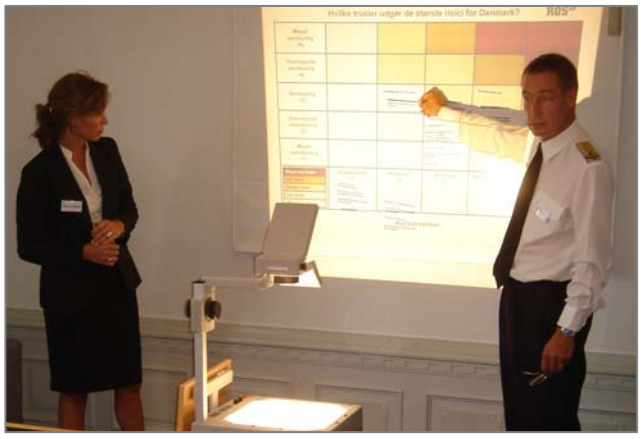
ROS 60



En introduktion til risiko- og sårbarhedsanalyse på 60 minutter

Vejledning

Revideret 2008

Beredskabsstyrelsen

Formål og udbytte af ROS60

ROS[60] er en gruppeøvelse, som enkelt og hurtigt introducerer de centrale begreber i risiko- og sårbarhedsanalyse.

ROS[60] går ud på, at en gruppe medarbejdere (opdelt i undergrupper på 6 - 8 personer) i løbet af 60 minutter identificerer mulige risici og sårbarheder i organisationens beredskab over for større uheld og andre hændelser.

ROS[60]-øvelsen er lagt an på, at deltagerne tager afsæt i deres umiddelbare viden om organisationen og bruger deres erfaringer og intuition til at vurdere risici og sårbarheder.

ROS[60] kræver således kun meget kort tid til forberedelse og opsamling.

Deltagerne i ROS[60] kan være medarbejdere, som skal gennemføre en risiko- og sårbarhedsanalyse, eller det kan være ledelsen, som ønsker et hurtigt overblik over opgaven.

Nødvendigt udstyr for at gennemføre ROS[60]

For at gennemføre ROS[60] har hver undergruppe brug for:

- ❑ Et lokale, hvor deltagerne kan stå omkring et whiteboard.
- ❑ En overheadprojektor /powerpointprojektor.
- ❑ Et stort whiteboard (minimum 150 x 150 cm).
- ❑ 10 - 15 store post-its
- ❑ Røde, gule og grønne magneter, 5 – 10 i hver farve.
  (Alternativ: markeringer med røde, gule og grønne whiteboardpenne)
- ❑ ROS[60] powerpointpræsentation med tre dias (findes på Beredskabsstyrelsens hjemmeside: www.brs.dk/fagomraade/tilsyn/csb/ROS/ROS60.htm).

Forløbet af ROS^{60}

ROS^{60} består af fire trin:

1. Identifikation af de kritiske aktiviteter og funktioner (typisk forberedt af arrangørerne)
2. Identifikation af relevante trusler (dias A)
3. Identifikationer af de største risici (dias B)
4. Identifikation af sårbarheder i beredskabet (dias C)

De enkelte dias vises efter tur på whiteboardet.

Deltagerne opdeles i grupper med 6 – 8 personer i hver. Derved bliver lettere at inddrage alle deltagere i diskussionen og at sammenligne resultaterne til sidst.

Det er en fordel at notere vurderingerne undervejs i processen for at fastholde resultaterne.

Trin 1: Identifikation af kritiske funktioner

Identifikationen af organisationens kritiske aktiviteter og funktioner skal danne et fælles grundlag for diskussionen af risici og sårbarheder.

De kritiske funktioner er delt i to hovedtyper:

- Særligt væsentlige driftsopgaver er de dele af den ”almindelige” virksomhed, som også bør fortsætte under en ekstraordinær hændelse.
- Opgaver vedrørende krisestyring er de ekstraordinære aktiviteter, som bør kunne sættes i værk, ved en større hændelse, som kræver strategisk ledelse og aktiv indsats.

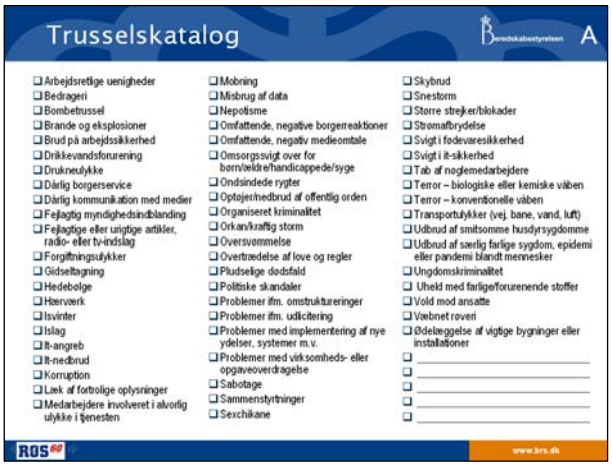
Arrangørerne af øvelsen kan have identificeret kritiske aktiviteter og funktioner på forhånd og præsentere resultatet for deltagerne. Alternativt kan ROS^{60} begynde med at deltagerne diskutere dette.. Der bør dog så afsættes lidt ekstra tid til øvelsen, hvis de kritiske aktiviteter og funktioner skal identificeres af deltagerne.

Trin 2: Identifikation af relevante trusler

Under trin 2 identificeres de hændelser, som umiddelbart vurderes at kunne true organisationens kritiske aktiviteter og funktioner.

1. ***Vis dias A på whiteboardet.***

2. ***Udvælg de trusler, som I vil analysere og skriv dem på post-its (én trussel pr. seddel).***



Truslerne kan udvælges fra eksemplerne på dias A eller udarbejdes specifikt til jeres organisation.

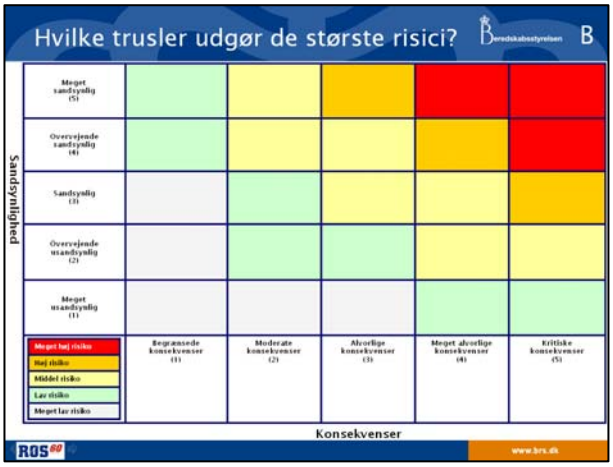
Trin 2 kan være forberedt på forhånd, ved at arrangørerne af øvelsen har udvalgt en række trusler. Det er dog vigtigt at have ekstra post-its, så deltagerne selv kan tilføje nye trusler.

Trin 3: Identifikation af de største risici

Målet med denne del er at afgøre, hvilke af de udvalgte trusler, der indebærer den største risiko for, at organisationen kritiske aktiviteter eller funktioner bliver afbrudt eller sat under alvorligt pres.

3. ***Vis dias B på whiteboardet.***

4. ***Placerer jeres post-its med truslerne nederst i matrixen i forhold til konsekvenserne.***



I første omgang skal I kun forholde sig til konsekvenserne (vurdering af sandsynligheden følger i pkt. 5).

Konsekvenserne af hver trussel vurderes ud fra, hvor store konsekvenser den kan få for evnen til at opretholde de kritiske aktiviteter og funktioner.

5. ***Ryk post-its med enkelte trusler op i matrixen alt efter deres sandsynlighed.***

6. ***Udvælg de 5 - 7 trusler, der udgør den største risiko for jeres organisation.***

De trusler, der udgør den største risiko er placeret længst oppe i højre hjørne.

Trin 4: Identifikation af sårbarheder i beredskabet

Formålet med denne del er at skabe et umiddelbart overblik over, hvor godt organisationen har forberedt sig på de trusler, der udgør de største risici. Det indikerer, hvor jeres beredskab er sårbart/robust – både i forhold til de enkelte trusler og inden for fire områder: forebyggelse, planer, uddannelse og øvelser samt indsatskapacitet.

7. ***Vis dias C på whiteboardet.***

8. ***Post-its med de valgte trusler fra punkt 6 placeres i venstre kolonne i sårbarheds-oversigten.***

9. ***Vurdér derefter jeres beredskab inden for hvert af de fire områder ved hjælp af de farvede magneter.***

Anvend magneterne efter følgende skala:

RØD: Behov for større ændringer.
GUL: Behov for justeringer.
GRØN: Intet umiddelbart behov for ændringer.

De fire områder dækker følgende:

- FOREBYGGELSE: Tiltag som forhindrer hændelsen i at indtræffe eller nedbringer konsekvenserne af hændelsen.
- PLANER: Beredskabsplaner, indsatsplaner, instrukser, action cards, m.v., der 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 – f.eks. krisestyringsorganisation, personale, materiel m.v.

Afslutning af ROS^{60}: Opsamling i fællesskab

Hvis deltagerne var opdelt i undergrupper, kan I med fordel samle op ved at præsentere og sammenligne resultaterne af undergruppernes diskussioner.

ROS^{60} er for et for løst grundlag til at træffe beslutninger på, men den kan danne grundlag for at diskutere behovet for egentlige risiko- og sårbarhedsanalyser.

Flere informationer

På www.brs.dk/fagomraade/tilsyn/csb/ROS/ROS.htm findes flere informationer om Beredskabsstyrelsens værktøjer til risiko- og sårbarhedsanalyse:

- ROS^{60}
- ROS-modellen (Beredskabsstyrelsens generelle model for risiko- og sårbarhedsanalyse)
- Scenariebanken

Bilag: Eksempler på trusler

- ❑ Arbejdsretlige uenigheder
- ❑ Bedrageri
- ❑ Bombetrussel
- ❑ Brande og eksplosioner
- ❑ Brud på arbejdssikkerhed
- ❑ Drikkevandsforurening
- ❑ Drukneulykke
- ❑ Dårlig borgerservice
- ❑ Dårlig kommunikation med medier
- ❑ Fejlagtig myndigheds-indblanding
- ❑ Fejlagtige artikler, radio- eller tv-indslag
- ❑ Forgiftningsulykker
- ❑ Gidseltagning
- ❑ Hedebølge
- ❑ Hærværk
- ❑ Isvinter
- ❑ Islag
- ❑ It-angreb
- ❑ It-nedbrud
- ❑ Korruption
- ❑ Læk af fortrolige oplysninger
- ❑ Medarbejdere involveret i alvorlig ulykke i tjenesten
- ❑ Mobning
- ❑ Misbrug af data
- ❑ Nepotisme
- ❑ Omfattende, negative borgerreaktioner
- ❑ Omfattende, negativ medieomtale
- ❑ Omsorgssvigt over for børn/ældre/handicappede/syge
- ❑ Ondsindede rygter
- ❑ Optøjer/nedbrud af offentlig orden
- ❑ Organiseret kriminalitet
- ❑ Orkan/kraftig storm
- ❑ Oversvømmelse
- ❑ Overtrædelse af love og regler
- ❑ Pludselige dødsfald
- ❑ Politiske skandaler
- ❑ Problemer ifm. omstruktureringer
- ❑ Problemer ifm. udlicitering
- ❑ Problemer med at implementere nye ydelser, systemer m.v.
- ❑ Problemer med virksomheds- eller opgaveoverdragelse
- ❑ Sabotage
- ❑ Sammenstyrtninger
- ❑ Sexchikane
- ❑ Skybrud
- ❑ Snestorm
- ❑ Større strejker/blokader
- ❑ Strømafbrydelse
- ❑ Svigt i fødevaresikkerhed
- ❑ Svigt i it-sikkerhed
- ❑ Tab af nøglemedarbejdere
- ❑ Terror – biologiske eller kemiske våben
- ❑ Terror – konventionelle våben
- ❑ Transportulykker (vej, bane, vand, luft)
- ❑ Udbrud af smitsomme husdyrsygdomme
- ❑ Udbrud af særlig farlige sygdom, epidemi eller pandemi blandt mennesker
- ❑ Ungdomskriminalitet
- ❑ Uheld med farlige/forurenende stoffer
- ❑ Vold mod ansatte
- ❑ Væbnet røveri
- ❑ Ødelæggelse af vigtige bygninger eller installationer
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____
- ❑ _____