BN450

VEJLEDNING FOR KOLONNE 3-VIRKSOMHEDER

SIKRING AF RISIKOVIRKSOMHEDER

August 2017

Rigspolitiet
National Beredskabsafdeling

INDHOLD

Forsidefoto leveret af: Det rådgivende ingeniørfirma NIRAS

INDLEDNING

Den 1. maj 2016 trådte bekendtgørelse nr. 372 af 25. april 2016 om kontrol med risikoen for større uheld med farlige stoffer (risikobekendtgørelsen) i kraft og erstattede samtidig bekendtgørelse nr. 1666 af 14. december 2006.

Den nye risikobekendtgørelse indeholder primært regler, der gennemfører EUs risikodirektiv 2012/18/EU (Seveso III-direktivet), som regulerer virksomheder med større oplag af farlige stoffer med henblik på at forebygge og begrænse følgerne af større uheld.

Som noget nyt blev der i risikobekendtgørelsen samtidig indført krav om sikring af kolonne 3-virksomheder (herefter også kaldet "virksomheder" eller "risikovirksomheder"), som har til formål at forebygge forsætlige skadevoldende handlinger - terrorhandlinger med andre ord - mod eller med virksomhedernes farlige stoffer. Reglerne om sikring af risikovirksomheder findes i risikobekendtgørelsens § 11 og bilag 6.

Kravet om sikring af risikovirksomhederne mod forsætlige skadevoldende handlinger er en udmøntning af den såkaldte anbefaling 42o i tillægsrapport af 10. januar 2011 til "Regeringens handlingsplan for terrorbekæmpelse" (Terrorhandlingsplanen) fra november 2005. De nye regler om sikring hviler således ikke på forpligtelser efter Seveso III-direktivet, men skal ses som et supplement til de øvrige regler i risikobekendtgørelsen, som omhandler forebyggelse og begrænsning af større uheld.

Efter afgivelsen af tillægsrapporten i 2011 blev udmøntningen af anbefaling 42o sat midlertidigt i bero og derefter genoptaget i forbindelse med arbejdet med den nye risiko-bekendtgørelse.

De nye regler om sikring indebærer i hovedtræk, at virksomhederne fremover skal udarbejde en vurdering af deres sårbarhed over for forsætlige skadevoldende handlinger. Sårbarhedsvurderingen skal godkendes af den stedlige politikreds (herefter kaldet "politiet"), som kan beslutte, at virksomheden tillige skal udarbejde en sikringsplan og udpege en sikringsansvarlig, hvis det skønnes nødvendigt for, at virksomheden opnår et acceptabelt sikringsniveau.

Forebyggende sikringsforanstaltninger er nødvendige for i videst muligt omfang at forhindre forsætlige skadevoldende handlinger og minimere de samfundskritiske følgekonsekvenser ved sådanne handlinger. Konsekvensen af manglende eller mangelfuld sikring kan i værste fald langt overstige værdien af de sparede omkostninger ved ikke at etablere sikringsforanstaltningerne. Sikring af risikovirksomheder er både økonomisk og samfundsmæssigt forsvarligt. Sikringen af den enkelte virksomhed skal samtidig være proportional og imødegå de faktiske risici, som virksomheden står over for.

Der er for tiden ca. 55 kolonne 3-virksomheder på landsplan, som efter de nye regler skal udarbejde en sårbarhedsvurdering, medmindre virksomheden er omfattet af regler om havnefacilitetssikring. Hvor mange af virksomhederne, der vil blive mødt med et krav om at udarbejde en sikringsplan og udpege en sikringsansvarlig, beror på politiets konkrete

vurdering af behovet herfor. Typisk sikrer risikovirksomheder sig allerede mod eksempelvis uautoriseret adgang for at imødegå tyveri, spionage, hærværk osv., men ikke nødvendigvis mod egentlige terrorhandlinger. Det er dog Rigspolitiets vurdering, at selvom der konkret kan være behov for yderligere sikringsforanstaltninger på den enkelte virksomhed, vil der i vid udstrækning være tale om opgaver, der ikke er fremmede for virksomhederne.

Denne vejledning har til formål at vejlede virksomhederne i udarbejdelsen af sårbarhedsvurderingen og sikringsplanen, herunder om hvilke oplysninger dokumenterne skal indeholde, samt opstille nogle praktisk anvendelige værktøjer til risikovurderingen. Det er endvidere hensigten, at der med vejledningen sikres en ensartet anvendelse af terminologien og strukturen i sårbarhedsvurderingen og sikringsplanen.

Herudover fastsætter vejledningen rammen for de opgaver, der skal varetages i politikredsene i forbindelse med vurderingen af de udarbejde sårbarhedsplaner og eventuelle sikringsplaner.

1. ANVENDELSESOMRÅDE

Risikobekendtgørelsens § 11 finder alene anvendelse på virksomheder, der i medfør af risikobekendtgørelsen kategoriseres som kolonne 3-virksomheder. Det vil sige virksomheder med oplag af farlige stoffer eller kategorier af farlige stoffer, som overstiger tærskelmængderne i risikobekendtgørelsens bilag 1, del 1, kolonne 3, eller bilag 1, del 2, kolonne 3. Baggrunden herfor er, at det netop er disse virksomheder, hvor de største mængder farlige stoffer er til stede, og hvor der dermed også er størst potentiale for skade ved en eventuel terrorhandling.

Kolonne 2-risikovirksomheder og andre virksomheder, som har oplag af farlige stoffer, er således ikke omfattet af kravene i risikobekendtgørelsens § 11.

Endvidere følger det af risikobekendtgørelsens § 11, stk. 9, at kravene ikke gælder for risikovirksomheder, som er omfattet af bekendtgørelsen om sikring af havnefaciliteter (bekendtgørelse nr. 1462 af 30. november 2016 om sikring af havnefaciliteter), da havnefaciliteter er omfattet af særlige internationale regler (ISPS-koden). Det vil dog være hensigtsmæssigt, at virksomheden ved førstkommende ajourføring af havnefacilitets-sårbarhedsvurderingen (PFSA) og -sikringsplanen (PFSP) vurderer, om sikringen i tilstrækkeligt omfang omfatter de farlige stoffer.

Såfremt en virksomhed omfattet af bekendtgørelsen om sikring af havnefaciliteter har områder under driftskontrol, hvor farlige stoffer er til stede i et eller flere anlæg, herunder de fælles eller tilknyttede infrastruktur- og serviceanlæg eller aktiviteter, og som ikke er omfattet af bekendtgørelsen om sikring af havnefaciliteter, skal der udarbejdes en sårbarhedsvurdering for denne del af virksomheden efter reglerne i risikobekendtgørelsen. Hensynet er på den ene side at undgå, at den samme virksomhed skal sikres efter to forskellige regelsæt og på den anden side, at der ikke er dele af virksomheden, som ikke er (tilstrækkeligt) sikrede, fordi de falder uden for afgrænsningen af havnefaciliteten.

2. OPGAVER OG ANSVAR

2.1. KOLONNE 3-VIRKSOMHEDEN

2.1.1. Sårbarhedsvurdering

Det påhviler alle kolonne 3-virksomheder at udarbejde en sårbarhedsvurdering og sende denne til politiet til godkendelse, jf. risikobekendtgørelsens § 11, stk. 1.

Sårbarhedsvurderingen skal som udgangspunkt indsendes før virksomhedens etablering. Heri ligger også en forudsætning om, at der skal indsendes en sårbarhedsvurdering, inden der gennemføres en væsentlig ændring af en bestående kolonne 2-virksomhed, som indebærer, at virksomheden ændrer status til kolonne 3-virksomhed. Det svarer til fristerne for indsendelse af sikkerhedsrapport m.v. til kommunalbestyrelsen i risiko-bekendtgørelsens § 8, stk. 1.

Allerede eksisterende virksomheder, som ved den nye risikobekendtgørelses ikrafttrædelse den 1. maj 2016 enten blev kolonne 3-virkomhed, ændrede status fra kolonne 2 til kolonne 3, eller som fortsatte med at have status som kolonne 3-virksomhed, skal indsende sårbarhedsvurderingen til politiet senest den 1. juni 2017. Herudover er der en frist på to år for virksomheder, som er blevet eller bliver kolonne 3-virksomhed alene som følge af en ændret klassificering af farlige stoffer. Der henvises til de enkelte overgangsbestemmelser, som fremgår af § 8, stk. 5, og kapitel 14 i risikobekendtgørelsen.

2.1.2. Sikringsplan

Såfremt politiet på baggrund af sårbarhedsvurderingen beslutter, at der skal udarbejdes en sikringsplan og udpeges en sikringsansvarlig, påhviler det virksomheden at udarbejde sikringsplanen og indsende den til godkendelse inden for en af politiet fastsat frist, jf. risikobekendtgørelsens § 11, stk. 2 og 3.

Når politiet har godkendt sikringsplanen, skal virksomheden, som udgangspunkt senest 6 måneder efter datoen for godkendelsen, gennemføre de sikringsforanstaltninger, der fremgår af planen. Såfremt virksomheden af særlige årsager ikke har mulighed for at gennemføre (nogle af) sikringsforanstaltningerne inden for denne frist, angives det i den indsendte sikringsplan sammen med en begrundelse herfor. Se hertil afsnit 5.5. SIKRINGSFORANSTALTNINGER.

Det er virksomhedens ansvar, at sikringsforanstaltningerne gennemføres i overens-stemmelse med det i sikringsplanen anførte.

2.1.3. Gennemgang og ajourføring

Sårbarhedsvurderingen og sikringsplanen skal være retvisende og udtryk for de faktiske forhold på virksomheden. For at holde dokumenterne opdaterede, skal virksomheden efter risikobekendtgørelsens § 11, stk. 5, regelmæssigt og mindst hvert femte år, eller i øvrigt når der sker ajourføring af sikkerhedsrapporten, gennemgå og om nødvendigt ajourføre dokumenterne. De situationer, hvor der skal ske ajourføring af sikkerhedsrapporten, som

således også indebærer, at der skal ske ajourføring af sårbarhedsvurderingen og sikringsplanen, er anført i risikobekendtgørelsens § 9 og § 10. Det drejer sig blandt andet om de tilfælde, hvor der sker en ændring i risikovirksomheden, som vil kunne indvirke på risikoen for større uheld (§ 9), ved den regelmæssige ajourføring af sikkerhedsrapporten mindst hvert femte år, efter større uheld på virksomheden, efter anmodning fra risikomyndighederne eller på eget initiativ, på grund af nye forhold eller ny teknologisk viden m.v. (§ 10).

Hvis gennemgangen har givet anledning til ajourføring af sårbarhedsvurderingen og/eller sikringsplanen, skal den nye version fremsendes til politiet umiddelbart efter ajourføringen.

2.1.4. Øvelser

Har virksomheden udarbejdet en sikringsplan, skal planen effektivt afprøves ved afholdelse af øvelser mindst én gang hvert kalenderår, eller i øvrigt efter politiets nærmere bestemmelse herom, jf. risikobekendtgørelsens § 11, stk. 6. Virksomheden udarbejder en øvelsesevaluering, som sendes til politiet senest tre måneder efter øvelsens afslutning.

Der stilles ikke bestemte krav til, hvordan øvelserne tilrettelægges, blot at der skal være tale om en effektiv afprøvning af planen. Det er Rigspolitiets opfattelse, at som udgangspunkt for øvelserne bør virksomheden se på de væsentligste områder i sikringsplanen og den forudgående sårbarhedsvurdering. Det kan eventuelt være en fordel at afprøve en ny sikringsplan mere generelt ved den førstkommende øvelse for at få en grundig evaluering af planen og udfinde læringspunkter, som det vil være relevant at have særlig fokus på ved efterfølgende øvelser.

Øvelserne kan af praktiske årsager samkøres med og afholdes som en del af de generelle beredskabsøvelser.

Øvelser kan gennemføres på mange måder (procedureøvelser, fuldskalaøvelser osv.), og der kan hertil henvises til Beredskabsstyrelsens vejledninger, som findes på www.brs.dk under ”øvelser”. Politiet skal som udgangspunkt ikke medvirke, men kan eventuelt vejlede om metoder, og det kan med fordel drøftes, om det er relevant at inddrage virksomhedens øvelser i de øvelser, der i forvejen afholdes af politiet og de øvrige beredskabsmyndigheder.

2.1.5. Strafansvar

Det skal bemærkes, at manglende iagttagelse af virksomhedens ansvar efter risikobekendtgørelsens § 11, kan være forbundet med strafansvar. Således kan det straffes med bøde, hvis virksomheden undlader at indsende sårbarhedsvurderingen eller sikringsplanen (hvor dette er besluttet af politiet), ikke gennemfører sikringsforanstaltningerne inden for fristen, ikke foretager gennemgang og ajourføring af dokumenterne, ikke efterkommer politiets påbud osv., jf. risikobekendtgørelsens § 29, stk. 4. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens kapitel 5.

2.2. POLITIET

2.2.1. Godkendelse af sårbarhedsvurdering og sikringsplan

Som før anført er det virksomhedens ansvar at udarbejde sårbarhedsvurderingen og sikringsplanen og indsende dokumenterne til politiet. Politiet er den myndighed, der skal godkende dokumenterne, og deltager således ikke som sådan i selve udarbejdelsen, men kan i et vist omfang vejlede virksomheden om udarbejdelsen, herunder om de relevante sårbarheder og trusler, som virksomheden kan forholde sig til.

På baggrund af sårbarhedsvurderingen vurderer politiet, hvorvidt virksomheden har et acceptabelt sikringsniveau. Findes det ikke at være tilfældet, beslutter politiet, at virksomheden tillige skal udarbejde en sikringsplan og udpege en sikringsansvarlig, jf. risikobekendtgørelsens § 11, stk. 2. Sikringsplanen sendes også til politiet til godkendelse, jf. risikobekendtgørelsens § 11, stk. 3.

2.2.2. Inddragelse af andre myndigheder

Politiet hører inden godkendelsen af sikringsplanen relevante myndigheder, jf. risikobekendtgørelsens § 11, stk. 3, 2. pkt. Høringen af relevante myndigheder har til formål at orientere disse om de sikringsforanstaltninger, der påtænkes gennemført på virksomheden med henblik på at forhindre, at der etableres foranstaltninger, som ikke harmonerer med anden sektorlovgivning.

Det skal understreges, at sikringsplanen (og sårbarhedsvurderingen) i sagens natur kan indeholde følsomme oplysninger, som ikke er egnede til udbredelse til uvedkommende. ”Relevante myndigheder” skal derfor alene forstås som de myndigheder, hvor politiet vurderer, at en høring er nødvendig på grund af risikoen for, at sådanne snitfladeproblematikker kan opstå i forhold til de pågældende myndigheders sektorlovgivning. Relevante myndigheder i denne sammenhæng vil typisk være risikomyndighederne, men er ikke begrænset til disse. I tvivlstilfælde anbefales det at drøfte med den pågældende myndighed, hvorvidt der risiko for sådanne snitfladeproblematikker, inden der foretages en egentlig høring (og dermed udlevering af sikringsplanen eller dele heraf).

Høringen af de relevante myndigheder kan helt undlades eller begrænses, hvis politiet anser det for nødvendigt til beskyttelse af væsentlige sikkerhedsmæssige hensyn, herunder hensyn til forebyggelse, efterforskning og forfølgning af lovovertrædelser. Denne beslutning beror på politiets konkrete vurdering af oplysningerne i sikringsplanen. Se i øvrigt afsnit 6. OFFENTLIGHED OG AKTINDSIGT. Findes hensynene kun at gøre sig gældende for en del af oplysningerne i sikringsplanen, kan politiet således i stedet foretage høringen over de bestemte oplysninger/dele af sikringsplanen.

Hvis politiet eksempelvis vurderer, at det er nødvendigt at høre Arbejdstilsynet for at påse, at en bestemt påtænkt indretning af virksomheden ikke strider mod arbejdsmiljøreglerne, men at oplysningerne i sikringsplanen i øvrigt (helt eller delvist) bør undtages på grund af ovennævnte hensyn, kan høringen således begrænses til alene at angå oplysningen om den påtænkte indretning (og eventuelt andre oplysninger, som ikke undtages).

Det fremgår af risikobekendtgørelsens § 11, stk. 5, sidste pkt., at politiet i fornødent omfang orienterer de øvrige risikomyndigheder ved ajourføring af sårbarhedsvurderingen og sikringsplanen. Orienteringen skal ses i sammenhæng med høringspligten, således at det som udgangspunkt kun anses for fornødent at orientere de relevante myndigheder om ændringer i de oplysninger, de pågældende myndigheder har været hørt over i forbindelse med godkendelsen af sikringsplanen efter § 11, stk. 3, 2. pkt. Dette indebærer også, at såfremt virksomheden ikke har udarbejdet en sikringsplan men alene ajourført dens sårbarhedsvurdering, vil det ikke være fornødent at orientere andre myndigheder om den ajourførte sårbarhedsvurdering.

Hvis der ved ajourføringen tilføjes helt nye sikringsforanstaltninger i sikringsplanen eller sker væsentlige ændringer i bestående sikringsforanstaltninger, bør der foretages en egentlig høring af de relevante myndigheder med henblik på at sikre snitfladerne til anden sektorlovgivning.

Får en anden myndighed dokumenterne eller uddrag heraf i besiddelse i forbindelse med høringen/orienteringen, bør der udvises særlig opmærksomhed i forhold til udlevering af dokumenterne eller oplysningerne heri til udenforstående, se nærmere i afsnit 6. OFFENTLIGHED OG AKTINDSIGT.

2.2.3. Påbud om ændring

Efter risikobekendtgørelsens § 11, stk. 7, kan politiet meddele virksomheden påbud om ændring af sårbarhedsvurderingen og sikringsplanen, når:

- det på baggrund af en konkret trusselsvurdering (som følge af en ændret trusselsvurdering, en erkendt trussel eller en konkret sikringsrelateret hændelse) skønnes nødvendigt for at forebygge forsætlige skadevoldende handlinger, eller
- der ved ajourføring, øvelser, tilsyn eller lignende konstateres utilstrækkelig sikring i den godkendte sikringsplan i forhold til potentielle skadevoldende handlinger eller fejl og mangler i øvrigt

For så vidt angår den første pind kan som eksempel tænkes den situation, at der sker et terrorangreb mod en risikovirksomhed i udlandet, hvor der ses et modus hos gerningsmændene, som der ikke er taget højde for hos en lignende risikovirksomhed i Danmark. I denne situation kan det efter omstændighederne være relevant for politiet at bede virksomheden om at forholde sig til denne trussel i sårbarhedsvurderingen og sikringsplanen. Politiet og virksomheden bør først og fremmest søge en løsning gennem dialog, inden der eventuelt skrides til påbud.

2.2.4. Tilsyn

Når virksomheden har udarbejdet en sikringsplan, skal politiet regelmæssigt foretage tilsyn med, at planen overholdes. Politiet kan herunder afprøve effektiviteten af sikringsplanen og foretage uanmeldte tilsyn, jf. risikobekendtgørelsens § 11, stk. 8.

Der er ikke i risikobekendtgørelsen fastsat en bestemt tilsynsfrekvens. Hvis politiet finder det hensigtsmæssigt, kan tilsynet med sikringsplanens overholdelse eventuelt tilrettelægges i sammenhæng med eller i forlængelse af de tilsyn, som risikomyndighederne gennemfører i fællesskab i forhold til virksomhedernes overholdelse

af de øvrige krav i risikorisikobekendtgørelsen (sikkerhedsrapporten, forebyggelsesplanen m.v.). Risikomyndighedernes planlagte tilsyn følger et tilsynsprogram, som mindst skal omfatte ét årligt fysisk tilsyn på virksomheden, med mindre der efter en systematisk vurdering af risikoen for større uheld er fastlagt et længere interval, jf. risikobekendtgørelsens §§ 20-22 og bilag 9.

2.2.5. Afgørelser og klageadgang

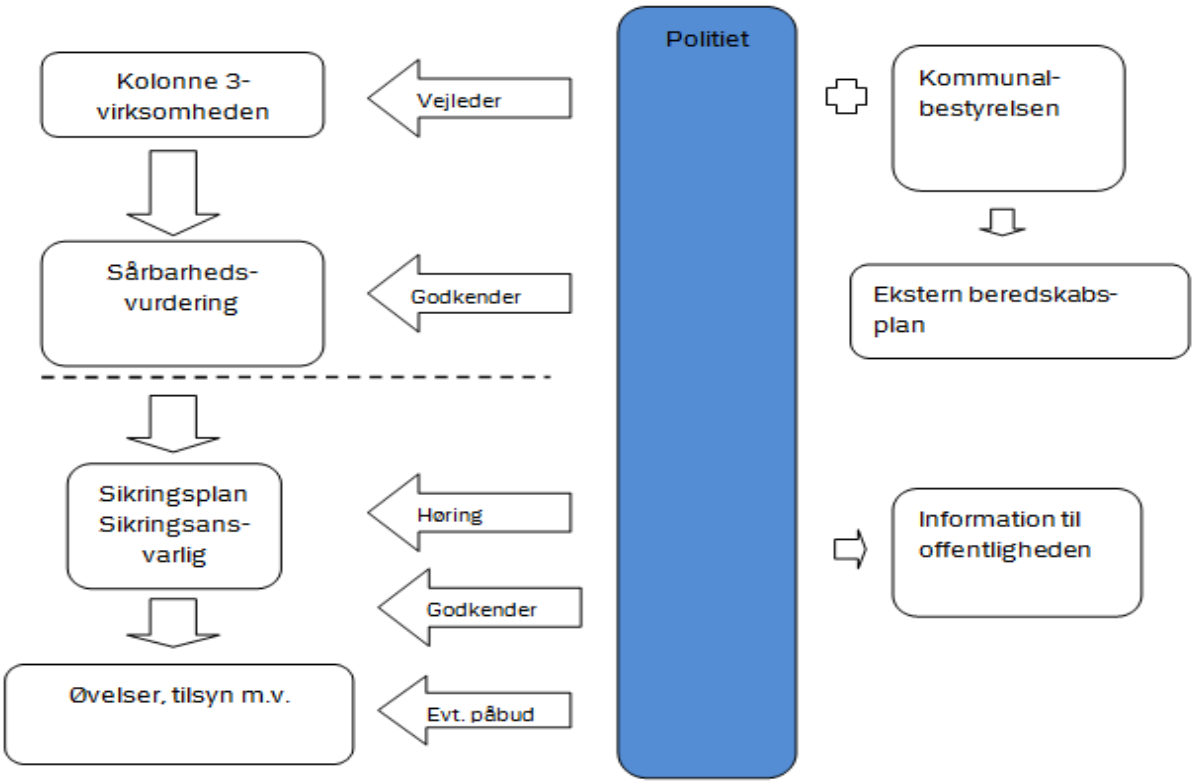
Politiets afgørelser efter risikobekendtgørelsens § 11, herunder vedrørende godkendelse af sårbarhedsvurderingen og sikringsplanen, afholdelse af øvelser og påbud, er omfattet af de almindelige forvaltningsretlige regler om partshøring, begrundelse, klagevejledning m.v.

Afgørelserne kan påklages til Rigspolitiet, Almen Jura, Polititorvet 14, 1780 København V. Klagen skal dog indledningsvis indgives til politikredsen, som sender sagens akter og en udtalelse til Rigspolitiet.

2.2.6. Politiets opgaver i forhold til risikovirksomheder

Det bemærkes endeligt, at politiet efter risikobekendtgørelsen - ud over arbejdet med sårbarhedsvurderinger og sikringsplaner - har til opgave at udarbejde en ekstern beredskabsplan i samarbejde med kommunalbestyrelsen, jf. bekendtgørelsens § 15, stk. 1, samt informere offentligheden om bl.a. forholdsregler ved uheld på virksomheden m.v. jf. § 16, stk. 2.

Politiets opgaver kan illustreres således:



3. FORSÆTLIGE SKADEVOLDENDE HANDLINGER

3.1. DEFINITION

Som anført indledningsvist er formålet med kravene om sikring af kolonne 3-virksomheder at forebygge såkaldte forsætlige skadevoldende handlinger mod eller med virksomhedens farlige stoffer.

"Forsætlig skadevoldende handling" er i risikobekendtgørelsens § 4, nr. 17, defineret som en handling, der har karakter af et angreb mod risikovirksomheden, som er omfattet af straffelovens § 114, stk. 1, eller ulovlig indtrængen på virksomheden med henblik på tyveri af farlige stoffer med det formål at anvende disse til en handling, som er omfattet af straffelovens § 114, stk. 1.

Straffelovens § 114, stk. 1 (populært kaldet "terrorparagraffen"), lyder således:

§ 114. For terrorisme straffes med fængsel indtil på livstid den, som med forsæt til at skræmme en befolkning i alvorlig grad eller uretmæssigt at tvinge danske eller udenlandske offentlige myndigheder eller en international organisation til at foretage eller undlade at foretage en handling eller at destabilisere eller ødelægge et lands eller en international organisations grundlæggende politiske, forfatningsmæssige, økonomiske eller samfundsmæssige strukturer begår en eller flere af følgende handlinger, når handlingen i kraft af sin karakter eller den sammenhæng, hvori den begås, kan tilføje et land eller en international organisation alvorlig skade:

1) *Manddrab efter § 237.*
2) *Grov vold efter § 245 eller § 246.*
3) *Frihedsberøvelse efter § 261.*
4) *Forstyrrelse af trafiksikkerheden efter § 184, stk. 1, retsstridige forstyrrelser i driften af almindelige samfærdselsmidler m.v. efter § 193, stk. 1, eller groft hærværk efter § 291, stk. 2, hvis disse overtrædelser begås på en måde, der kan bringe menneskeliv i fare eller forårsage betydelige økonomiske tab.*
5) *Kapring af transportmidler efter § 183 a.*
6) *Overtrædelser af lovgivningen om våben og eksplosivstoffer under særligt skærpende omstændigheder efter § 192 a.*
7) *Brandstiftelse efter § 180, sprængning, spredning af skadevoldende luftarter, oversvømmelse, skibbrud, jernbane- eller anden transportulykke efter § 183, stk. 1 og 2, sundhedsfarlig forurening af vandforsyningen efter § 186, stk. 1, sundhedsfarlig forurening af ting bestemt til almindelig udbredelse m.v. efter § 187, stk. 1.*
8) *Besiddelse eller anvendelse m.v. af radioaktive stoffer efter § 192 b.*

Når der i denne vejledning tales om "sikring" af virksomheden, er det i betydningen sikring mod disse terrorhandlinger og ikke i forhold til f.eks. forebyggelse af uheld, som ellers er formålet med hovedparten af reglerne i risikobekendtgørelsen.

Sikringen af virksomheden skal i stedet forebygge, at der kan gennemføres terrorhandlinger mod virksomheden (de farlige stoffer) og/eller tyveri af de stoffer, som vil kunne anvendes til gennemførelse af en terrorhandling, der ikke er rettet mod virksomheden selv.

Som ”farlige stoffer” forstås de stoffer, der udløser, at virksomheden kategoriseres som en kolonne 3-virksomhed i risikobekendtgørelsen. Et ”farligt stof” er i risikobekendtgørelsens § 4, nr. 7, defineret som et stof eller en blanding, hvis farekategori er omfattet af bilag 1, del 1, eller som er opført som navngivet stof i bilag 1, del 2, herunder i form af råstof, produkt, biprodukt, reststof eller mellemprodukt.

Som anført i straffelovens § 114, stk. 1, betegnes det som terrorisme, når den ulovlige handling sker af de grunde, som er nævnt i bestemmelsen (forsættet), og når handlingen i kraft af sin karakter eller den sammenhæng, hvori den begås, kan tilføje et land eller en international organisation alvorlig skade.

De forsætlige skadevoldende handlinger, der er fokuseret på i reglerne i risikobekendtgørelsen, er altså de handlinger - eller forbrydelser - mod eller med virksomhedens farlige stoffer, som kan siges at have alvorlig negativ virkning på *samfundet*. Målet er således heller ikke at forebygge f.eks. hærværk eller erhvervsspionage, som nok kan have en negativ, økonomisk betydning for virksomheden, men som ikke har negativ betydning for samfundet som sådan. Virksomheden skal med andre ord have et samfundsmæssigt acceptabelt sikringsniveau. Når det er sagt, så vil sikringsforanstaltningerne naturligvis have en forebyggende effekt på terrorhandlinger såvel som andre ulovlige handlinger mod virksomheden.

3.2. TERRORTRUSLEN

Politiets Efterretningstjeneste (PET) har ansvaret for at vurdere terrortruslen mod Danmark. Efterretningstjenestens Center for terroranalyse (CTA) offentliggør i den forbindelse Vurdering af terrortruslen mod Danmark (VTD), som kan findes på efterretningstjenestens hjemmeside www.pet.dk. CTA udgiver desuden andre analyser, der vedrører forskellige aspekter af trusselsbilledet.

I den seneste VTD fra 7. februar 2017 vurderer CTA, at terrortruslen mod Danmark fortsat er alvorlig. Det betyder, at der er personer med intention om og kapacitet til at begå terrorangreb i Danmark. Angreb kan finde sted, uden at der på forhånd foreligger efterretningsmæssige indikationer herpå.

CTA vurderer samtidig, at der i Danmark er kapacitet til at udføre terrorangreb med kemiske stoffer i form af simple kemiske våben. Kapaciteten til at begå terror med anvendelse af kemiske stoffer vurderes dog som værende begrænset.

CTA vurderer, at der er en meget begrænset kapacitet til at fremstille kemiske stoffer, der kan anvendes i en angreb. Kemiske stoffer til et terrorangreb vil derfor skulle anskaffes. Dette kan ske ved indbrud eller tyveri hos virksomheder, der ligger inde med kemiske materialer, der kan benyttes til fremstilling af simple kemiske våben. Manglende eller fraværende sikkerhedsforanstaltninger hos virksomheder, der opbevarer kemiske materialer, kan dermed bidrage til at øge terrortruslen mod Danmark.

4. UDARBEJDELSE AF SÅRBARHEDSVURDERING

I sårbarhedsvurderingen klarlægges virksomhedens sikringsniveau i forhold til forsætlige skadevoldende handlinger. Sårbarhedsvurderingen skal give et samlet overblik over sårbarheder og trusler sammenholdt med virksomhedens eksisterende sikringsniveau, hvorved der identificeres et eventuelt behov for yderligere sikring af virksomheden. I så fald skal sårbarhedsvurderingen også indeholde anbefalinger til forbedring af sikringen.

Sårbarhedsvurderingen skal således give politiet de nødvendige oplysninger til brug for vurderingen af, om der er et acceptabelt sikringsniveau på virksomheden, eller om der er behov for, at der tillige udarbejdes en sikringsplan og udpeges en sikringsansvarlig. Det skal understreges, at det er afgørende for politiets mulighed for at fortage denne vurdering, at beskrivelserne i sårbarhedsvurderingen er både dækkende og præcise for de faktiske forhold på virksomheden.

I dette afsnit beskrives, hvordan sårbarhedsvurderingen udarbejdes, herunder hvilke oplysninger den skal indeholde, ligesom der gives forslag til metoder til brug for risikovurderingsprocessen og forslag til, hvilke spørgsmål, problemer og risici, det som udgangspunkt vil være naturligt at overveje i forbindelse med udarbejdelsen.

Sårbarhedsvurderingen skal mindst indeholde de oplysninger, der fremgår af risikobekendtgørelsens bilag 6, del 1. Virksomheden kan eventuelt anvende det vedlagte Bilag 1 Skabelon til sårbarhedsvurdering, hvor de overordnede indholdskrav er oplistet. Beskrivelserne tilpasses den enkelte virksomheds helt konkrete forhold, og da der er tale om mindstekrav i bekendtgørelsen, skal listen over oplysninger ikke forstås som udtømmende. Virksomheden bør derfor også overveje, om der er andre oplysninger, som vil være relevante at medtage i sårbarhedsvurderingen i forhold til at kunne bedømme virksomhedens sikringsmæssige forhold.

Der kan med fordel hentes inspiration - med de justeringer, som måtte være relevante - i virksomhedens anmeldelse og sikkerhedsrapport, som indeholder nogle af de samme oplysninger om virksomheden og de farlige stoffer, jf. risikobekendtgørelsens bilag 2 og 4, som sårbarhedsvurderingen skal indeholde. Det anbefales ikke blot at henvise til oplysningerne i anmeldelsen og/eller sikkerhedsrapporten, da sårbarhedsvurderingen udgør et selvstændigt dokument og skal kunne læses uafhængigt af de øvrige dokumenter, men der kan eventuelt kopieres og/eller vedlægges uddrag herfra m.v.

4.1. INDLEDNING

Sårbarhedsvurderingen indledes med en kort beskrivelse af baggrunden og formålet samt eventuelle definitioner.

Der kan i indledningen henvises til, at sårbarhedsvurderingen er udarbejdet efter risikobekendtgørelsens § 11 og bilag 6, del 1, under anvendelse af nærværende vejledning og eventuelt andet vejledningsmateriale.

Beskrivelsen af formålet kan inddrage det overordnede formål med risikobekendtgørelsens § 11, nemlig at forebygge forsætlige skadevoldende handlinger, ligesom sårbarhedsvurderingen har til formål at oplyse om virksomhedens sikringsniveau i forhold til disse handlinger og opstille eventuelle anbefalinger til forbedring af sikringen.

Endvidere skal indledningen indeholde oplysninger om navn, stilling og telefonnummer på den/de personer, som har udarbejdet dokumentet med henblik på, at politiet kan kontakte pågældende.

Såfremt eksterne rådgivere, politiet eller andre har vejledt eller på anden måde været involveret i udarbejdelsen af sårbarhedsvurderingen, bør dette tillige fremgå.

4.2. GENEREL BESKRIVELSE AF VIRKSOMHEDEN OG DE FARLIGE STOFFER

Afsnittet skal blandt andet indeholde oplysninger om virksomhedens navn, adresse, telefonnummer og CVR-nummer samt eventuelle P-numre til brug for identificering af de enkelte produktionsenheder, hvis virksomheden har flere, og ellers en entydig identifikation af den produktionsenhed/lokalitet, som sårbarhedsvurderingen gælder for.

Herudover skal der anføres en alment forståelig beskrivelse af aktivitet eller påtænkt aktivitet på virksomheden, herunder oplag.

Endelig skal der være en identifikation af de farlige stoffer, som er til stede eller kan være til stede på virksomheden, herunder stoffernes mængde, fysiske tilstand, almindelige betegnelse samt en alment forståelig angivelse af stoffernes vigtigste farlige karakteristika. Det bemærkes her, at relevante oplysninger om virksomhedens potentielle farlighed, herunder om konsekvenszoner, også med fordel kan gengives fra sikkerhedsrapporten.

4.3. VIRKSOMHEDENS ORGANISATION

I dette afsnit beskrives virksomhedens organisation, herunder ledelsessystemet/ sikkerhedsledelsessystemet og eventuelle sikringsorganisation, hvis en sådan er etableret.

Såfremt virksomheden har en sikringsorganisation, bør beskrivelsen indeholde de samme oplysninger om den sikringsansvarlige og personale med sikringsopgaver samt om uddannelse, træning og øvelser, som er påkrævet ved udarbejdelsen af en sikringsplan efter risikobekendtgørelsens bilag 6, del 2, nr. 3. Der henvises til kapitel 5.3. SIKRINGSORGANISATION og 5.4. UDDANNELSE, TRÆNING OG ØVELSER. Dog stiller risikobekendtgørelsen alene krav om, at den sikringsansvarlige meddeler samtykke til indhentelse af personoplysninger til brug for en vandelsvurdering, når denne udpeges efter politiets bestemmelse i forbindelse med, at der skal udarbejdes en sikringsplan, jf. risikobekendtgørelsens § 11, stk. 2.

Findes der ikke en egentlig sikringsorganisation, men er der personale med sikringsopgaver, eller som har modtaget særlig instruktion, uddannelse m.v. i forhold til sikring, kan dette i stedet anføres.

Herudover oplyses der generelt om det personale, som har adgang til de farlige stoffer på den eller de produktionsenheder/lokaliteter, som sårbarhedsvurderingen angår.

Det vil også være relevant at inddrage oplysninger om (eksternt) personale, der er stillet til rådighed af tredjemand, og som har opgaver eller adgang til farlige stoffer, der kan have betydning i den sikringsmæssige sammenhæng.

Det bemærkes, at beskrivelsen af eget/eksternt personale med sikringsopgaver og/eller adgang til de farlige stoffer ikke skal indeholde personoplysninger om de enkelte ansatte, men der kan eventuelt inddeles i funktioner, faggrupper osv., alt efter, hvad der findes mest hensigtsmæssigt. Antallet af personer inden for de enkelte funktioner m.v. skal anføres.

4.4. FYSISK BELIGGENHED OG INDRETNING

Afsnittet skal indeholde en mere detaljeret beskrivelse af virksomhedens fysiske beliggenhed og indretning, herunder beskrivelse af vigtig ejendom og infrastruktur, placeringen af farlige stoffer osv.

Her skal blandt andet fremgå nærmere oplysninger om virksomhedens placering og afgrænsning, areal(er) og omgivelser (f.eks. om virksomheden er beliggende i bymæssig bebyggelse eller er omkranset af åbne arealer), om naborisikovirksomheder osv.

Det er vigtigt at få kortlagt placeringen af alle relevante objekter på virksomhedens område så som bygninger, anlæg, områder m.v., hvor der er oplag eller sker håndtering af farlige stoffer, og en beskrivelse af de pågældende objekters karakter og funktion.

Adgangsveje til virksomheden og de pågældende objekter skal ligeledes beskrives. Det gælder alle typer adgangsveje, det være sig veje, tunneler, fra vandsiden osv.

Beskrivelsen skal suppleres med kortmateriale, hvor de beskrevne forhold er markeret. Kortmaterialet skal blandt andet vise virksomhedens placering og afgrænsning, bygninger, anlæg, adgangsveje osv.

4.5. EKSISTERENDE SIKRINGSFORHOLD

Som anført i indledningen er det Rigspolitiets opfattelse, at risikovirksomheder - særligt de større - i vidt omfang allerede sikrer sig mod eksempelvis uautoriseret adgang for at imødegå tyveri, spionage, hærværk m.v., men ikke nødvendigvis mod egentlige terrorhandlinger.

I det omfang, der er etableret sikringsforanstaltninger på virksomheden, som kan have indflydelse på forebyggelsen af forsætlige skadevoldende handlinger, er det vigtigt, at disse beskrives præcist og detaljeret i dette afsnit.

Det er de faktiske forhold på virksomheden, der er afgørende at få beskrevet, og således er det ikke relevant, hvilket udstyr eller indretninger, der ikke er til rådighed. Sikringsforanstaltninger, som ikke er etableret (endnu), men som anbefales til forbedring af virksomhedes sikring, skal derimod beskrives i konklusion og anbefalinger, jf. afsnit 4.7. KONKLUSION OG ANBEFALINGER.

Det har indvirkning på virksomhedens sikringsniveau, i hvilket omfang de eksisterende sikringsforanstaltninger har kapacitet til at imødegå en forhøjet trussel. Afsnittet bør derfor også indeholde oplysninger om, hvorvidt virksomheden har etableret procedurer for ændringer i beredskabsniveauer og i så fald en beskrivelse af, hvad de procedurer indebærer. Der henvises til kapitel 5.6. PROCEDURER FOR NORMALT BEREDSKABSNIVEAU og 5.7. PROCEDURER FOR FORHØJET BEREDSKABSNIVEAU.

Som eksempler på **eksisterende sikringsforanstaltninger**, herunder allerede etableret sikringsudstyr og -indretninger, kan nævnes:

- Perimetersikring (indhegning, belysning, naturlige barrierer osv.)
- Kameraovervågning (placering og kameravinkler)
- Adgangskontrol (tidsrum, evt. zoneinddeling, hvordan foretages kontrollen, opsyn med besøgende m.v.)
- Alarmering (AIA-automatisk indbrudsalarm, ADK-automatisk adgangskontrol, ABA-automatisk brandalarmeringsanlæg)
- Kommunikationsudstyr
- Procedurer for beredskabsniveauer
- Procedurer ved indbrudsalarm, brand og evakuering, sikringsrelaterede hændelser m.v.

Det anbefales også at beskrive eksisterende sikringsforanstaltningers styrker, svagheder og pålidelighed/holdbarhed, da det kan have betydning for, om foranstaltningerne virker tilstrækkeligt.

De eksisterende sikringsforanstaltninger skal så vidt muligt fremgå af kortmaterialet, hvor foranstaltningerne er markeret tydeligt. Det kan være placeringen af hegn, særligt adgangsbegrænsede områder, overvågningsudstyr, porte, belysning osv.

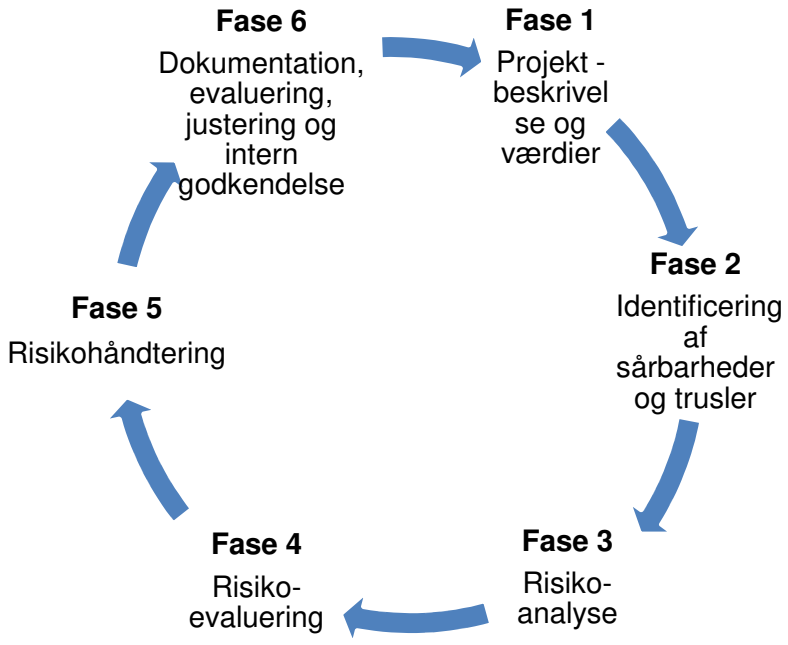
4.6. RISIKOVURDERING

Ansvaret for udarbejdelsen af sårbarhedsvurderingen påhviler som anført virksomheden, og det er også op til virksomheden selv, hvilken fremgangsmåde, model, form osv., der anvendes til brug herfor. Der er med andre ord metodefrihed i forhold til risikovurderingen.

Der findes flere, branchespecifikke metoder og værktøjer til risikovurderinger. Eksempelvis har Beredskabsstyrelsen udarbejdet nogle værktøjer, herunder ROS-modellen, som kan findes på www.brs.dk.

Rigspolitiet kan anbefale nedenstående metode, som er tilpasset risikovirksomheder. Metoden gennemføres med et overordnet sigte og anvender primært kvalitative data. Kvaliteten af risikovurderingen er derfor afhængig af, at de rette kompetencer/ressourcepersoner bidrager til arbejdet, herunder i identificeringsprocesserne og indekseringen i forhold til sandsynlighed og konsekvens. Metoden er inddelt i faser, så der fastholdes en struktureret proces.

Der anvendes et såkaldt **"sikringshjul"** til risikovurderingen ved denne metode:



4.6.1. Fase 1 Projektbeskrivelse og værdier

Før virksomheden udfærdiger en risikovurdering, er det vigtigt at samle de rette kompetencer/ressourcepersoner. Relevante ressourcepersoner er eksempelvis personale, som har et indgående kendskab til og ansvar for virksomhedens drift, det være sig mellemledere, sikkerhedsledere og medlemmer af sikkerheds- og/eller sikringsorganisationen. Personer med forskellige ansvarsområder og faglighed bidrager til en mere komplet risikovurdering. Virksomheden kan overveje, om eksterne ressourcepersoner også skal indgå i arbejdet.

Indledningsvis udarbejdes en kort projektbeskrivelse for risikovurderingen, hvor virksomhedens værdier beskrives. Som før omtalt er de værdier, virksomheden skal identificere og risikovurdere på efter risikobekendtgørelsen, afgrænset til virksomhedens

farlige stoffer. Risikovurderingen skal således omhandle, hvordan virksomhedens farlige stoffer beskyttes mod forsætlige skadevoldende handlinger.

4.6.2. Fase 2 Identificering af sårbarheder og trusler

En effektiv måde at identificere sårbarheder og trusler på er gennem en simpel, men struktureret brainstorm hos ressourcepersonerne.

Sårbarhederne er de lokaliteter, forhold, situationer, procedurer osv., som direkte eller indirekte påvirker sikringen af virksomheden i forhold til de farlige stoffer.

Følgende **sårbarheder** kan medtages (ikke udtømmende) i identificeringsprocessen:

- Opbevaringsanlæg
- Driftsanlæg
- Produktionsanlæg
- Sikkerhedsanlæg
- Håndterings- og vedligeholdelsessituationer
- Energi, el og vandtilførsel
- Transport og håndtering af de farlige stoffer på virksomhedens område
- Personale
- Leverandører/tredjeparter (renovation, kantinelevering, anden afhentning og levering m.v.)
- Sikkerhedsprocedurer
- IT-systemer, som kan have indvirken på de farlige stoffer (cyberangreb)
- Virksomhedens indretning
- Kommunikation internt og eksternt

Truslerne er de forskellige former for forsætlige skadevoldende handlinger, altså terrorhandlinger mod virksomheden eller ulovlig indtrængen med henblik på tyveri af farlige stoffer med det formål at anvende dem til terrorhandlinger, som er omfattet af straffelovens § 114, stk. 1.

Følgende **trusler** kan medtages (ikke udtømmende) i identificeringsprocessen:

- Uautoriseret adgang på virksomheden, f.eks. kørende, gående eller via vandsiden, eventuelt efter forcering af perimetersikring (hegn m.v.)
- Smugling af personer, eksplosiver, våben og andet ind på virksomhedens areal eventuelt via vareleverancer, renovation m.v.
- Beskadigelse eller ødelæggelse af virksomheden eller dele heraf eksempelvis ved sprængstofsanordninger, ildspåsættelse m.v.
- Modtagelse af mistænkelige forsendelser (post, pakker m.v.)
- Tyveri og udsmugling af farlige stoffer fra virksomheden
- Tyveri af sikringsudstyr, id-kort, dokumenter m.v. på virksomhedens område
- Manipulation af de farlige stoffer, herunder ved cyberangreb
- Indbrud på virksomheden eller i lagerområder og bygninger i grænsefladen, hvor uvedkommende uset eller nemt kan tilsnige sig adgang
- Nedbrud eller sabotage mod alarmer/TV-overvågning på perimeter- og skalsikringen
- Droner på virksomhedens område

Virksomheden skal udvælge realistiske trusler/trusselsscenarier over for de enkelte sårbarheder. Formålet med brainstormmetoden er at identificere så mange sårbarheder og trusler, som deltagerne kan komme i tanke om, for derefter at "skære til". Herefter grupperes sårbarheder og trusler i overordnede emner, som analyseres nærmere. Ved at gruppere sårbarheder og trusler i overordnede emner, opnås et mere generelt sikringsniveau, hvilket også vil omfatte de trusler, som virksomheden ikke har mulighed for at identificere eller forudse.

Når sårbarhederne er identificeret, vurderes det, hvilken **fare** der vil kunne indtræffe, hvis sårbarheden udsættes for en eller flere af truslerne. Ved en fare forstås en uønsket tilstand, hændelse eller begivenhed, som vil medføre tab af kontrol med de farlige stoffer og en eller flere konsekvenser. En fare kan eksempelvis være eksplosion på et lager med farlige stoffer eller tyveri af disse. Identificeringen og vurderingen af den potentielle fare, som sårbarheden indeholder, hjælper til at vurdere konsekvensen af, at sårbarheden angribes.

De konsekvenser, som skal medtages i risikovurderingen, er konsekvenser for samfundet og de samfundskritiske funktioner, som betegner de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets funktionsdygtighed, og som skal kunne opretholdes og videreføres i tilfælde af en forsætlig skadevoldende handling.

Konsekvenser for samfundet identificeres inden for fire grupper:

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

De præcise konsekvenser kan være svære at vurdere på forhånd, men ud fra en "worst case"-tilgang beskrives den mulige konsekvens forårsaget af en realistisk trussel for hver af sårbarhederne.

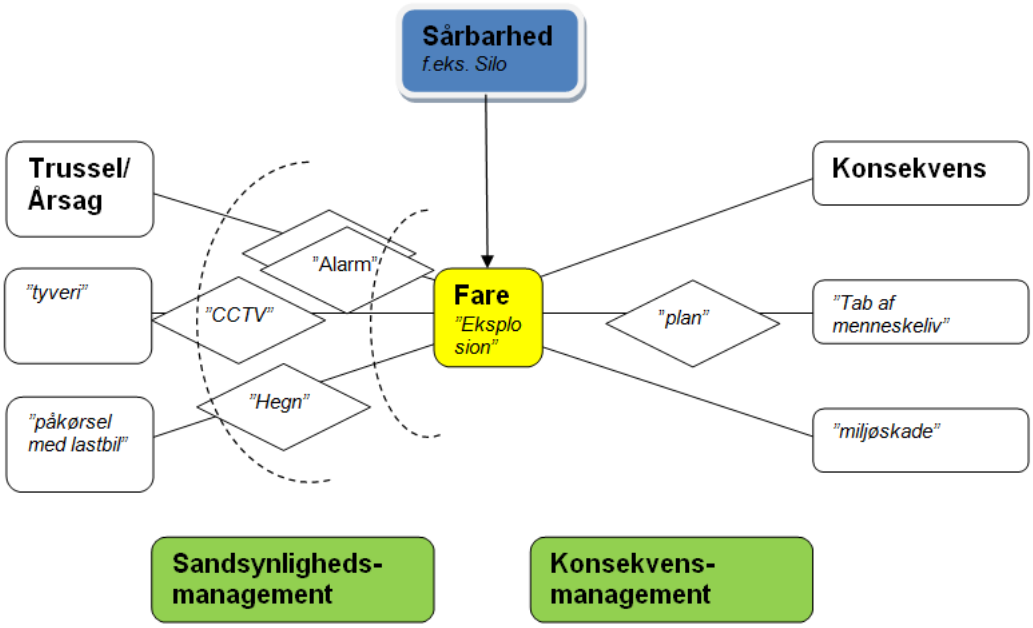
ROS-modellens bilag A på www.brs.dk beskriver de samfundskritiske funktioner mere detaljeret.

4.6.3. Fase 3 Risikoanalyse

Formålet med risikoanalysen er at skabe forståelse for sammenhængen mellem trusler, sårbarheder, farer og konsekvenser.

Virksomheden skal i denne fase for hver enkelt sårbarhed analysere, hvilke realistiske trusler, der forårsager en fare og derved medfører en eller flere konsekvenser. Risikoanalysen bidrager til at skabe et overblik og en forståelse, så effekten og placeringen af de eksisterende sikringsforanstaltninger kan inddrages i analysen.

En egnet model til at skabe et visuelt overblik er **"bow tie"-modellen**:



<> = Eksisterende sikringsforanstaltninger. Disse kan have effekt på en eller flere trusler og konsekvenser.
---- = Perimetersikring og skalsikring.

4.6.4. Fase 4 Risikoevaluering

Ved risikoevalueringen vurderes sandsynligheden for, at truslerne indtræder, og alvorligheden af konsekvensen ved en fare. Samlet i en risikomatrix vil det give et overblik over virksomhedens risikoprofil.

Det anbefales at sætte talværdi på både sandsynlighed og konsekvens, og når disse ganges med hinanden, fremkommer der en risikofaktor, som er et udtryk for risikoens farlighed og prioritet.

Sandsynlighed x Konsekvens = Risikofaktor

Inden sandsynligheden vurderes, er det vigtigt at have identificeret virksomhedens svagheder. Svaghederne skal medtages i sandsynlighedsvurderingen i forhold til trusler, sårbarheder og konsekvenser, da de vil kunne øge sandsynligheden for, at en forsætlig skadevoldende handling kan indtræffe samt mindske effekten af en eller flere af de eksisterende sikringsforanstaltninger.

Følgende er eksempler på **svagheder**, som kan medtages (ikke udtømmende) i identificeringsprocessen:

- Fysiske rammer og tilstand
- Overeksponering i medierne
- Associering med konfliktfyldte samarbejdspartnere eller interesseområder
- Oversigtsforhold (afskærmning, belysning, indsigt m.v.)
- Tilkørselsforhold
- Personale

Sandsynligheden for, at en forsætlig skadevoldende handling gennemføres på den konkrete virksomhed, skal vurderes i forhold til det trusselsniveau/trusselsbillede, som beskrives i den gældende Vurdering af Terrortruslen mod Danmark (VTD), se hertil afsnit 3.2. TERRORTRUSLEN, samt virksomhedens egen trusselsprofil. Såfremt virksomheden er eksponeret i medierne og/eller associeres med konfliktfyldte samarbejdspartnere eller interesseområder, kan dette medføre en øget sandsynlighed for, at virksomheden udsættes for en skadevoldende handling. Det kan være hensigtsmæssigt, at sandsynligheden indledningsvist vurderes på to måder; en sandsynlighed for, at den konkrete virksomhed udsættes for en forsætlig skadevoldende handling, hvilket påvirkes af virksomhedens trusselsprofil og VTDen, samt en sandsynlighed for, om den pågældende handling kan gennemføres under de eksisterende sikringsforanstaltninger. I vejledningen tages udgangspunkt i en samlet sandsynlighed, som omfatter begge disse tilgange.

Trusselsniveauet for en forsætlig skadevoldende handling er dynamisk og aldrig konstant, men sandsynligheden vurderes ud fra normalbilledet, som anvendes ved virksomhedens normale beredskabsniveau. Det er dog vigtigt for virksomheden at notere sig, hvilke eksisterende sikringsforanstaltninger, der har kapacitet til at imødekomme en forhøjet trussel, som anvendes ved forhøjet beredskabsniveau.

Sandsynligheden vurderes i forhold til de eksisterende sikringsforanstaltningers effekt, og samtlige udvalgte trusler og konsekvenser indekseres som illustreret i Bilag 2 Sandsynlighedsindeks og konsekvensindeks og i Bilag 3 Risikovurderingsskema.

Sandsynligheden for, at en given forsætlig skadevoldende handling indtræffer, er vanskelig at vurdere, hvorfor indekseringen skal ses som en måde til at prioritere truslerne.

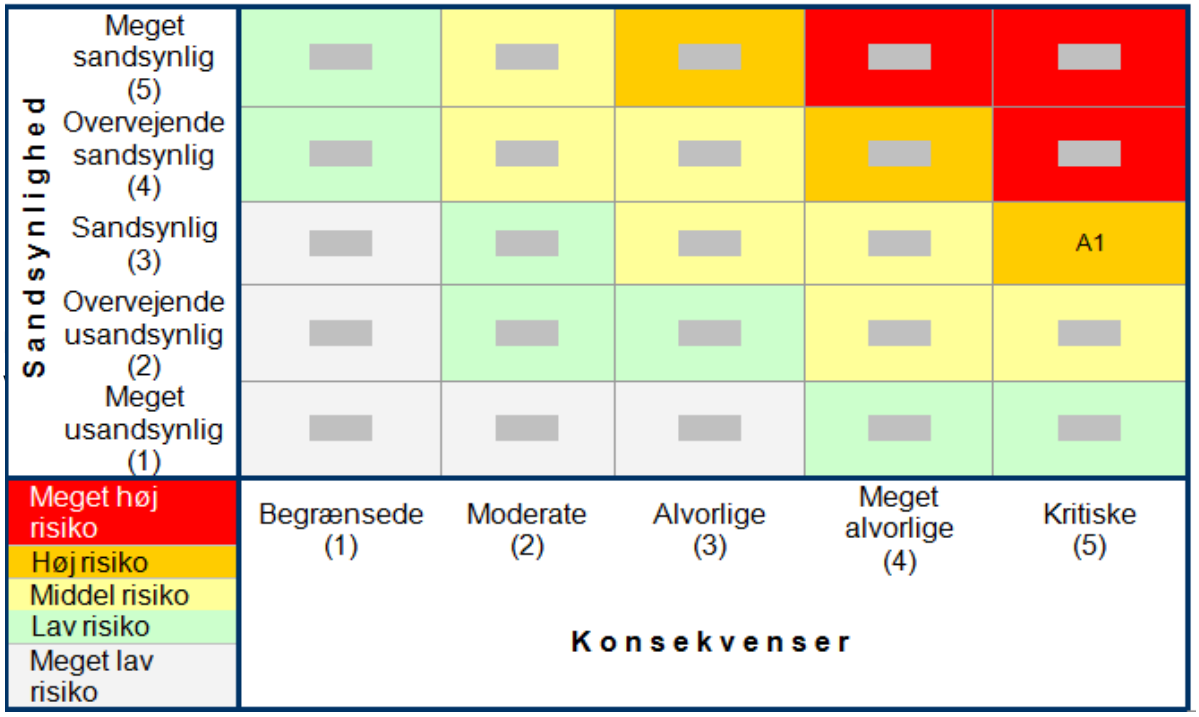
Når sandsynligheden er indekseret, skal de samfundsmæssige konsekvenser vurderes og indekseres. Virksomheden kan med fordel vælge at udarbejde en særskilt og intern risikovurdering, hvor de virksomhedsmæssige konsekvenser medtages. Erfaringer fra terrorangreb i Europa har f.eks. vist, at virksomheder kan lide store og langvarige tab af finansielle aktiver, markedsandele og omdømme efter et terrorangreb.

Konsekvenserne indekseres på baggrund af deres maksimale potentielle konsekvens. Risikovurderingsskemaet i bilag 3 anvendes således, at den potentielle delkonsekvens bestemmer, hvordan den samlede konsekvens indekseres. Flere tab af menneskeliv vil eksempelvis altid indekseres som ”kritiske” (5), selvom der ikke sker afbrydelse af samfundets kritiske funktioner.

Når alle relevante sandsynligheder og konsekvenser er identificeret, analyseret og prioriteret med tal, kan man sammenstille de analyserede risici i en risikomatrix. Det giver et godt overblik over virksomhedens risikoprofil.

Nedenstående er et eksempel på en **risikomatrix** udfyldt for én trussel og én konsekvens:

Sårbarhedsbeskrivelse:	**Trusler og fare:**	**Konsekvenser:**
A. Lagersilo	*Trussel 1: Påkørsel med bil/lastbil* *Fare: udslip af 3 tons farligt stof.*	*Tab af flere menneskeliv og omfattede miljøskade på omgivende vandmiljø.*



Når risikoen er identificeret, vurderes muligheden for at nedbringe den ved etablering af sikringsforanstaltninger, eller om risikoen skal accepteres som værende så lav som praktisk mulig.

Nedenstående skema viser, hvordan virksomheden bør agere ud fra en given **risikofaktor**:

Risikoens alvorlighed = risikofaktor	**Hvordan skal der handles**
20-25. Risiko kan ikke tolereres	En risiko, der ikke kan tolereres, skal fjernes med det samme.
15-16. Alvorlig risiko	En alvorlig risiko bør fjernes med det samme.
8-12. Moderat risiko	En moderat risiko bør fjernes eller begrænses.
4-6. Risiko kan tolereres	En risiko, der kan tolereres, bør medtages i forbindelse med fastsættelse af mål.
1-3. Ubetydelig risiko	En ubetydelig risiko kræver ingen handling her og nu.

4.6.5. Fase 5 Risikohåndtering

I risikohåndteringsfasen er formålet, at der ageres mest hensigtsmæssigt på risici, der ikke kan accepteres, så sikringsniveauet bliver acceptabelt. Det skal også overvejes, om de identificerede risici skal reduceres yderligere, selvom de måtte ligge inden for det acceptable.

Risikohåndteringsfasen er medtaget under sårbarhedsvurderingen, idet det danner grundlaget for de eventuelle anbefalinger til forbedring af virksomhedens sikring.

Virksomheden udvælger de sikringsforanstaltninger, som vil give størst effekt på sikringsniveauet, uden at der er trusselsspecifikke "huller" i sikringen af virksomheden. Her er det ofte hensigtsmæssigt at vælge sikringsforanstaltninger, der supplerer og understøtter hinanden.

I udvælgelsen af sikringsforanstaltningerne skal der samtidig tages hensyn til proportionaliteten, således at sikringen imødegår de faktiske risici, som virksomheden står over for.

"Bow tie"-modellen kan med fordel anvendes til at vise et billede af, hvor sikringsforanstaltningerne skal placeres.

Ved udvælgelsen af yderligere sikringsforanstaltninger er det hensigtsmæssigt, at de virker flere forskellige steder og har forskellig karakter. Sikringsforanstaltninger kan blandt andet være menneskelige, tekniske, organisatoriske, forsinkende/forhindrende, detekterende, verificerede, reagerende osv. Sikringsforanstaltninger kan også styrkes ved at have understøttende sikringsforanstaltninger (f.eks. nødgenerator til overvågningssystemerne).

Virksomhedens sikring kan struktureres ved inddeling i zoner eller "ringe" omkring sårbarhederne, hvilket vil hjælpe med placeringen og typeudvælgelsen af sikringsforanstaltningerne. Som eksempler på zoner kan nævnes perimetersikring og skalsikring. Nogle sikringsforanstaltninger så som opmærksomhedskultur og procedurer virker mere generelt på sikringsniveauet og er svære at placere i zoner.

Sikringsforanstaltningerne kan overordnet inddeles i forebyggende og reaktive tiltag og har effekt på henholdsvis sandsynligheden eller konsekvensen.

Følgende eksempler på **sikringsforanstaltninger** (ikke udtømmende) kan anvendes i identificerings- og prioriteringsprocessen:

Forebyggende	Reaktive
• Overvågning (alarmsystemer) • Vagter og sikkerhedspersonale • Perimetersikring (sikring af området, herunder adgangskontrol, hegn, sensorer, porte, afskærmning, skiltning m.v.) • Skalsikring (sikring af bygninger, herunder døre og vinduer m.v.) • Vagtcentral • Adgangskort til ansatte • Besøgskontrol • Begrænset personaleadgang til relevante afdelinger • Fysisk indretning af virksomheden (belysning, tilkørselsforhold m.v.) • Kontrol af sikkerhedsprocedurer • Internt beredskab • Sikkerheds- og opmærksomhedskultur • Intern og ekstern kommunikation • Sikkerhedstjek	• Forsinkende foranstaltninger (røg, tågekanoner m.v.) • Automatiserede zonelåsesystemer • Intern beredskabsplan • Sikringsorganisation • Sikringsansvarlige • Krisestyring • Intern og ekstern kommunikation

På www.pet.dk findes der endvidere publikationer med generel information om sikkerhed, herunder om beskyttelse af virksomheder, sikkerhed ved ansættelser osv.

4.6.6. Fase 6 Dokumentation, evaluering, justering og intern godkendelse

Risikovurderingen dokumenteres, evalueres, justeres og godkendes internt af de relevante ressourcepersoner og kan herefter indgå i den samlede sårbarhedsvurdering.

4.7. KONKLUSION OG ANBEFALINGER

Sårbarhedsvurderingen afsluttes med en samlet konklusion om virksomhedens sikringsniveau over for forsætlige skadevoldende handlinger.

Hvis der på baggrund af risikoanalysen konstateres et behov for yderligere sikring af virksomheden, skal der i sårbarhedsvurderingen tillige opstilles anbefalinger til forbedring af sikringen.

Anbefalingerne skal indeholde forslag til konkrete sikringsforanstaltninger, som virksomheden vil indføre på baggrund af den godkendte sårbarhedsvurdering, herunder etablering af nye sikringsforanstaltninger og/eller forbedring af eksisterende. Forslagene kan være alt fra proceduremæssige ændringer til fysiske tiltag og uddannelse af personale.

De nye/ændrede sikringsforanstaltninger (fysiske tiltag) bør så vidt muligt tillige fremgå af kortmaterialet.

Det kan anbefales, at Fase 3. Risikoanalyse og Fase 4. Risikoevaluering, efterfølgende gennemføres igen, hvor de yderligere sikringsforanstaltninger indgår, for på den måde at kunne prioritere hvilke foranstaltninger, der vil være mest hensigtsmæssige at implementere.

4.8. GENNEMGANG OG AJOURFØRING

Endeligt beskrives den procedure, virksomheden vil anlægge i forhold til den periodiske gennemgang og ajourføring af sårbarhedsvurderingen, som er omtalt i afsnit 2.1. KOLONNE 3-VIRKSOMHEDEN.

4.9. POLITIETS GODKENDELSE

Det kan efter omstændighederne være formålstjenligt, at virksomheden og politiet har en dialog, når sårbarhedsvurderingen er klar til godkendelse, så vurderingen følges op af mundtlige forklaringer. Virksomheden indsender eller indleverer herefter den færdiggjorte sårbarhedsvurdering til politiet til godkendelse.

Politiet kan i forbindelse med godkendelsen af sårbarhedsvurderingen eventuelt identificere nye sårbarheder, trusler osv., som virksomheden skal forholde sig til, før sårbarhedsvurderingen kan godkendes. Politiet vil i så fald oplyse om årsagen hertil, og der fastsættes en frist for indsendelse af en tilrettet version. Det kan i så fald være nødvendigt at gentage nogle af faserne i sikkerhedshjulet.

Sårbarhedsvurderingen godkendes i hovedtræk, når:

- Den indeholder de oplysninger, der er påkrævet, jf. risikobekendtgørelsens bilag 6, del 1
- Den på fyldestgørende og korrekt vis klarlægger virksomhedens sikringsniveau i forhold til forsætlige skadevoldende handlinger, herunder identificerer og vurderer relevante sårbarheder og trusler, og opstiller eventuelle anbefalinger til forbedring af sikringsniveauet

På baggrund af sårbarhedsvurderingen foretager politiet en konkret vurdering af, om virksomhedens sikringsniveau kan anses for acceptabelt set i forhold til truslerne.

Til grund for vurderingen ligger en nøje gennemgang af bl.a. virksomhedens sårbarheder sammenholdt med parametre så som karakteren af virksomheden og de farlige stoffer, beliggenhed, påvirkninger fra det omkringliggende samfund (nærhed til boliger og andre virksomheder) og den generelle og/eller sektorspecifikke terrortrussel m.v.

For at opnå et acceptabelt sikringsniveau skal virksomheden i tilstrækkeligt omfang have sikret, at en simpel, uhindret og uopdaget forsætlig skadevoldende handling ikke kan indtræffe, og at sandsynligheden for andre - mere komplekse - former for forsætlige skadevoldende handlinger minimeres og/eller besværliggøres. En simpel, forsætlig skadevoldende handling kan eksempelvis være en gerningsmand, der med en personbil uhindret kan påkøre et lager med farlige stoffer og derved forårsage brand, eksplosion, udslip m.v. En kompleks, forsætlig skadevoldende handling kræver mere planlægning, flere ressourcer, viden om virksomheden o.lign, og kan eksempelvis være et organiseret angreb, hvor flere gerningsmænd forsøger at trænge ind forskellige steder på virksomheden samtidig.

Virksomheden skal have tilstrækkelige sikringsforanstaltninger til dels at forhindre forsætlige skadevoldende handlinger i at indtræffe og til dels at håndtere og minimere konsekvenserne, såfremt en sådan handling alligevel indtræffer.

Politiet kan på baggrund af denne vurdering komme til den konklusion, at virksomheden allerede har etableret et acceptabelt sikringsniveau, hvorfor der ikke er behov for yderligere sikring. Virksomheden skal i givet fald ikke udarbejde en sikringsplan eller udpege en sikringsansvarlig, men skal dog påse at sårbarhedsvurderingen gennemgås og ajourføres efter reglerne herom.

Såfremt politiet konkret vurderer, at yderligere sikringsforanstaltninger er påkrævede for at opnå et acceptabelt sikringsniveau, beslutter politiet, at virksomheden skal udarbejde en sikringsplan og udpege en sikringsansvarlig.

Såfremt sårbarhedsvurderingen viser, at sikringsniveauet ikke er helt tilstrækkeligt, men kan blive det ved ganske få, mindre og umiddelbart implementerbare foranstaltninger eller ændringer, kan politiet godkende sårbarhedsvurderingen under forudsætning af, at virksomheden gennemfører sikringsforanstaltningerne øjeblikkeligt eller inden for en ganske kort frist.

5. UDARBEJSELSE AF SIKRINGSPLAN

Sikringsplanen beskriver de eksisterende og gennemførelsen af nye sikringsforanstaltninger med henblik på at opnå et acceptabelt sikringsniveau på virksomheden.

I dette kapitel beskrives, hvordan sikringsplanen udarbejdes, herunder hvilke oplysninger den skal indeholde.

Sikringsplanen skal mindst indeholde de oplysninger, der fremgår af risikobekendtgørelsens bilag 6, del 2. Virksomheden kan eventuelt anvende det vedlagte Bilag 4 Skabelon til sikringsplan, hvor de overordnede indholdskrav er oplistet.

Ligesom med sårbarhedsvurderingen er der tale om mindstekrav i bekendtgørelsen, hvorfor listen over oplysninger ikke skal forstås som udtømmende. Virksomheden bør således også overveje, om der er andre oplysninger, som vil være relevante at medtage i sikringsplanen.

5.1. INDLEDNING

Sikringsplanen indledes med en kort beskrivelse af baggrunden og formålet med planen samt eventuelle definitioner.

Der kan i indledningen ligeledes henvises til, at sikringsplanen er udarbejdet efter risikobekendtgørelsens § 11 og bilag 6, del 2, under anvendelse af nærværende vejledning og eventuelt andet vejledningsmateriale.

Beskrivelsen af formålet kan inddrage det overordnede formål med risikobekendtgørelsens § 11, nemlig at forebygge forsætlige skadevoldende handlinger, ligesom sikringsplanen har til formål at beskrive de eksisterende og gennemførelsen af nye sikringsforanstaltninger med henblik på at opnå et acceptabelt sikringsniveau på virksomheden.

Endvidere skal indledningen indeholde oplysninger om navn, stilling og telefonnummer på den/de personer, som har udarbejdet dokumentet med henblik på, at politiet og eventuelt andre myndigheder kan kontakte pågældende.

Såfremt eksterne rådgivere, politiet eller andre har vejledt eller på anden måde været involveret i udarbejdelsen af sårbarhedsvurderingen, bør dette tillige fremgå.

5.2. IDENTIFIKATION AF VIRKSOMHEDEN

Dette afsnit kan gengives fra sårbarhedsvurderingen, og skal - ligesom i sårbarhedsvurderingen - indeholde oplysninger om virksomhedens navn, adresse, telefonnummer og CVR-nummer samt eventuelle P-numre til brug for identificering af de enkelte produktionsenheder, hvis virksomheden har flere, og ellers en entydig identifikation af den produktionsenhed/lokalitet, som sikringsplanen gælder for.

5.3. SIKRINGSORGANISATION

I afsnittet anføres, hvem virksomheden har udpeget som overordnet sikringsansvarlig, herunder dennes navn, stillingsbetegnelse, ansvar og opgaver. Hvis der er flere sikringsansvarlige for den samme virksomhed, skal oplysningerne anføres for dem alle.

Da den sikringsansvarlige er kontaktperson i spørgsmål omkring virksomhedens sikring, anføres den sikringsansvarliges almindelige kontaktoplysninger (telefonnummer, e-mailadresse m.v.) og døgn-kontaktoplysninger (vagtnummer), hvor den vagthavende sikringsansvarlige kan kontaktes 24/7. Det er vigtigt at være opmærksom på at holde kontaktoplysningerne opdateret, og politiet skal straks have meddelelse ved ændringer i kontaktoplysningerne.

Den sikringsansvarlige skal meddele samtykke til, at politiet indhenter personoplysninger om denne i CPR- og Kriminalregisteret samt i politiets øvrige registre. På baggrund af samtykkeerklæringen foretager politiet et individuelt check for at sikre, at den pågældende ikke er opdateret i politiets registre på baggrund af aktiviteter, der er åbenbart uforenelige med den opgave, han/hun skal varetage som sikringsansvarlig for virksomheden (vandelsvurdering).

Risikobekendtgørelsen stiller alene krav om vandelsvurdering af den sikringsansvarlige og ikke om f.eks. sikkerhedsgodkendelse fra Politiets Efterretningstjeneste. Det er i herudover op til virksomheden at vurdere, hvilke krav der eventuelt skal stilles i forhold til øvrigt personale, herunder om fremvisning af straffeattest osv. Se eventuelt Politiets Efterretningstjenestes brochure ”Tænk sikkerhed når du ansætter”, som kan findes på www.pet.dk.

Afsnittet skal endvidere indeholde oplysninger om eget og/eller eksternt personale med sikringsopgaver sammen med en beskrivelse af personalets ansvar og opgaver. I princippet kan alt personale i virksomheden i større eller mindre omfang have sikringsmæssigt ansvar og opgaver og dermed bidrage til sikringen af virksomheden. Eksternt personale med sikringsopgaver kan eksempelvis være vagter fra en autoriseret vagtvirksomhed, som varetager adgangskontrollen på virksomheden.

Selvom det ikke er alt personale/personalegrupper, der måtte være direkte involveret i sikringsarbejdet, anbefales det, at det øvrige personale har et generelt kendskab til sikringsforhold på virksomheden, og hvad dette indebærer, hvilket bidrager til en god og effektiv sikring.

Det bemærkes, at beskrivelsen af eget/eksternt personale med sikringsopgaver ikke skal indeholde personoplysninger om de enkelte ansatte, men der kan eventuelt inddeles i funktioner, faggrupper osv., alt efter, hvad der findes mest hensigtsmæssigt. Antallet af personer inden for de enkelte funktioner m.v. skal anføres.

Det er også vigtigt at inddrage virksomhedens ledelse i sikringsarbejdet. Ledelsen behøver ikke have sikringsopgaver som sådan, men sikringen af virksomheden bør være forankret i ledelsen med henblik på tildeling af midler til formålet, overordnede politikker osv.

Sikringsorganisationen kan med fordel illustreres i et organisationsdiagram med supplerende beskrivelse.

5.4. UDDANNELSE, TRÆNING OG ØVELSER

I dette afsnit beskrives, hvilken uddannelse og/eller træning af den overordnede sikringsansvarlige og andet personale med sikringsopgaver, der er gennemført eller påtænkes gennemført. Der er ikke i risikobekendtgørelsen fastsat bestemte krav hertil, men det er afgørende, at uddannelsen og træningen kan tilføre det pågældende personale tilstrækkelige kompetencer i forhold til deres sikringsopgaver.

I afsnittet beskrives endvidere virksomhedens plan for afholdelse af øvelser, se nærmere i kapitel 2.1. KOLONNE 3-VIRKSOMHEDEN, og der vedlægges dokumentation og evalueringer fra allerede gennemførte øvelser (hvem har deltaget, hvad er blevet øvet, forløb, evaluering, konsekvens af øvelsen m.v.).

5.5. SIKRINGSFORANSTALTNINGER

Med udgangspunkt i sårbarhedsvurderingen beskrives i dette afsnit de eksisterende sikringsforanstaltninger på virksomheden, herunder allerede etableret sikringsudstyr- og indretninger som f.eks. indhegning, kameraovervågning, adgangskontrol, alarmer, kommunikationsudstyr m.v.

Endvidere beskrives de nye sikringsforanstaltninger eller ændringer af eksisterende sikringsforanstaltninger, som virksomheden har gennemført eller påtænker gennemført med henblik på at opnå et acceptabelt sikringsniveau. Der henvises her til konklusionen og anbefalingerne i den godkendte sårbarhedsvurdering.

Beskrivelsen skal også indeholde en plan for etableringen af nye eller ændringer af de eksisterende sikringsforanstaltninger, som endnu ikke er gennemført. Som anført i afsnit 2.1. KOLONNE 3-VIRKSOMHEDEN, skal sikringsforanstaltningerne være gennemført senest 6 måneder efter datoen for godkendelsen af sikringsplanen. Såfremt virksomheden af særlige årsager ikke har mulighed for at gennemføre (nogle af) sikringsforanstaltningerne inden for denne frist, skal det fremgå sammen med en begrundelse herfor. En forlængelse kan eksempelvis skyldes længere leveringstid på udstyr, at der er tale om et omfattende arbejde osv. Politiet kan på denne baggrund fastsætte en længere frist i forbindelse med godkendelsen af sikringsplanen.

Beskrivelserne suppleres af kortmateriale over virksomhedens beliggenhed og indretning, som også fremgår af sårbarhedsvurderingen, hvor de eksisterende og nye/ændrede sikringsforanstaltninger så vidt muligt skal fremgå. Det kan eksempelvis være indtegning af faste indretninger så som eksisterende indhegning, nye kameraers placering osv.

5.6. PROCEDURER FOR NORMALT BEREDSKABSNIVEAU

Som anført i afsnit 4.5. EKSISTERENDE SIKRINGSFORHOLD, har det indvirkning på virksomhedens sikringsniveau, at sikringsforanstaltningerne har kapacitet til at imødegå en forhøjet trussel. Sikringsplanen skal derfor indeholde procedurer for henholdsvis et normalt og et forhøjet beredskabsniveau.

I dette afsnit beskrives virksomhedens normale beredskabsniveau, som er de procedurer for håndtering af sikringstrusler og brud på sikringen, som skal opretholdes til enhver tid. Normalt beredskabsniveau er således "normalsituationen", hvor trusler og brud på sikringen kan håndteres med de sikringsforanstaltninger, som udgør den daglige og normale sikring.

Sikringsforanstaltninger, der skal opretholdes til enhver tid, kan eksempelvis være:

- Adgangskontrol
- Fast hegn
- Procedurer for vareleverancer
- Procedurer for pakke- og posthåndtering
- Procedurer for gæstehåndtering
- Sikkerhedskultur (sikkerhedsinstruks)

5.7. PROCEDURER FOR FORHØJET BEREDSKABSNIVEAU

I dette afsnit beskrives procedurerne for håndtering af trusler og brud på sikringen, hvor der er en sandsynlig eller overhængende fare for forsætlige skadevoldende handlinger mod virksomheden.

De kan indebære yderligere sikringsforanstaltninger i form af eksempelvis:

- Yderligere (forstærket) adgangskontrol til hele eller dele af virksomheden
- Yderligere overvågning
- Yderligere sikring af lagre
- Yderligere sikring af processer
- Skærpede procedurer for håndtering af farlige stoffer m.v.
- Rundering med vagter (eksterne eller interne) til hele eller dele af virksomheden

Politiet vil samtidig hermed kunne iværksætte egne foranstaltninger. I det omfang, det er nødvendigt, vil virksomheden blive orienteret om disse.

De yderligere sikringsforanstaltninger forventes kun at skulle opretholdes i en begrænset periode, indtil faren ikke længere er sandsynlig eller overhængende, hvorefter der nedjusteres til normalt beredskabsniveau.

Ændring i trusselsniveauet

Det vil som udgangspunkt være politiet, der foranlediger, at virksomheden iværksætter forhøjet beredskabsniveau på grund af en ændring i trusselsniveauet.

Ved en generel eller sektorspecifik ændring i trusselsniveauet, som giver anledning til at iværksætte forhøjet beredskabsniveau, underretter Politiets Efterretningstjeneste Rigspolitiet, som underretter politikredsen.

I tilfælde af en specifik trussel rettet direkte mod virksomheden vil Politiets Efterretningstjeneste kontakte politikredsen, som underretter virksomheden.

Politiets Efterretningstjeneste vurderer, hvilke oplysninger vedrørende trussel og trusselsniveau, som kan videregives.

Det er også Politiets Efterretningstjeneste, der - eventuelt via Rigspolitiet – meddeler politikredsen, hvornår det igen er relevant at nedjustere beredskabsniveauet. Politikredsen underretter virksomheden herom.

Meldevejene ved en ændring i trusselsniveauet kan illustreres således:

Sikringsrelateret hændelse
Virksomheden kan også af egen drift iværksætte forhøjet beredskabsniveau. Der tænkes særligt på de situationer, hvor virksomheden konstaterer en sikringsrelateret hændelse, herunder brud på sikringen, en mistænkelig handling, person eller omstændighed m.v., som kan udgøre en sandsynlig eller overhængende fare for forsætlige skadevoldende handlinger.

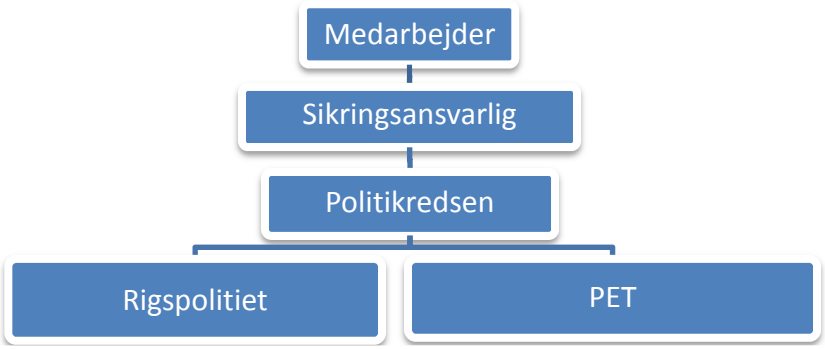
Hvis der konstateres en påbegyndt forsætlig skadevoldende handling mod virksomheden, kontaktes alarmcentralen straks via 112.

Ved en sikringsrelateret hændelse i øvrigt skal medarbejder(e), der konstaterer hændelsen, underrette den sikringsansvarlige, som straks underretter politiet. Det er vigtigt, at virksomheden over for politiet beskriver omstændighederne så detaljeret som muligt, herunder personer/signalementer, køretøjer, vidner m.v. Eventuel videoovervågning sikres hurtigst muligt.

Politiet vurderer på baggrund af oplysningerne hændelsen og underretter Rigspolitiet og Politiets Efterretningstjeneste, hvis det findes relevant. Den sikringsansvarlige og eventuelt

virksomhedens ledelse anbefales i samråd med politiet at vurdere, om ekstra sikringsforanstaltninger skal iværksættes øjeblikkeligt.

Meldevejene ved en sikringsrelateret hændelse kan illustreres således:



5.8. GENNEMGANG OG AJOURFØRING

Endeligt beskrives den procedure, som virksomheden vil anlægge i forhold til den periodiske gennemgang og ajourføring af sikringsplanen og evaluering af planens funktion (afholdelse af øvelser), som er omtalt i afsnit 2.1.3. Gennemgang og ajourføring og 2.1.4. Øvelser.

5.9. POLITIETS GODKENDELSE

Som anført vedrørende godkendelse af sårbarhedsvurderingen kan det efter omstændighederne være formålstjenligt, at virksomheden og politiet har en dialog, når også sikringsplanen er klar til godkendelse, så beskrivelserne følges op af mundtlige forklaringer. Virksomheden indsender eller indleverer herefter den færdiggjorte sikringsplan til politiet til godkendelse.

Sikringsplanen godkendes i hovedtræk, når:

- Den indeholder de oplysninger, der er påkrævet, jf. bilag 6, del 2
- De eksisterende og nye sikringsforanstaltninger medfører, at virksomheden opnår et acceptabelt sikringsniveau

Politiet foretager således en konkret vurdering af, om virksomhedens sikringsniveau på baggrund af sikringsplanen kan anses for acceptabelt set i forhold til truslerne. Se hertil uddybningen vedrørende det acceptable sikringsniveau i afsnit 4.9. POLITIETS GODKENDELSE.

Politiet vil oplyse om årsagen, såfremt sikringsplanen ikke kan godkendes i den foreliggende form, og der fastsættes en frist for indsendelse af en tilrettet version.

6. OFFENTLIGHED OG AKTINDSIGT

Som før anført kan sårbarhedsvurderingen og sikringsplanen (samt eventuelt øvelsesevalueringer m.v.) i sagens natur indeholde følsomme oplysninger, som ikke er egnede til udbredelse til uvedkommende. Det kan efter omstændighederne være konkrete og detaljerede oplysninger om de farlige stoffer, om virksomhedens sikring og sårbarheder over for forsætlige skadevoldende handlinger og andre sikringsrelaterede oplysninger m.v.

Der er imidlertid ikke i risikobekendtgørelsen fastsat regler om, hvordan dokumenterne og oplysningerne heri skal håndteres og beskyttes mod f.eks. uautoriseret adgang og udbredelse. Rigspolitiet skal dog anbefale, at der udvises særlig opmærksomhed på dette i forbindelse med sikringsarbejdet. Det kan eventuelt være nødvendigt med procedurer for, hvem der har adgang til dokumenterne/oplysningerne og hvordan de opbevares, sendes/leveres, destrueres osv.

Når dokumenterne/oplysningerne er indgået til politiet, bør politiet tillige være opmærksom på, hvordan dokumenterne håndteres, og hvem de udleveres til, jf. også afsnit 2.2.2. Inddragelse af andre myndigheder, og om eventuelt behov for klassificering efter Cirkulære nr. 10338 af 17/12/2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (Sikkerhedscirkulæret).

Regler om aktindsigt i bl.a. offentlighedsloven, forvaltningsloven og lov om aktindsigt i miljøoplysninger gælder alene inden for den offentlige forvaltning. Private virksomheder er således ikke bundet af regler om aktindsigt og kan derfor beslutte, at virksomhedens dokumenter, herunder sårbarhedsvurderingen og sikringsplanen m.v., ikke må deles med uvedkommende uden virksomhedens tilladelse. Men når dokumenterne og oplysninger i øvrigt er udvekslet med politiet (eller anden offentlig forvaltningsmyndighed), bliver de omfattet af reglerne om aktindsigt.

Politiet kan således blive mødt med en anmodning om aktindsigt i eksempelvis den indsendte sårbarhedsvurdering eller sikringsplan, som i så fald skal behandles efter reglerne herom.

Dette er dog ikke ensbetydende med, at der skal gives aktindsigt i (hele) dokumentet. Retten til aktindsigt kan under visse betingelser begrænses blandt andet i forhold til tekniske indretninger, fremgangsmåder eller drifts- og forretningsforhold, til beskyttelse af statens sikkerhed eller rigets forsvar, forebyggelse, efterforskning og forfølgning af lovovertrædelser osv.

Det beror på en konkret vurdering, om hele dokumenter eller oplysninger i dokumenterne kan undtages fra aktindsigt, og denne vurdering foretages af politiet. Politiet indhenter til brug herfor en udtalelse fra virksomheden.

Får en anden myndighed dokumenterne eller uddrag heraf i besiddelse i forbindelse med høringen/orienteringen, jf. afsnit 2.2.2. Inddragelse af andre myndigheder, bør denne gøres opmærksom på, at i tilfælde af, at der begæres aktindsigt i dokumenterne hos den

pågældende myndighed, skal politiet og virksomheden have lejlighed til at udtale sig forinden med henblik på at sikre, at ovennævnte hensyn inddrages i vurderingen.

Det bemærkes, at Politiets Efterretningstjeneste generelt anbefaler i forhold til risikovirksomheder, at myndighederne, på baggrund af en konkret vurdering, tilbageholder deltaljerede oplysninger om følgende, da disse oplysninger vurderes at kunne være til fare for rigets sikkerhed:

- Virksomhedens produktions- og sikkerhedsforhold
- Virksomhedens eller anlæggets opbygning
- Risici, der er forbundet med en virksomhed eller et anlægs drift
- Mængden af farlige stoffer, der opbevares af en virksomhed, og placering af de farlige stoffer, herunder placering af overjordiske oplag

Der henvises endvidere til Folketingets Ombudsmands redegørelse af 5. juli 2010 vedrørende aktindsigt i oplysninger om risikovirksomheder.

Det bemærkes i øvrigt, at miljømyndigheden og politiet skal offentliggøre visse oplysninger om virksomheden efter risikobekendtgørelsens § 16. Der kan således være oplysninger, som er gengivet i sårbarhedsvurderingen eller sikringsplanen m.v., som allerede er offentliggjort på f.eks. www.dma.mst.dk (Digital MiljøAdministration) eller på politiets hjemmeside.

7. HENVISNINGER

Miljøstyrelsen har udsendt Risikohåndbogen, som beskriver de fleste forhold omkring risikovirksomheder. Håndbogen findes på www.risikohaandbogen.mst.dk.

Endvidere henvises til de i afsnittene omtalte vejledninger på www.brs.dk og www.pet.dk.

8. BILAG

Bilag 1 Skabelon til sårbarhedsvurdering
Bilag 2 Sandsynlighedsindeks og konsekvensindeks
Bilag 3 Risikovurderingsskema
Bilag 4 Skabelon til sikringsplan

Bilag 1 Skabelon til sårbarhedsvurdering

Afsnit	Indhold i afsnit	Bilag mv.
1. Indledning	*Kort beskrivelse af baggrund og formål.* *Eventuelle definitioner.* *Oplysninger om deltagende personer, eksterne rådgivere, politiet eller andre.*	
2. Generel beskrivelse af virksomheden og de farlige stoffer.	*Navn, adresse, telefonnummer, CVR-nummer/P-nummer, identifikation af produktionsenhed/lokalitet.* *Alment forståelig beskrivelse af aktivitet eller påtænkt aktivitet, herunder oplag.* *De farlige stoffer, mængde, tilstand, almindelige betegnelse, farlige karakteristika.*	
3. Virksomhedens organisation	*Organisationen, ledelsessystem/sikkerhedsledelsessystem.* *Eventuel sikringsorganisation og/eller personale med sikringsmæssige opgaver.* *Personale med adgang til farlige stoffer.* *Evt. beskrivelse af sikringsrelateret uddannelse, træning og øvelser.*	*Evt. organisationsdiagram*
4. Fysisk beliggenhed og indretning	*Beskrivelse af virksomhedens fysiske forhold, herunder beliggenhed, indretning, vigtig ejendom, infrastruktur/adgangsveje, afgrænsning, arealer, omgivelser, naborisikovirksomheder.* *Relevante objekter med oplag eller håndtering af farlige stoffer.*	*Kortmateriale*
5. Eksisterende sikringsforhold	*Eksisterende sikringsforanstaltninger, herunder allerede etableret sikringsudstyr og indretninger.* *Sikringsforanstaltningernes styrker, svagheder, pålidelighed/holdbarhed.* *Evt. procedurer for normalt og forhøjet beredskabsniveau.*	*Kortmateriale*
6. Relevante sårbarheder og trusler	*Beskrivelse af relevante sårbarheder og trusler.* *Dette afsnit er i vejledningen sammenkoblet med den beskrevne metode til risikovurderingen.*	
7. Risikovurdering	*Oversigt over identificerede sårbarheder og trusler* *Risikovurdering af sårbarheder og trusler ved fastsættelse af sandsynlighed og konsekvens, eventuelt ved anvendelse af den beskrevne metode "sikringshjul" med fase 1-6.*	*Evt. Risikomatrix og "bowtie"- model.*
8. Konklusioner og anbefalinger	*Samlet konklusion om sikringsniveauet.* *Eventuelle anbefaling til forbedring af sikringen, herunder etablering af nye sikringsforanstaltninger og/eller forbedring af eksisterende.* *Evt. gennemgang af fase 3 og 4.*	*Kortmateriale*
9. Gennemgang og ajourføring	*Procedure for gennemgang og ajourføring af sårbarhedsvurderingen*	

Bilag 2 Sandsynlighedsindeks og konsekvensindeks

Sandsynlighedsindeks

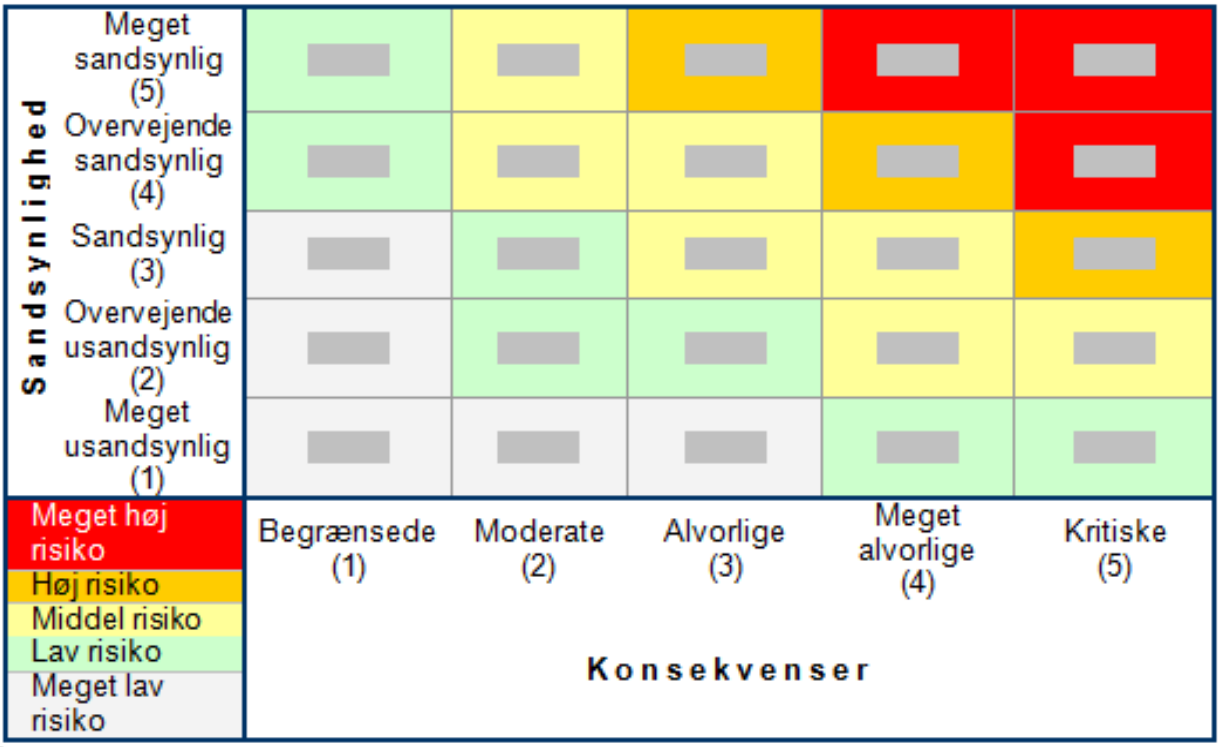
Meget sandsynligt (5)	En forsætlig skadevoldende handling kan gennemføres under de eksisterende sikringsforanstaltninger uden særlig forberedelse eller ressourcer.
Overvejende sandsynligt (4)	En forsætlig skadevoldende handling kan gennemføres, men vil kræve mindre forberedelse og ressourcer under de eksisterende sikringsforanstaltninger.
Sandsynligt (3)	En forsætlig skadevoldende handling kan gennemføres, men vil kræve betydelige ressourcer og forberedelse under de eksisterende sikringsforanstaltninger.
Overvejende usandsynligt (2)	En forsætlig skadevoldende handling kan gennemføres, men vil kræve betydelige ressourcer, omfangsrig forberedelse og viden om virksomheden under de eksisterende sikringsforanstaltninger.
Meget usandsynligt. (1)	En forsætlig skadevoldende handling kan gennemføres, men vil kræve betydelige ressourcer, omfangsrig forberedelse og detaljeret "insider" viden om virksomheden og dennes sikringsforanstaltninger under de eksisterende sikringsforanstaltninger.

Konsekvensindeks

Kritiske (5)	Flere tab af menneskeliv og alvorlig personskade. Større tab af aktiver. Langvarig afbrydelse af samfundets kritiske funktioner. Stor og langvarig utryghed hos befolkningen.
Meget alvorlige (4)	Enkelte tab af menneskeliv og/eller alvorlig personskade. Omfattende tab af aktiver og/eller kortvarig afbrydelse af samfundets kritiske funktioner. Stor utryghed hos befolkningen.
Alvorlige(3)	Ingen tab af menneskeliv men alvorlig personskade. Omfattende tab af aktiver og mindre afbrydelse af samfundets kritiske funktioner. Stor utryghed hos befolkningen.
Moderate (2)	Ingen tab af menneskeliv eller alvorlig personskade. Moderat tab af aktiver og afbrydelse af samfundets kritiske funktioner. Moderat utryghed hos befolkningen.
Begrænsede (1)	Ingen tab af menneskeliv eller alvorlig personskade. Begrænset tab af aktiver og afbrydelse af samfundets kritiske funktioner. Begrænset utryghed hos befolkningen.

Bilag 3 Risikovurderingsskema

Sårbarhedsbeskrivelse:	Trusler og fare:	Konsekvenser:
		.



Risikofaktor:	Forventet udvikling

Eksisterende sikringsforanstaltninger:	
Forbyggende	Reaktive
Sikringsniveau 1.	Sikringsniveau 1.
Sikringsniveau 2.	Sikringsniveau 2.

Yderlige sikringstiltag	
Forbyggende	Reaktive
Sikringsniveau 1.	Sikringsniveau 1.
Sikringsniveau 2.	Sikringsniveau 2.
Ansvarlig for implementering:	Ansvarlig for implementering:

Dato for vurdering	Udført af

Bilag 4 Skabelon til sikringsplan

Afsnit	Indhold i afsnit	Bilag mv.
1. Indledning	*Kort beskrivelse af baggrund og formål.* *Eventuelle definitioner.* *Oplysninger om deltagende personer, eksterne rådgivere, politiet eller andre.*	
2. Identifikation af virksomheden	*Navn, adresse, telefonnummer, CVR-nummer/P-nummer, identifikation af produktionsenhed/lokalitet.*	
3. Sikringsorganisation	*Oplysninger om overordnet sikringsansvarlig og kontaktoplysninger.* *Eget og eksternt personale med sikringsopgaver.*	Evt. organisationsdiagram Samtykkeerklæring
4. Uddannelse, træning og øvelser	*Uddannelse og/eller træning af sikringsansvarlig og personale med sikringsopgaver* *Plan for afholdelse af øvelser* *Dokumentation og evalueringer fra gennemførte øvelser*	Evt. uddannelsesplaner, øvelsesevalueringer m.v.
5. Sikringsforanstaltninger	*Eksisterende sikringsforanstaltninger, herunder allerede etableret sikringsudstyr og indretninger.* *Nye sikringsforanstaltninger eller ændring af eksisterende sikringsforanstaltninger* *Planer for etablering/ændring af sikringsforanstaltninger, evt. begrundelse for forlængelse af fristen for gennemførelsen.*	*Kortmateriale*
6. Procedure for normalt beredskabsniveau	*Procedurer for håndtering sikringstrusler og brud på sikringen, som skal opretholdes til enhver tid.*	
7. Procedure for forhøjet beredskabsniveau	*Procedurer for håndtering af sikringstrusler og brud på sikringen ved sandsynlig eller overhængende fare for forsætlige skadevoldende handlinger.*	
8. Gennemgang og ajourføring	*Procedure for gennemgang og ajourføring af sikringsplanen.* *Procedure for evaluering af planens funktion (øvelser).*	