# Introduktion til ROS60

I en tid, hvor udviklingen i risikolandskabet stiller større og mere dynamiske krav til myndigheder og organisationer og deres evne til at opretholde samfundsvigtige funktioner end hidtil, er det vigtigere end nogensinde at være på forkant med beredskabsplanlægning. For at kunne modstå trusler skal enhver organisation skabe et stærkt fundament bestående af en solid forståelse af de risici, der kan påvirke den givne organisation og dens samfundsvigtige og/eller forretningskritiske funktioner samt underlagt kritisk infrastruktur. En sådan forståelse er med til at danne analysegrundlaget for organisationens videre arbejde med beredskabsplanlægning.

Beredskabsstyrelsen har udviklet to værktøjer til risiko- og sårbarhedsanalyse: ROS-modellen og ROS60. ROS-modellen er en fuldt udbygget analysemodel, hvorimod ROS60 er en kort øvelse, som kan være med til at introducere organisationen til risiko- og sårbarhedsanalyse på en hurtig og engagerende måde. ROS60 kan gennemføres af alle fra medarbejdere, som senere skal sidde med risiko- og sårbarhedsanalyser, til topledere, der ønsker et hurtigt overblik over opgaven.

ROS60 er en gruppeøvelse, som introducerer de centrale begreber i en risiko- og sårbarhedsanalyse. Øvelsen har til formål at identificere mulige risici og sårbarheder i organisationens beredskab i løbet af 60 minutter. Deltagerne skal tage afsæt i deres umiddelbare viden om organisationen, herunder organisationens risikobillede og bruge deres erfaringer til at vurdere risici og sårbarheder. Den kræver således kun meget kort tid til forberedelse og opsamling.

Øvelsen består af fire trin suppleret af tre slides, som bruges til at illustrere resultaterne af øvelsens sidste tre trin. Disse slides kan endvidere refereres tilbage til i det videre arbejde med risiko- og sårbarhedsanalyse.

# Forløbet af ROS60

For at gennemføre ROS60 skal hver undergruppe bruge:

[ ]  Et lokale, hvor deltagerne kan stå omkring et whiteboard.

[ ]  En projektor

[ ]  Et stort whiteboard (min. 150 x 150 cm)

[ ]  10-15 store post-its

[ ]  Røde, gule og grønne magneter, 5-10 i hver farve (alternativt kan man blot markere med røde, gule og grønne whiteboardpenne)

[ ]  ROS60 PowerPoint-præsentation med tre slides (findes på Beredskabsstyrelsens hjemmeside)

ROS60 består af fire trin:

1. Kortlægning af organisationens samfundsvigtige eller forretningskritiske aktiviteter og/eller funktioner samt underlagt kritisk infrastruktur (typisk forberedt af arrangørerne på forhånd)
2. Identifikation af relevante trusler (slide A)
3. identifikation af de største risici (slide B)
4. Identifikation af sårbarheder i beredskabet (slide C)

Deltagerne skal dele sig op i grupper af 6-8 personer.

## Trin 1: Identifikation af samfundsvigtige og/eller forretningskritiske funktioner samt evt. underlagt kritisk infrastruktur

Identifikationen af organisationens samfundsvigtige og/eller forretningskritiske aktiviteter og funktioner samt evt. underlagt kritisk infrastruktur[[1]](#footnote-1) er med til at danne et fælles grundlag for diskussionen af risici og sårbarheder.

Funktionerne kan med fordel deles op i to hovedtyper:

1. **Særlig væsentlige driftsopgaver:** de dele af den ’almindelige’ virksomhed, som også bør kunne fortsætte under en ekstraordinær hændelse
2. **Krisestyringsopgaver:** de ekstraordinære aktiviteter, som bør kunne sættes i værk ved en større hændelse, og som kræver strategisk ledelse og aktiv indsats

Øvelsens facilitator kan med fordel identificere organisationens samfundsvigtige og/eller forretningskritiske aktiviteter og funktioner samt underlagt kritisk infrastruktur på forhånd og præsentere resultatet for deltagerne. Alternativt kan ROS60 starte med en deltager-ledet drøftelse af dette.

## Trin 2: Identifikation af relevante trusler

På trin 2 identificeres trusler eller de hændelsestyper, som umiddelbart vurderes at kunne true organisationens samfundsvigtige og/eller forretningskritiske aktiviteter og funktioner og/eller kritisk infrastruktur.

Ved hjælp af trusselskataloget på slide A i bilag skal I derefter udvælge de trusler, som I vil analysere og nedskrive dem (I kan evt. anvende post-its – én trussel pr. post-it). Truslerne kan udvælges fra eksemplerne på slide A i bilag eller udarbejdes specifikt tilpasset jeres organisation. Hvis I ønsker at lave jeres eget katalog, kan denne med fordel være forberedt af arrangørerne på forhånd.

## Trin 3: Identifikation af de største risici

På trin 3 afgør I, hvilke af de udvalgte trusler, der indebærer den største risiko for, at organisationens samfundsvigtige og/eller forretningskritiske aktiviteter eller funktioner samt evt. underlagt kritisk infrastruktur bliver afbrudt eller sat under alvorlig pres.

I øvelsen på slide B i bilag skal I placere jeres udvalgte trusler (post-its) nederst i matrixen ift. konsekvenserne. Forhold jer først til konsekvenserne og fordel truslerne på konsekvens-aksen. Derefter skal I vurdere truslernes sandsynlighed og rykke post-its’ene op på sandsynligheds-aksen.

Til sidst skal I udvælge de 5-7 trusler, som udgør den største risiko for jeres organisation ud fra dem, der er placeret længst oppe i højre hjørne.

## Trin 4: Identifikation af sårbarheder i beredskabet

**FOREBYGGELSE:** beredskabstiltag, som forhindrer hændelsen i at indtræffe eller nedbringer konsekvenserne af hændelsen.

**PLANER:** beredskabsplaner, indsatsplaner, delplaner, planer for fortsat drift, instrukser, action cards, m.v., det opstiller retningslinjer for hvordan hændelsen håndteres.

**UDDANNELSE OG ØVELSER:** tiltag, der giver personerne i beredskabet de færdigheder, der er nødvendige for at de kan håndtere hændelsen.

**INDSATSKAPACITET:** den nødvendige kapacitet for akut indsats, afhjælpning og reetablering (fx krisestyringsorganisation, personale, materiel m.v.)

På dette trin skal I skabe et umiddelbart overblik over, hvor godt organisationen er forberedt på de største trusler, som I har identificeret på trin 3. Det giver et godt billede af, hvor jeres beredskab er sårbart/robust, både ift. de enkelte risici og inden for fire områder: forebyggelse, planer, uddannelse og øvelser samt indsatskapacitet.

Placer de udvalgte trusler (post-its) i venstre ’trussel’-kolonne på slide C. Vurder derefter jeres beredskab inden for hvert af de fire områder vha. farvede magneter/whiteboardpenne efter følgende skala:

**RØD:** behov for større ændringer

**GUL:** behov for justeringer

**GRØN:** intet umiddelbart behov for ændringer

# Afslutning af ROS60: opsamling i fællesskab

I kan med fordel samle op, ved at hver gruppe præsenterer sine resultater af deres drøftelser og ved en sammenligning af resultaterne. ROS60 kan ikke bruges alene som et grundlag til at træffe beslutninger på, men den kan danne grundlaget for yderligere drøftelse af behovet for egentlige risiko- og sårbarhedsanalyser.

# Flere informationer

På Beredskabsstyrelsens hjemmeside brs.dk kan du finde flere informationer om Beredskabsstyrelsens værktøjer til risiko- og sårbarhedsanalyse, herunder ROS-modellen, som er Beredskabsstyrelsens generelle, fuldt udbyggede model for risiko- og sårbarhedsanalyse.

1. *Kritisk infrastruktur* defineres således som”infrastruktur – herunder faciliteter, systemer, processer, netværk, teknologier, aktiver samt serviceydelser – som er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner.” [↑](#footnote-ref-1)