlægning. Herved forbedres mulighederne for at opretholde og videreføre samfundsvigtige og forretningskritiske funktioner. Risiko- og sårbarhedsanalyser er et vigtigt indledende trin i dette planlægningsarbejde.

Alle sektoransvarlige myndigheder har ansvar for at foretage 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 større ulykker og katastrofer, herunder udarbejde beredskabsplaner.”***

Det overordnede formål med risiko- og sårbarhedsanalyser er at skabe et stærkt grundlag for en målrettet og prioriteret beredskabsplanlægning. I denne sammenhæng kan ROS-modellen bruges til flere forskellige formål:

* **Et værktøj til at skabe 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 of videreførelsen af samfundsvigtige funktioner.
* **Et prioriteringsværktøj**: Risiko- og sårbarhedsanalyser giver grundlag for at opstille prioriterede forslag til nye eller supplerende risiko- og sårbarhedsreducerende tiltag. På samme vis kan analyserne afdække overflødige foranstaltninger eller identificere mere effektive alternativer.
* **Et værktøj til beslutningsstøtte**: Risiko- og sårbarhedsanalyser bidrager endvidere 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, samt at der skabes og opretholdes en stærk beredskabskultur.
* **Et koordineringsværktøj**: Risiko- og sårbarhedsanalyser kan bl.a. lægge op til, at organisationen forholder sig til afhængigheder og afledte konsekvenser. Analyserne kan dermed afdække trusler, risici og sårbarheder på tværs af samfundets sektorer, organisationer og samfundsvigtige funktioner. Viden om disse tværgående forhold kan bruges til at koordinere indsatsen i krydsfeltet mellem flere beredskabsansvarlige aktører og er afgørende for arbejdet i tværgående krisestyringsfora.
* **Et øvelsesværktøj**: De anvendte scenarier kan danne grundlag for forskellige former for kompetenceudvikling, fx 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.

## Principper i ROS-modellen

### Hensigten med modellen

Den primære hensigt med ROS-modellen er at stille et redskab til rådighed for offentlige myndigheder samt private virksomheder, og især myndigheder og virksomheder med ansvar for samfundsvigtige funktioner og underlagt kritisk infrastruktur. Modellen kan dog i princippet anvendes af alle aktører med beredskabsansvar eller -opgaver. I så fald kan organisationen rette fokusset mod forretningskritiske funktioner. Potentielle brugere kan anvende modellen i sin helhed, ændre dele af den til specifikke behov, eller blot bruge den som inspiration ved udvikling af alternative metoder.

Modellen lægger op til risiko- og sårbarhedsanalyser, der tegner et *generelt* billede af de trusler og risici, som kan ramme organisationen med henblik på at kortlægge organisationens sårbarheder. Modellen skal derfor ikke erstatte andre, mere specialiserede analyseredskaber, som allerede er i brug. Den er derimod beregnet til organisationer, der ønsker at styrke deres robusthed i forbindelse med deres beredskabsplanlægning.

1. *Samfundsvigtige funktioner, kritisk infrastruktur og forretningskritiske funktioner*

Modellen er lagt an på at vurdere trusler, risici og sårbarheder i forhold til kritisk infrastruktur og de funktioner, som er særlig kritiske for, at samfundet kan fungere effektivt, også under ulykker og katastrofer (dvs. samfundsvigtige funktioner). Begrebet *samfundsvigtige funktioner* betegner ”de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed”, og derfor skal kunne opretholdes og videreføres under større ulykker eller katastrofer. En oversigt over samfundsvigtige funktioner findes i bilag A. *Kritisk infrastruktur* defineres jf. den officielle danske definition som”infrastruktur – herunder faciliteter, systemer, processer, netværk, teknologier, aktiver samt serviceydelser – som er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner.”

Som nævnt ovenfor kan organisationer, som ikke har ansvar for samfundsvigtige funktioner eller kritisk infrastruktur også bruge dette værktøj til risiko- og sårbarhedsanalyser. I så fald vil der være tale om *forretningskritiske funktioner*, eller de funktioner, der er nødvendige for at organisationen kan opretholde sin virksomheds drift og dermed kritiske leverancer på et acceptabelt niveau, eller funktioner, hvis mangel vanskeliggør overholdelse af organisationens forvaltningsmæssige forpligtelser.

### Metoder

ROS-modellen er hovedsagligt et kvalitativt værktøj. Arbejdet kan derfor ikke ses som en rent objektiv proces, men nærmere en proces, hvori man identificerer, vurderer og sammenfatter organisationens opfattelse af forskellige risici og trusler. I det konkrete arbejde kan man forvente, at vurderingerne påvirkes af analysedeltagernes erfaringer, kompetencer og holdninger. Disse normative betragtninger kan (og bør) ikke undgås. I stedet for anbefales det at fokusere på gennemsigtighed – altså at beskrive, hvilke antagelser, erfaringer og oplevelser, der lægges til grund for hver enkelt vurdering – og løbende at beskrive disse overvejelser.

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’.

## 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. Det anbefales at bruge bilag C til inspiration til organisationens konkrete aktivitets- og tidsplaner.

Erfaringer fra arbejde med risiko- og sårbarhedsanalyser viser, at ledelsesforankring er væsentligt for et godt forløb. Derfor kan det med fordel sikres, at organisationens ledelse bakker op om analyseprocessen inden påbegyndelse af analysearbejdet, og at ledelsen løbende inddrages i processen, fx via en styregruppe.

### Teambaseret analysearbejde

ROS-modellen er designet med henblik på en fælles dialogbaseret analyseproces. Deltagerne er derfor de vigtigste garanter for et godt og retvisende resultat.

Antallet af deltagere afhænger bl.a. af ressourcer og ambitionsniveau, og det anbefales at nedsætte bredt funderede grupper, så man kan sikre både detailkendskab til området og tværgående faglighed. Man kan endvidere involvere eksterne eksperter og interessenter i det omfang deres ekspertise vurderes relevant for analysen.

Før analysearbejdet påbegyndes kan analysegruppen med fordel drøfte egne forståelse af modellens metodik og nøglebegreber (se evt. 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 analysegruppens forslag til konkrete beredskabstiltag.

## Det praktiske arbejde med ROS-modellen

ROS-modellen består af fire skabeloner udarbejdet i Word-format. Det anbefales, at analysegruppen arbejder med disse skabeloner elektronisk, da dokumenter indeholder en række funktioner (fx foruddefinerede rullemenuer, tekstfelter), som ikke kan bruges i papirform.

### 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 afklare spørgsmål om fortrolighed og dokumentsikkerhed.

## ROS-modellens opbygning

ROS-modellen er opdelt i fire trin:

* **Trin 1:** Udgangspunktet for analysen
* **Trin 2:** Identifikation af risici og trusler
* **Trin 3:** Analyse af hvert enkelt scenarie
* **Trin 4:** Risiko- og sårbarhedsprofil

Under analysen skal der udfyldes ét dokument for trin 1 og ét dokument for trin 4, mens der på trin 2 og 3 skal udfyldes et dokument for hvert scenarie, der indgår i analysen.

### Trin 1: Udgangspunkt for analysen

På trin 1 skal I identificere deltagerne i analysearbejdet, organisationens beredskabsansvar og de samfundsvigtige eller forretningskritiske funktioner, som skal indgå i den endelige risiko- og sårbarhedsanalyse. Hvis I ønsker at foretage separate analyser for separate samfundsvigtige eller forretningskritiske funktioner, eller for underliggende organisationer, kan det overvejes at bruge modellen flere gange blandt forskellige arbejdsgrupper.

### Trin 2: Identifikation af trusler

ROS-modellen tager udgangspunkt i scenariebaserede analyser af ekstraordinære hændelser, som kan resultere i konsekvenser for liv, helbred, miljø, økonomi, ejendom, kritisk infrastruktur, samfundsvigtige (eller forretningskritiske) funktioner eller andre værdier. På trin 2 opstilles der derfor ét eller flere realistiske scenarier, som er repræsentative for det aktuelle trusselsbillede. Disse kan med fordel tage udgangspunkt i eksisterende lokale/organisation-specifikke risikobilleder eller det aktuelle nationale risikobillede udgivet af Beredskabsstyrelsen. Hvert scenarie skal efterfølgende analyseres i modellens trin 3.

Hensigten med opstilling af scenarier er at få indsnævret feltet af potentielle trusler, så I kan fokusere på de områder, hvor indledende drøftelser peger på *væsentlige* trusler, risici og sårbarheder – dvs. ikke en ’totalliste’ over alle tænkelige trusler.

### Trin 3: Analyse af hvert enkelt scenarie

På trin 3 foretages der separate risiko- og sårbarhedsvurderinger for hvert af de scenarier, I har opstillet på trin 2.

Indledningsvis angiver I hvilke funktioner, kapaciteter eller faciliteter, herunder evt. udpegede samfundsvigtige funktioner og underlagt kritisk infrastruktur og/eller forretningskritiske funktioner, der skal opretholdes og videreføres såfremt den pågældende type hændelse indtræffer. Derefter vurderer I henholdsvis sandsynligheden for at hændelsestypen vil kunne indtræffe, samt de konsekvenser dette vil medføre. I når derved frem til et samlet risikoniveau. Endelig vurderer I de sårbarheder, der knytter sig til organisationens evne til at imødegå og håndtere den pågældende hændelsestype.

### Trin 4: Risiko- og sårbarhedsprofil

På trin 4 sammenstiller I analyseresultaterne fra de forskellige scenarieanalyser (trin 3). Resultatet er en risiko- og sårbarhedsprofil, som giver et samlet overblik over hvilke hændelsestyper, der udgør den største fare for organisationen.

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

Den endelige sårbarhedsoversigt illustrerer således hvor relativt robust eller sårbart organisationens beredskab er ift. 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 dette kapitel kan man finde trin-for-trin vejledning i hvordan man udfylder skabelonerne. Det er derfor en god ide at finde skabelonerne frem, så man kan referere til dem, mens man læser vejledningen.

## Trin 1: Udgangspunkt for analysen

Som medlemmer af analysegruppen skal I indledningsvis udfylde baggrundsoplysninger om jer selv (navn, stilling, ansættelsessted). Herefter skal I identificere og kort beskrive de forretningskritiske funktioner samt evt. samfundsvigtige funktioner og kritisk infrastruktur, som jeres organisation har beredskabsansvar for, og som risiko- og sårbarhedsanalysen skal omfatte.

*Forretningskritiske funktioner* refererer til de funktioner, der er nødvendige for at organisationen kan opretholde sin virksomheds drift og dermed kritiske leverancer på et acceptabelt niveau, eller funktioner, hvis mangel vanskeliggør overholdelse af organisationens forvaltningsmæssige forpligtelser.

*Samfundsvigtige funktioner* betegner ”de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed”, og hvis afbrydelse vil have uacceptable konsekvenser. Det kan fx være elproduktion og transmission, data- og teletransmission, behandling i sygehusvæsenet mv. Til støtte for identifikation er der i Bilag A opstillet en oversigt over samfundsvigtige funktioner. Hertil kommer underlagt kritisk infrastruktur, som defineres som ”infrastruktur – herunder faciliteter, systemer, processer, netværk, teknologier, aktiver samt serviceydelser – som er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner.”

For organisationer med beredskabsansvar for samfundsvigtige funktioner og underlagt kritisk infrastruktur 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, om jeres organisation også har overordnet beredskabsansvar for samfundsvigtige funktioner og/eller kritisk infrastruktur, som er udliciteret.

## Trin 2: Identifikation af trusler og risici

Modellens trin 2 indeholder en skabelon til at opstille scenarier. Skabelonen angiver en række forhold, som I skal beskrive. Scenariebeskrivelsen sikrer samtidig, at alle deltagere i analysen har et fælles udgangspunkt for den efterfølgende analyse.

Det er imidlertid vigtigt, at vurderingerne af sandsynlighed, konsekvenser og sårbarheder gennemføres ud fra det pågældende scenaries overordnede tema (hændelsestypen) og ikke ud fra meget præcise detaljer i scenariebeskrivelsen såsom datoer, klokkeslæt, hændelsens udbredelse i antal kvadratkilometer mv.

### Hvor mange scenarier?

**Alvorlige samfundsmæssige konsekvenser kan fx være:**

* Mange omkomne, kvæstede, syge og/eller udsatte personer
* Meget stort pres på, ustabilitet eller nedbrud af forretningskritiske funktioner, samfundsvigtige funktioner, underlagt kritisk infrastruktur eller dele heraf
* Store skader på miljøet eller immaterielle værdier
* Massiv tab af ejendom 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.

I beslutter selv, hvor mange scenarier, der skal anvendes. Et godt formuleret scenarie sætter fokus på problemer, der også forekommer ved lignende hændelsesforløb.

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

### Det gode scenarie

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

Scenarierne bør være *realistiske*. 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 forretningskritiske funktioner, samfundsvigtige funktioner og/eller kritisk infrastruktur, som er udpeget under afgrænsningen på modellens trin 1. I bør undgå at opstille scenarier for de absolut værst tænkelige, og dermed mest usandsynlige katastrofer (’worst case’). Omvendt burde der heller ikke være tale om hyppige eller dagligdags hændelser.

Eksempler kunne være særligt ekstreme vejrfænomener, alvorlige industriulykker, forureningsuheld, sygdomsudbrud, forsyningssvigt eller ondsindede menneskelige handlinger såsom sabotage, cyber- eller terrorangreb.

Scenariet bør være beskrevet så *detaljeret*, som det er nødvendigt for at kunne analysere de tilknyttede trusler, risici og sårbarheder. Scenariet bør således indeholde beskrivelser af hvilken trusselskategori, der er tale om, samt detaljer om truslens karakter, omfang, varighed mv. Overvej i denne sammenhæng, om det er mest hensigtsmæssigt at opstille specifikke eller generelle hændelser (fx ’kryptering af forretningskritisk data hos X-styrelse’ vs. ’cyberangreb mod offentlige myndigheder’).

## Trin 3: Analyse af scenarier

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

* I **afsnit A** anføres de forretningskritiske funktioner, samfundsvigtige funktioner og underlagt kritisk infrastruktur ift. 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).

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

Under pkt. 1 skal I mere præcist anføre, de forretningskritiske funktioner, samfundsvigtige funktioner og kritisk infrastruktur 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.

**Indeks til vurdering af sandsynlighed**

1. Meget lav / ingen
2. Lav
3. Middel
4. Høj
5. Meget høj

**Indeks til vurdering af konsekvenser**

1. Ubetydelige / meget begrænsede
2. Begrænsede
3. Alvorlige
4. Meget alvorlige
5. Kritiske / katastrofale

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 dog vigtigt at forsøge, da sandsynlighedsvurderingen sammen med de efterfølgende konsekvensvurderinger skal anvendes til at fastsætte risikoniveauet for scenariet (pkt. 8).

Vurderingen af sandsynlighed kan eventuelt støttes af overvejelser om hyppighed 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.

Under pkt. 3-7 skal I vurdere de mulige konsekvenser af hændelsestypen for hhv. egen organisation/ansvarsområde og for samfundet generelt. I begge tilfælde anvendes konsekvensindekset.

I skal først beskrive og vurdere hændelsestypens direkte konsekvenser for evnen til at opretholde og videreføre de samfundsvigtige eller forretningskritiske funktioner, som I anførte i afsnit A (pkt. 1). Det kan eksempelvist vedrøre hændelsens påvirkning af bygninger og installationer, personale, nødvendige leverancer mv.

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.

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

1. Tab af liv og helbred
2. Tab af aktiver (materielle, finansielle, miljømæssige mv.)
3. Angst, utryghed, vrede, harme eller politiske implikationer
4. Afbrydelse af kritisk infrastruktur (fx teleinfrastruktur, elnettet, banenettet, rørledninger osv.)

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

### Scenariets risikoniveau

Under punkt 7 fastsætter I hændelsestypens samlede konsekvenser ved at angive det højeste konsekvensniveau fra punkt 4 til punkt 6. Det bliver dermed det højeste konsekvensniveau, der slår igennem i det overordnede 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 punkt 2 med talværdien fra den samlede vurdering af konsekvenser fra punkt 7.

### Vurdering af sårbarheder

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

1. Forberedelser før hændelsen indtræffer (pkt. 9-11)
2. Kapaciteter til indsats og afhjælpning under selve hændelsen (pkt. 12-13)
3. 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 bør fokusere på de kapaciteter, som er relevante ift. den konkrete hændelsestype, som scenariet beskriver, og for de specifikke funktioner, faciliteter og kapaciteter, herunder forretningskritiske funktioner og udpegede samfundsvigtige funktioner og/eller kritisk infrastruktur, 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 |

Under punkt 9-10 beskrives de forberedelser, som organisationen har gjort sig for at kunne håndtere hændelsestypen. Her bør fokusset være på de tiltag og foranstaltninger, som er mest relevante for organisationens ’modstandskraft’ før hændelsen er indtruffet.

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

Under punkt 10 beskriver I de mere håndgribelige foranstaltninger, som enten kan forebygge at hændelsen indtræffer eller begrænse skaderne. De forebyggende eller skadesbegrænsende foranstaltninger kan fx 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 samfundsvigtige og/eller forretningskritiske funktioner samt underlagt kritisk infrastruktur. Eksempler herpå er:

* 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 punkt 11 vurdere, hvor virkningsfulde de forberedelser I har beskrevet samlet set er i forhold til den pågældende hændelsestype.

Under punkt 12 beskrives organisationens eksisterende kapacitet til akut indsats og afhjælpning, såfremt hændelsestypen indtræffer. Det kan bl.a. dreje sig om ledelse, personale, materiel, organisering, logistik, lagre, finansiering m.v. Under punkt 13 vurderer I efterfølgende, hvor effektive de beskrevne kapaciteter samlet set er for jeres organisations evne til at håndtere hændelsestypen.

Under det sidste punkt på trin 3 skal I først beskrive, og derefter samlet set vurdere, de kapaciteter organisationen råder over til reetablering. Fokus er her på de 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 4: Risiko- og sårbarhedsprofil

### Risikomatrix

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SANDSYNLIGHED | Meget høj (5) |  |  |  |  |  |
| Høj (4) |  |  |  |  |  |
| Middel (3) |  |  |  |  |  |
| Lav (2) |  |  |  |  |  |
| Meget lav / ingen (1) |  |  |  |  |  |
| Meget høj risiko | | Meget begrænsede / ubetydelige (1) | Begrænsede (2) | Alvorlige (3) | Meget alvorlige (4) | Kritiske / katastrofale (5) |
| Høj risiko | |
| Middel risiko | |
| Lav risiko | |
| Meget lav risiko | | KONSEKVENSER | | | | |

### Sårbarhedsoversigt

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| • • • • • Meget høj sårbarhed  • • • • Høj sårbarhed  • • • Middel sårbarhed  • • Lav sårbarhed  • Meget lav sårbarhed | | **VURDERING AF SÅRBARHEDSNIVEAU** | | |
| Forberedelse (planer, forebyggelse mv.) | Kapaciteter til indsats og afhjælpning | Kapaciteter til reetablering |
| **SCENARIER** | Anfør scenarie nr. og navn | • • • • |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |
| Anfør scenarie nr. og navn |  |  |  |

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

Trusler, 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 eller risiko påvirkes af hvor sårbart eller robust det system, som truslen eller risikoen retter sig imod, er. Under arbejdet med trin 4 anbefales I derfor at se tilbage på analyseresultaterne fra trin 3, og om nødvendigt foretage justering 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.

## Opfølgning på analysen

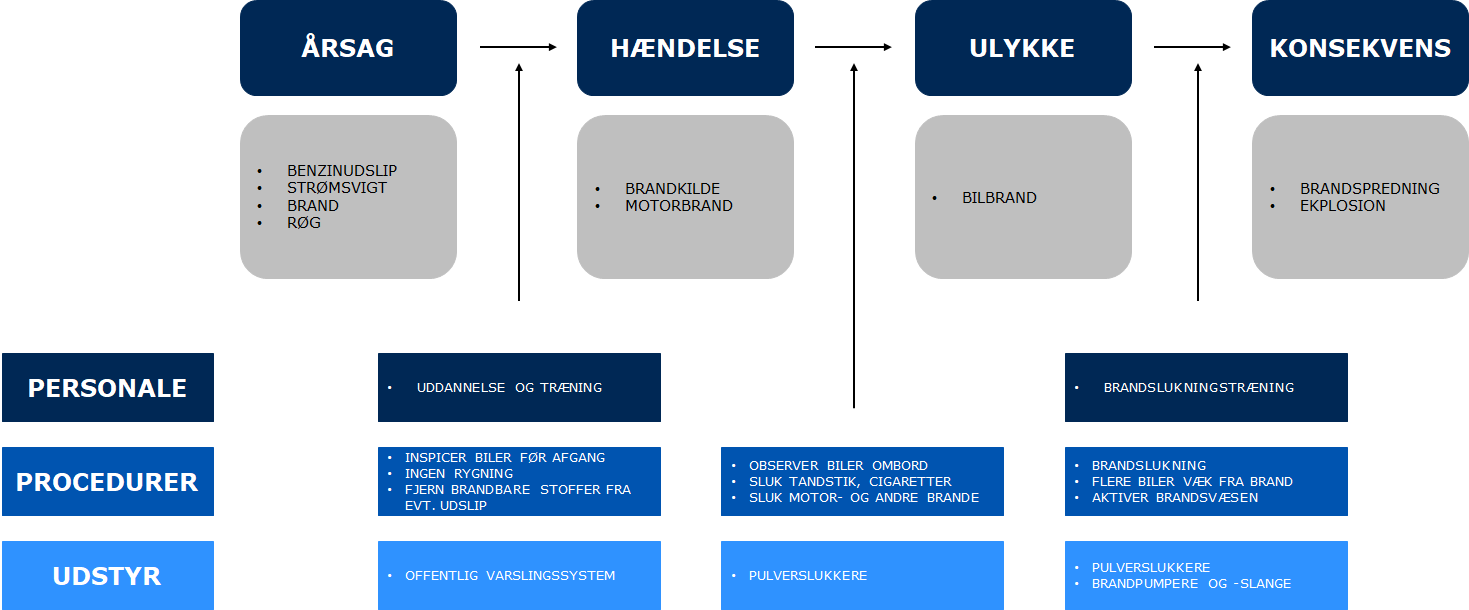
Brug af ROS-modellen bør ideelt set resultere i prioriterede anbefalinger til risiko- og sårbarhedsreducerende tiltag. Da det hverken er praktisk eller økonomisk muligt at imødegå alle trusler, er opgaven at udvælge de potentielt mest effektive tiltag over for de væsentligste trusler, risici og sårbarheder,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

### Forslag til risiko- og sårbarhedsreducerende tiltag

Risikoreducerende tiltag retter sig primært mod selve truslerne/risici 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.

Sårbarhedsreducerende tiltag retter sig primært mod interne karakteristika ved et givet system, og omfatter foranstaltninger som kan styrke dets generelle evne til at modstå trusler/risici 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 samfundsvigtige funktioner og/eller kritisk infrastruktur.

For nogle af scenarierne (fx med ’meget høj’ sandsynlighed og/eller ’kritiske/katastrofale’ konsekvenser) kan I også overveje at lave en grafik, der illustrerer scenariets årsag, hændelse, ’ulykke’ og konsekvens. Sådan en grafik kan bruges til at få tankerne i gang ift., hvor I kunne iværksætte tiltag, der ville kunne bryde en kædereaktion på forskellige ’trin’ af hændelsesforløbet. Den kan også bruges til at illustrere over for beslutningstagerne, hvordan og i hvilke situationer en sårbarhedsreducerende tiltag ville kunne styrke organisationens overordnede robusthed. Nedenstående eksempel er taget fra U.S. Coast Guards værktøj, Preliminary Hazard Analysis, og skitserer et hændelsesforløb hvori et udslip af brandbare stoffer forårsager brand i en bil på en færge.



*Kilde:* [*U.S. Coast Guard*](https://homeport.uscg.mil/Lists/Content/Attachments/23384/PVA%20Risk%20Guide.pdf)

Her bruges der overskrifterne ’personale’, ’procedurer’ og ’udstyr’, men disse kan skiftes ud med overskrifter, der er relevante for det givne scenarie og/eller den givne organisation.

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

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. Ift. 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, sammenfattes resultaterne af den samlede analyseproces 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.

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 fx gøre dette via en handlingsplan, som skitserer:

* *Opgaver:* Hvilke tiltag skal implementeres, hvor og hvornår?
* *Rationale:* Ud fra hvilke anbefalinger?
* *Ansvar:* Hvem skal implementere tiltagene?
* *Ressourcer:* Hvor mange midler skal bruges?

### Opdatering af analysen

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

# Bilag A: Oversigt over samfundsvigtige funktioner

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | **Oversigt over de 15 samfundsvigtige områder/sektorer og eksempler på samfundsvigtige funktioner** | | **1. Energi** | | Produktions- og lagringskapacitet samt transport (transmission og distribution) og levering af elektricitet | | Produktion, transport (transmission og distribution) og lagring af varme og køling | | Produktions- og lagringskapacitet samt transport (transmission og distribution) og levering af gas | | Produktion, lagring og transport af råolie samt olieprodukter til transport og den petrokemiske industri | | **2. Informations- og kommunikationsteknologi (IKT)** | | Data- og taletransmission via telenet, herunder mobilnet | | Databehandling og dataopbevaring | | Satellit-, radio- og tv-transmission | | Leverance af fællesoffentlige grunddata, herunder f.eks. geodata | | Personregistreringen | | Central virksomhedsregistrering | | Tidssynkronisering | | Konvertering af domænenavne til IP-adresser | | Oprettelse og vedligeholdelse af lokalplaner | | Udbud af public service og nyhedsformidling via satellit-, radio-, tv- og internettransmission. | | Opretholdelse af sikker kommunikation nationalt og internationalt | | Understøttelse af det offentliges IT-infrastruktur | | Offentlig digital identifikation og kommunikation | | **3. Transport** | | Afvikling, planlægning og trafikstyring af individuel og kollektiv person- og godstransport (vej, bane, luft og sø) | | Overvågning og vedligehold af infrastruktur (broer, tunneler, togstationer, transportcentre, kombiterminaler, lufthavne, havne m.v.) | | Post og kurérservice | | Sikkerhedsundersøgelser ifm. transportulykker (Havarikommissioner) | | Tilsyn med og certificering af danske skibe og søfarende samt havnestatskontrol | | Søopmåling | | **4. Beredskab, politi og civilbeskyttelse** | | Alarmering og varsling | | Skadestedshåndtering | | Brandbekæmpelse | | Redning (land/sø/luft) | | Evakuering (inkl. modtagelse, indkvartering og forplejning) | | Katastrofeberedskab (miljø, stormfald, stormflod, skybrud mv.) | | Kystbeskyttelse | | Vedligehold af dæmninger, diger, sluser og pumpeanlæg | | Beskyttelse af samfundet mod indførsel af illegale varer | | Beskyttelse/sikring af kulturarven | | Overvågning samt kontrol med produktion, opbevaring og transport af farlige stoffer (kemiske, biologiske, radiologiske, nukleare og eksplosive stoffer) | | Indsats ved hændelser som involverer eller kan involvere farlige stoffer | | Ammunitionsrydning | | Akut udrykning | | Ikke-akut kontakt til politiet | | Ordenshåndhævelse og kriminalitetsbekæmpelse, herunder forebyggelse og efterforskning | | Understøttende funktioner til ordenshåndhævelse, kriminalitetsbeskyttelse og politiets beredskab (kommu-nikation, logistik og it) | | **5. Sundhed** | | Indkøb, oplagring, distribution og forsyning af værnemidler til sundheds- og plejesektoren i forbindelse med epidemi-/pandemihåndtering. | | Præhospital indsats | | Forebyggelse og behandling i sygehusvæsenet og hos praktiserende læger | | Overvågning og varsling ifm. smitsomme sygdomme mv. | | Produktion, registrering, distribution og overvågning af lægemidler | | Psykosocial og kriseterapeutisk indsats | | Aktivering af sundhedsberedskabet (sygehusberedskab, primære sundhedstjenestes beredskab og læge-middelberedskab), når behov ikke kan hånderes i det alm. sundhedsvæsen | | **6. Sociale forhold** | | Opretholdelse af dagtilbud, SFO mv. | | Pleje og omsorg for ældre, handicappede, kronisk syge, ressourcesvage og udsatte personer | | Gejstligt beredskab | | Begravelsesvæsen | | **7. Drikkevand og fødevarer** | | Indvinding, produktion, lagring, kontrol med og forsyning af rent drikkevand og overvågning af grundvand | | Produktion og forsyning af fødevarer, foder og levende dyr | | Overvågning og kontrol med fødevaresikkerhed | | Varsling og indsats ifm. smitsomme husdyrsygdomme og zoonoser | | Varsling og indsats ifb. med plantekarantæneskadegører | | **8. Spildevand og renovation** | | Håndtering og rensning af spildevand | | Afhentning og bortskaffelse af affald | | Godkendelse og tilsyn med store forbrændingsanlæg | | **9. Finans og økonomi** | | Betalingsformidling | | Bankvirksomhed | | Forsikringsvirksomhed | | Håndtering af værdipapirer, herunder handel, opbevaring og corporate actions | | Udbetaling af lønninger, pensioner og overførselsindkomster | | Skatte- og afgiftsopkrævning | | Pensionsvirksomhed, herunder tegning, investering og formuepleje | | Håndhævelse af fusionskontrolreglerne i alle brancher | | Bankkontrol | | Årsafslutning | | Refusioner til statslige (og selvejende) arbejdsgivere | | **10. Uddannelse og forskning** | | Opretholdelse af undervisningen i grundskoler, på ungdomsuddannelser, efteruddannelser samt videregå-ende uddannelser. | | Opretholdelse af forskning (særligt repositorier og forskningsdata) | | **11. Meteorologi** | | Vejrudsigter og varsling af farligt vejr til borgere, beredskaber og søfarende. | | Meteorologisk betjening af forsvaret og civil luftfart med vejrobservationer og varslinger | | Meteorologisk service og beredskab i tilfælde af nukleare og kemiske udspil, bioterror samt spredning af luftbårne sygdomme. | | Produktion og levering af observations- og modeldata bl.a. på dmi.dk. | | Varsel af forhøjet ozon i luften | | Monitorering af havis og isbjerge i grønlandske farvande | | **12. Forsvar samt efterretnings- og sikkerhedstjeneste** | | Militært forsvar og sikkerhed, herunder konfliktforebyggelse, krisestyring og kollektivt forsvar samt planlæg-ning og gennemførelse af beredskabsforanstaltninger | | Suverænitetshåndhævelse | | Kontraterrorisme | | Kontraekstremisme | | Kontraspionage | | Personbeskyttelse | | Situations- og trusselsvurderinger | | Indhentning af oplysninger og vurderinger af forhold i udlandet af betydning for Danmark og danske interes-ser. | | Efterretnings- og efterforskningsmæssige opgaver samt militær og statslig varsling vedr. internettrusler. | | Værtsnationsstøtte | | **13. Udenrigstjeneste** | | Varetagelse af Danmarks udenrigsdiplomatiske interesser | | Borgerservice/konsulære tjenester | | Eksport og investeringsfremme | | Krisediplomati/sikkerhedspolitik | | Offentlighedsdiplomati | | **14. Myndighedsudøvelse generelt** | | Opretholdelse af Folketingets, regeringens, centraladministrationens, samt kommuners og regioners funkti-oner | | Gennemførelse af valghandlinger | | Kontrol med eksport af kritiske produkter og varer (dual-use eksportkontrol) | | Screening af udenlandske investeringer og særlige økonomiske aftaler mhp. beskyttelse af bl.a. kritisk infra-struktur | | Tinglysning, herunder skibsregistrering | | Tilsyn og kontrol med de retshåndhævende myndigheder mv. | | Straffuldbyrdende funktioner i fængsler, arrester, udslusningspensioner og kriminalforsorgsafdelingerne | | Støttefunktioner til straffesagskæden og straffuldbyrdelse (logistik mv.) | | Adgang til domstolsprøvelse | | Administration af domstole | | **15. Tværgående krisestyring** | | Krisestyring internt i organisationer og mellem enheder i det nationale krisestyringssystem | | Koordinerende krisestyring mellem dem nationale krisestyringssystem og private aktører og samfundskritisk forsyningsvirksomheder (vand, mad, energi, kommunikation mv.) | | Regeringens Sikkerhedsudvalg | | Embedsmandsudvalget for Sikkerhedsspørgsmål | | National Operativ Stab | | International Operativ Stab | | Lokale beredskabsstabe | | Kommandostader | | Krisestyringsstabene og andre krisestyringsunderstøttende funktioner | |

# Bilag B: Katalog over trusler (ikke udtømmende)

|  |  |
| --- | --- |
| ***Trusselskategorier/-typer*** | ***Eksempler*** |
| **Ekstreme naturfænomener** | |
| Atmosfæriske trusler | Orkan, snestorm, isvinter, islag, tæt tåge, skybrud, is storm, saltstorm, lynnedslag |
| Geologiske trusler | Jordskred, erosion |
| Oceanografiske trusler | Stormflod, oversvømmelse, hav is |
| 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 |
| **Transportulykkers (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/forurenede 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 eksplosion** | |
| 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” (risikovirksomheder), miljø/brandfarlige virksomheder, oplag af brandfarlige/eksplosive stoffer |
| Infrastruktur | Banegårde, lufthavne, tunneler, 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 |
| Plantesygdomme | Bakterier, virus, giftstoffer |
| **Ødelæggelse, afbrud eller andet svigt af samfundsvigtige funktioner** (se bilag A) | |
| **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 | |
| Spionage | | Industrispionage, spionage mod centraladministrationen, spionage mod forskningsinstitutioner | |
| Udslip af farlige stoffer i Danmarks nærområde | | Ulykker på atomkraftværker eller kemiske udslip | |
| Sammenstyrtninger | | Store bygninger, stadions, trafikanlæg | |
| Nedstyrtninger | | Satellitter, meteorer | |
| Rumhændelser | | Forstyrrelser af GNSS signalet, udfald af observations eller kommunikationssatellitter, påvirkning af radar, overspændinger i elnettet | |

# 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 vedr. 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 trin 1: baggrundsoplysninger, afgrænsning af samfundsvigtige funktioner og underlagt kritisk infrastruktur og/eller forretningskritiske funktioner, beredskabsansvar og analysefokus. |  |
| Udfyld modellens trin 2: opstil et passende antal scenarier. |  |
| Udfyld modellens trin 3: udfør risiko- og sårbarhedsvurderinger for hvert scenarie. |  |
| Udfyld modellens trin 4: opstil risiko- og sårbarhedsprofilen. Diskuter resultaterne og gå (on nødvendigt) tilbage til trin 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 trusler, 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 hvilke 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 men 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/risicis sandsynlighed og deres mulige konsekvenser, mens en sårbarhedsanalyse typisk vurderer et systems interne styrker og svarheder. 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.

*Samfundsvigtige funktioner* refererer til den officielle danske definition: ”*de aktiviteter, varer eller tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed*.” Disse funktioner skal derfor kunne opretholdes og videreføres under større ulykker eller katastrofer. I bilag A findes en oversigt over de 15 overordnede sektorer og et større antal delmængder af samfundsvigtige funktioner.

*Kritisk infrastruktur* er jf. den officielle danske definition *”infrastruktur – herunder faciliteter, systemer, processer, netværk, teknologier, aktiver samt serviceydelser – som er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner.”*

*Forretningskritiske funktioner* er de funktioner, der er nødvendige for at organisationen kan opretholde sin virksomheds drift og dermed kritiske leverancer på et acceptabelt niveau, eller funktioner, hvis mangel vanskeliggør overholdelse af organisationens forvaltningsmæssige forpligtelser.

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

*Risiko* betegner i denne kontekst kombinationen af sandsynlighed 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. Risikovurderingen 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, helbred, miljø, økonomi, ejendom, samfundsvigtige funktioner 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. En *sårbarhedsvurdering* sker ved at sætte trusler i forhold til eksisterende modforanstaltninger, kapaciteter og den fortrukne grad af beskyttelse.