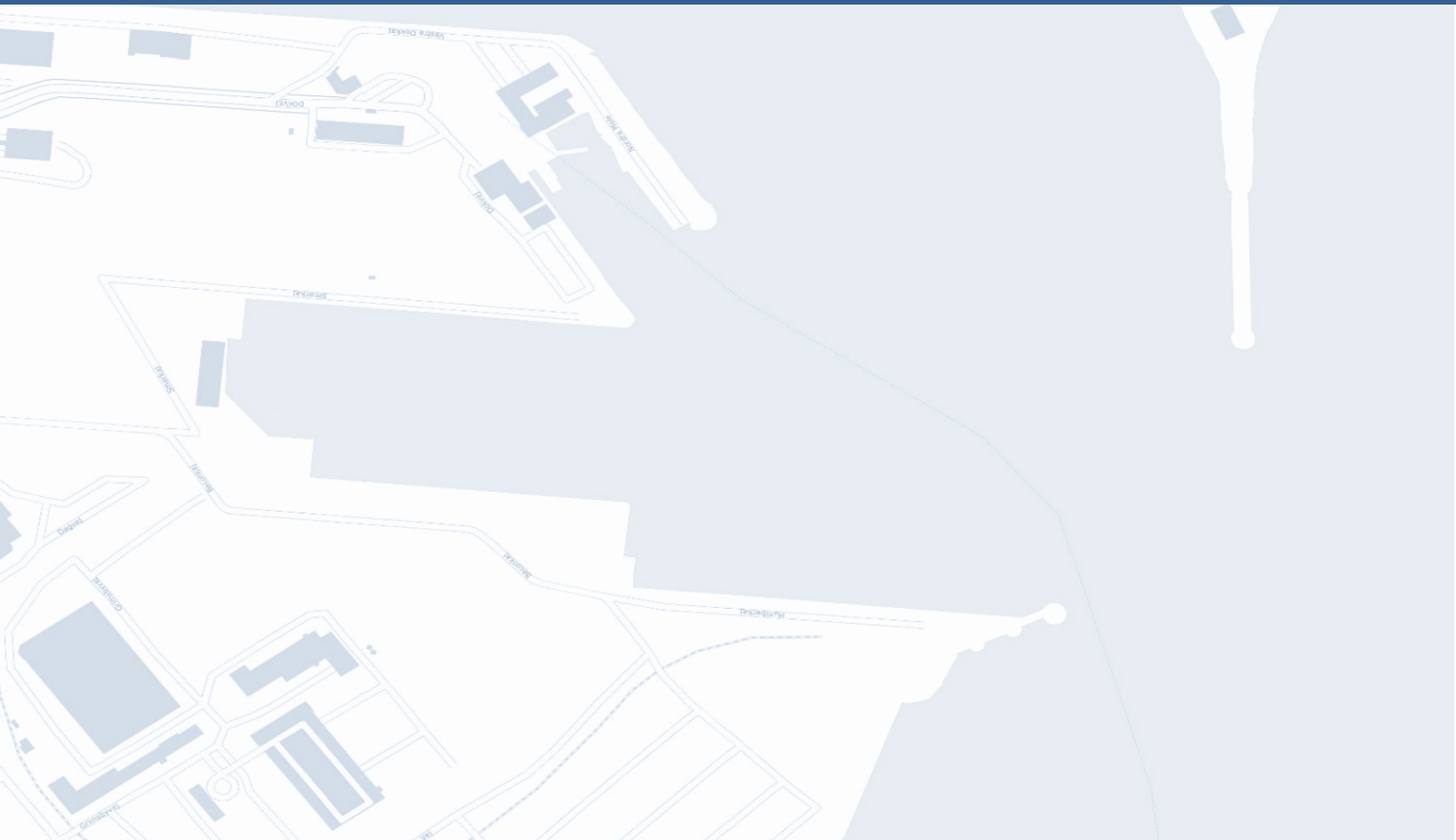
Trafikstyrelsen
Danish Civil Aviation and Railway Authority

Vejledning til udfyldelse af skabelon til havnefacilitetssårbarhedsvurdering

PFSA

Skridt-for-skridt guide

Version 4.0 (2025)



Trafikstyrelsen
Danish Civil Aviation and Railway Authority

Skridt-for-skridt guide - Udfyldelse af skabelonen (PFSA)

En sårbarhedsvurdering af en havnefacilitet skal udarbejdes ved brug af Trafikstyrelsens skabelon, som kan findes på styrelsens hjemmeside.

Selve skabelonen for sårbarhedsvurdering - herunder overskrifter, emnefelter og kategorier - må ikke ændres i forbindelse med udfyldelsen. Der er dog den undtagelse, at der er metodefrihed i forhold til, hvilken risikovurderingsmodel man anvender, se mere i vejledningens afsnit 7.

I denne vejledning gennemgås skabelonens enkelte dele, herunder vejledning til hvordan den udfyldes skridt-for-skridt, og hvad afsnittene forventes at indeholde.

Indholdsfortegnelse

Forord

Det overordnende formål med maritim sikring er at beskytte den internationale skibstrafik samt tilhørende havne og havnefaciliteter

De danske regler om maritim sikring er baseret på internationale aftaler og har sit udspring i FN's internationale maritime organisation (IMO).

Blandt andet på baggrund af terrorangrebene i USA i september 2001 færdiggjorde IMO arbejdet med ISPS-koden, som handler om iværksættelse af en række tiltag af hensyn til beskyttelse af den internationale skibstrafik mod forsætlige ulovlige handlinger.

EU gjorde i 2004 store dele af ISPS-koden obligatorisk ved indførelse af en forordning om bedre sikring af skibe og havnefaciliteter. I forordningen fremgår det desuden, at det til enhver tid er vigtigt at sikre søtransportsektoren og de borgere, der benytter denne transportform, samt miljøet mod forsætlige ulovlige handlinger.

Reglerne har derfor som sit primære overordnet formål at beskytte den internationale skibstrafik, og der er som sådan ikke tale om sikring af hensyn til beskyttelse af den enkelte havnefacilitet. Da havnefaciliteter i udgangspunktet ikke er ens, kan der ikke opstilles en facitliste for, hvilke sikringstiltag, der konkret er tilstrækkelige til at imødegå formålet om sikring af skibstrafikken i de enkelte havnefaciliteter.

EU supplerede i 2005 forordningen ved indførelse af et direktiv om bedre sikring af havne. Hovedformålet med direktivet er at forbedre sikringen af havne mod truslen for sikringsrelaterede hændelser. Direktivet skal sikre, at de foranstaltninger som allerede er iværksat på baggrund af ISPS-kodens regler, understøttes af bedre havnesikring.

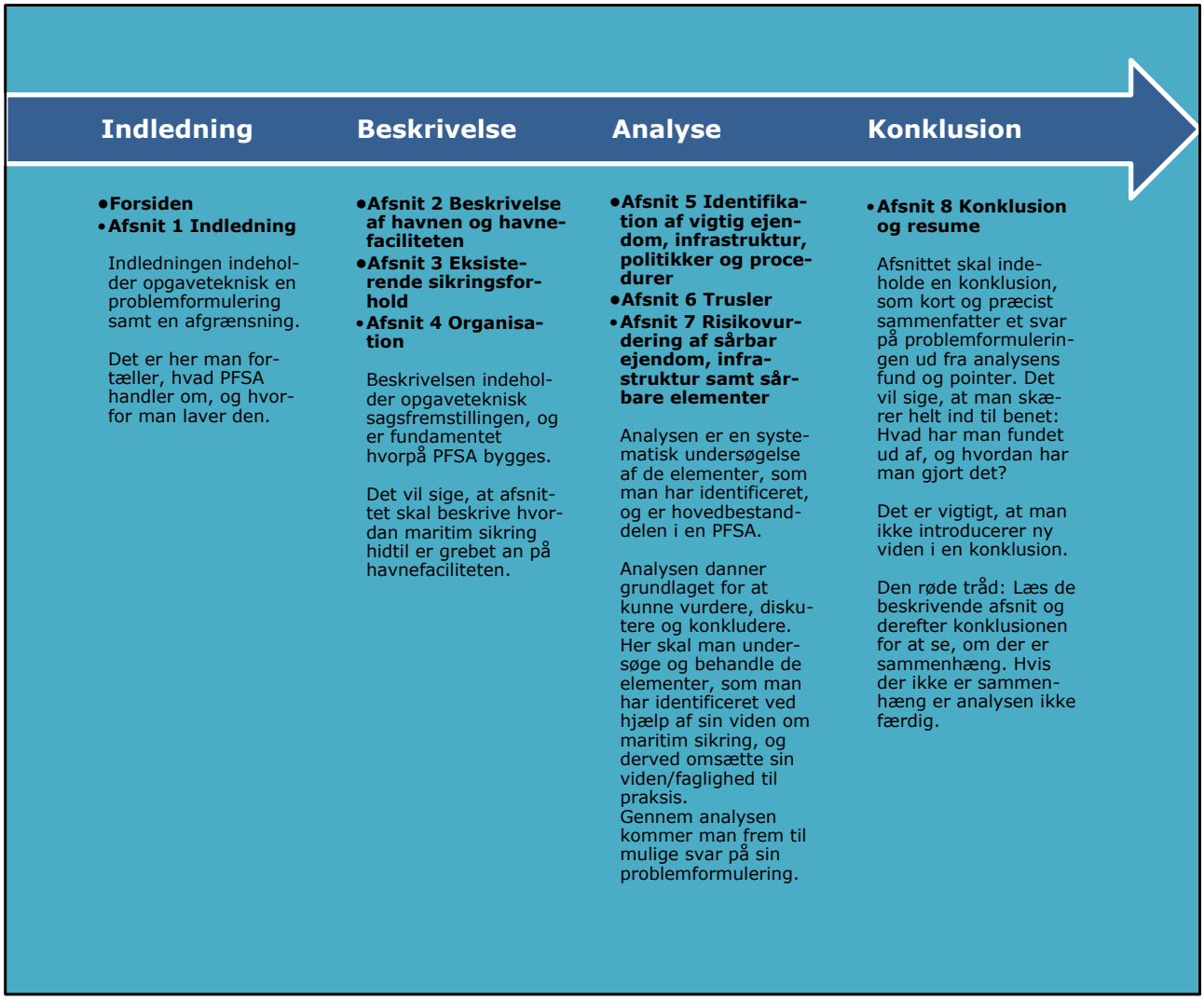
Erfaringer har vist, at der kan være en række positive sidegevinster ved maritim sikring. Det kan f.eks. betyde færre ulykker, da der kun færdes personale på faciliteten, der har kendskab til havneaktiviteter. Sikringen kan også medvirke til mindre tyveri og hærværk, ligesom det er oplevelsen, at flere af havnenes kunder, særligt skibene, efterspørger sikringstiltag i havnene, men hovedformålet med reglerne er at sikre den internationale skibstrafik.

Kunsten at skrive en sårbarhedsvurdering

Dette afsnit indeholder en beskrivelse af, hvordan skabelonen for sårbarhedsvurdering er opbygget. Skabelonen er baseret på en klassisk struktur, der tager højde for grundlæggende elementer indenfor analyserapportskrivning. En veldefineret struktur er afgørende for både forståelsen og kvaliteten af en sårbarhedsvurdering.

I skabelonen findes otte afsnit, som indbyrdes er afhængige af hinanden. Det er derfor vigtigt at bevare en rød tråd gennem hele dokumentet. Den skal guide læseren fra indledning til konklusion og sikre sammenhæng og kontinuitet mellem de forskellige afsnit. For at opnå dette kan man f.eks. fastholde et klart fokus gennem hele sårbarhedsvurderingen og etablere en forbindelse mellem de beskrivende afsnit i indledningen, analysen og konklusionen. Derudover er det vigtigt at opretholde en sproglig rød tråd ved at anvende de samme begreber gennem hele dokumentet. Når dokumentet er struktureret, bliver det nemmere for læseren at følge med og forstå indholdet. Skabelonen er derfor også lavet med det formål at guide forfatteren til nemmere at få struktur og en rød tråd i sårbarhedsvurderingen.

Nedenstående figur gennemgår strukturen og grundelementerne i skabelonen.



Forkortelser og definitioner

Følgende forkortelser og definitioner er brugt i vejledningen:

Forkortelse	Beskrivelse
Maritim sikring	Formålet med maritim sikring er at beskytte den internationale skibstrafik samt tilhørende havne og havnefaciliteter mod forsætlige ulovlige handlinger.
Havn	Ethvert specifikt land- og søområde, som de pågældende medlemsstater har afgrænset, bestående af anlæg og udstyr, som tjener til at lette kommerciel søtransport.
Havnefacilitet	Et område, hvor der er en grænseflade mellem skib og havn. Dette område omfatter f.eks. ankerpladser, ventepladser og ankomstfaciliteter fra søsiden, når det er relevant.
ON/OFF-facilitet	En godkendelse af, at havnefaciliteten kun behøver at iværksætte sikringstiltagene i sikringsplanen, når der er skibe, som skal anløbe kajen, eller hvor gods ligger til udskibning (dvs. faciliteten er ON). På alle andre tidspunkter kan faciliteten have offentlig adgang uden synlige fysiske sikringstiltag iværksat (dvs. faciliteten er OFF).
ESA	En godkendelse af, at der i stedet for en sikringsplan for havnefaciliteten udarbejdes og gennemføres et ækvivalent sikringsarrangement (Equivalent Security Arrangements) jf. § 8 i gældende bekendtgørelse om sikring af havnefaciliteter.
§ 9-dispensation	En dispensation fra kravet om udarbejdelse af en sikringsplan for havnefaciliteten jf. § 9 i gældende bekendtgørelse om sikring af havnefaciliteter.
Artikel 2.4 havn	Henvisningen til artikel 2.4 referer til direktivet om bedre havnesikring. Betegnelsen omfatter en havn bestående af én enkelt havnefacilitet, hvor havnens sikringsmæssige afgrænsning er sammenfaldende med havnefacilitetens afgrænsning.
Artikel 2.4 fritagelse	En dispensation fra kravet om udarbejdelse af en sikringsplan for en havn som har en enkelt havnefacilitet jf. gældende bekendtgørelse om sikring af havne.
Særligt adgangsbegrænset område	Herved forstås "områder med adgangsbegrænsning", jf. f.eks. ISPS-kodens del A, pkt. 1.3.3.
AIS	Automatic Identification System (AIS) er et maritimt radiosystem til automatisk identifikation af skibe og andre enheder i forbindelse med søfart.

Dato	Ved indsættelse af dato i skabelonen i enten fritekstfelter eller datofelter bruges formatet (dag–måned-år) f.eks. 1. juli 2024 eller DD-MM-ÅÅÅÅ.
Direktivet	EU-direktiv 205/65/EF om bedre havnesikring
DoS	Sikringserklæring (Declaration of Security) er en aftale indgået mellem et skib og enten en havnefacilitet eller et andet skib, som det har berøring med, hvori de sikringstiltag, som de hver især vil gennemføre, beskrives nærmere.
ENISA	EU's agentur for cybersikkerhed (European Union Agency for Cybersecurity)
Forordningen	EU-forordning 725/2004 om bedre sikring af skibe og havnefaciliteter
IMDG-koden	International Maritime Dangerous Goods Code
IMO	FN's internationale maritime organisation (International Maritime Organization)
IMO/GISIS	IMO's database "Global Integrated Shipping Information System"
IMSBC-koden	International Maritime Solid Bulk Cargoes Code
ISPS-koden	International Ship and Port Facility Security Code er regler som er vedtaget i IMO den 12. december 2002. ISPS-koden handler om iværksættelse af en række tiltag af hensyn til beskyttelse af den internationale skibstrafik.
LAN	Local area network
MARSEC	Maritime Security Committee (MARSEC) er et udvalg i EU, som bistår Kommissionen i spørgsmål om maritim sikring.
PFSA	Havnefacilitetssårbarhedsvurdering (Port Facility Security Assessment)
PFSO	Havnefacilitetens sikringsansvarlige (Port Facility Security Officer)
PFSP	Havnefacilitetssikringsplan (Port Facility Security Plan)
PSA	Havnesårbarhedsvurdering (Port Security Assessment)
PSP	Havnesikringsplan (Port Security Plan)
RSO	Anerkendt sikringsorganisation (Recognized Security Organization)
TS	Trafikstyrelsen
UN/LOCODE	United Nations Code for Trade and Transport Locations (DKXXX)

Forsiden

På skabelonens forside udfyldes en række grundlæggende oplysninger, som sætter rammen for sårbarhedsvurderingen.

I nedenstående skema beskrives de enkelte punkter på skabelonens forside.

	Beskrivelse
Havn	Havnens navn
Havnefacilitet	Navn på havnefaciliteten, som angivet i IMO/GISIS
IMO havnefacilitets nummer	IMO havnefacilitets nummer, som angivet i IMO/GISIS f.eks. DKTYB-0001
Ny havnefacilitet	Angiv hvorvidt der er tale om en ny havnefacilitet. Hvis der er tale om en ny havnefacilitet, vil TS oprette faciliteten i IMO/GISIS i forbindelse med godkendelse af sårbarhedsvurderingen.
Stedsangivelse	Havnens stedsangivelse i breddegrad og længdegrad. Positionen bør være i overensstemmelse med beliggenheden som angivet i den nautiske publikation Den Danske Havnelods. Formatet angives i grader og decimalminutter f.eks. 55°16,1' N; 009°53,1' Ø.
Postadresse på havnefacilitet	Postadressen på havnefaciliteten. Det vil sige enten på havnen eller den selvstændige terminaloperatør.
CVR-nummer	CVR-nummer på havnen. Det vil sige enten på havnen eller den selvstændige terminaloperatør.
Godkendelsesdato for eksisterende sårbarhedsvurdering	Godkendelsesdatoen for den eksisterende sårbarhedsvurdering for havnefaciliteten (PFSA) i formatet (dag-måned-år). Hvis der ikke foreligger en eksisterende sårbarhedsvurdering (f.eks. ved en ny havnefacilitet) efterlades feltet tomt.
Godkendelsesdato for eksisterende sikringsplan	Godkendelsesdatoen for den eksisterende sikringsplan for havnefaciliteten (PFSP) i formatet (dag-måned-år). Hvis der ikke foreligger en eksisterende sikringsplan (f.eks. ved en ny havnefacilitet) efterlades feltet tomt.
Ansøgning om godkendelse ved	Begrund hvorfor sårbarhedsvurderingen indsendes til TS, ved at vælge en af de 4 muligheder, som er: • *sårbarhedsvurdering* (ny facilitet) • *5 års fornyelse* En sårbarhedsvurdering udløber 5 år efter godkendelsesdatoen, medmindre den forinden af anden årsag er bortfaldet. • *større ændring* Ved en større ændring forstås en ændring, der har **betydning** for havnefacilitetens sårbarhed, herunder større ændringer i

	havnefacilitetens fysiske struktur, organisation, eller hvis havnefaciliteten skal anvendes til andre formål end de, der er angivet i den godkendte sårbarhedsvurdering. Eksempler på hvad en større ændring **kan** være: ➢ At havnefaciliteten overdrages til en selvstændig terminaloperatør ➢ At en selvstændig terminal får ny operatør ➢ At en facilitet, der er godkendt til at betjene stykgods, skal til at betjene krydstogtskibe ➢ At en facilitet, der er godkendt til at betjene tendere (mindre hjælpefartøjer) fra krydstogtskibe, skal til at betjene krydstogtskibe ➢ At havnefaciliteten ændrer adgangskontrol og overvågning fra tekniske løsninger til manuelle løsninger, at porte, låse og video erstattes af en vagt eller omvendt ➢ At faciliteten ønskes ændret fra status som standard ISPS-facilitet til ON/OFF-facilitet eller omvendt, ønsker en § 9-dispensation eller en ESA ➢ At faciliteten gennemgår en ombygning, eller ➢ Hvis faciliteten i forbindelse med ændring af omfang får grænseflade til et område, der kan udgøre en trussel mod faciliteten som f.eks.: - Et tankanlæg, oplæg af brandbare materialer mv. - Der etableres ejendom eller infrastruktur på faciliteten, på havnen eller hos en nabo til havnen, som kan udgøre en trussel mod faciliteten, som f.eks. kolonne 2 eller 3 virksomheder. • *andet* (det kan f.eks. være på baggrund af en inspektion af TS, hvor der er et krav om, at en sårbarhedsvurdering skal revurderes.)
Beskrivelse (større ændring eller andet)	Hvis "større ændring" eller "andet" er valgt under "Ansøgning om godkendelse ved" udfyldes dette felt. I feltet beskrives kort hvad den større ændring består i, eller hvad der ligger til grund for valget af "andet".
Facilitetens nuværende status	Her angives facilitetens nuværende status. Vælg en af nedenstående muligheder: • *Standard facilitet* • *ON/OFF-facilitet* • *Ækvivalent sikringsarrangement (ESA)* • *§ 9-dispensation* • *Ingen (dvs. ny facilitet)* Herved menes om faciliteten allerede har status af f.eks. standard facilitet, ON/OFF-facilitet, ESA, § 9-dispensation eller er en ny facilitet.

Facilitetens ønske til fremtidig godkendelse	Her angives facilitetens ønske til fremtidig godkendelse. Vælg en af nedenstående muligheder: • *Standard facilitet* • *ON/OFF-facilitet* • *Ækvivalent sikringsarrangement (ESA)* • *§ 9-dispensation* Herved menes om faciliteten ønsker en godkendelse som f.eks. standard facilitet, ON/OFF-facilitet, ESA eller en § 9-dispensation. Hvis der er specielle forhold som gør, at man ønsker at operere som ON/OFF-facilitet, ønsker en undtagelse for udarbejdelse af sikringsplan (§9-dispensation) eller ønsker status som havnefacilitet med ækvivalente sikringstiltag (ESA), skal dette begrundes tydeligt i skabelonens afsnit 8 om konklusion og resume. Det skal være begrundet i den samlede sårbarhedsvurdering. TS vil i forbindelse med sagsbehandlingen afgøre, om der vil være basis for lempeligere sikringsforhold.
Havnefacilitetens aktiviteter	Angiv hvilke typer aktiviteter som udføres på havnefaciliteten. Vælg en eller flere aktiviteter (vådbulk, skibsværft, containere, tørbulk, stykgods, passagerer eller andet). Hvis kategorien "*andet*" vælges skal det beskrives i tekstfeltet hvilken anden aktivitet, der er tale om. Det kan f.eks. være speciallaster.
Anerkendt sikringsorganisation (RSO)	Indsæt navn samt CVR-nummer på RSO, som har udarbejdet sårbarhedsvurderingen.
Dato for færdiggørelse af sårbarhedsvurdering	I datofeltet skrives den dato, hvor RSO har færdiggjort sårbarhedsvurderingen i formatet (dag-måned-år).
Versionsnummer	I feltet indsættes versionsnummer på sårbarhedsvurderingen f.eks. 1, 2, 3 osv.

1 Indledning

I dette afsnit beskrives, hvem der konkret har udarbejdet sårbarhedsvurderingen. Det skal ligeledes fremgå, at sårbarhedsvurderingen er udarbejdet i samarbejde med politiet.

1.2 Udarbejdelse

I skema 1.2 skrives navnene på de personer, som har deltaget i udarbejdelsen af sårbarhedsvurderingen, og i hvilken funktion, de har medvirket (f.eks. som PFSO, RSO, politiassistent mv.).

I de tilfælde, hvor godkendelsen som RSO består af flere navngivne personer, skal alle personer fra den pågældende RSO, som har medvirket ved udarbejdelse af sårbarhedsvurderingen, fremgå af listen.

I afsnittet anføres desuden hvilken politikreds og repræsentant fra politiet, som har medvirket i udarbejdelsen af sårbarhedsvurderingen. Bekræftelse på politiets medvirken fremsendes af politiets repræsentant til TS på mailadressen: maritimsikring@trafikstyrelsen.dk.

1.3 Forkortelser

I udgangspunktet bør indholdet af sårbarhedsvurderingen være selvforklarende. Anvendes der forkortelser i teksten, bør de være konkrete og relevante i forhold til sårbarhedsvurderingen.

I skema 1.3 skrives relevante forkortelser med tilhørende beskrivelse.

2 Beskrivelse af havnen og havnefaciliteten

Dette afsnit indeholder oversigtskort samt relevante beskrivelser af havnen og havnefaciliteten.

Der er ingen formkrav til kortmaterialet, men oversigtskortene skal være af en så god kvalitet, at de enkelte emner tydeligt kan identificeres.

Kortmaterialet skal underbygge teksten i sårbarhedsvurderingen. Det betyder f.eks., at hvis der benyttes vejnavne, kajnumre og virksomhedsnavne i beskrivelserne i sårbarhedsvurderingen, skal dette tydeligt fremgå af kortmaterialet, ligesom det skal indeholde en signaturforklaring.

Alle vedlagte kort indskrives i skema 2.1 og 2.2 med angivelse af bilagsnummer samt navn. Kortmateriale, som pga. format eller andet ikke kan sendes elektronisk, skal sendes som anbefalet brev til TS, jf. gældende bekendtgørelse om sikring af havnefaciliteter.

Relevante beskrivelser af havnen og havnefaciliteten indskrives i tekstfelterne efter skemaerne. Det kan f.eks. være havnekontorets funktion, da den maritime sikring ofte overvåges og styres herfra. Det kan også være bygninger eller installationer, som har en relation til formålet med maritim sikring, eller det kan være andre beskrivelser, som er med til at underbygge forståelsen af kortmaterialet.

Havne med kun en havnefacilitet (artikel 2.4 havn)

I en havn, hvor der kun er en havnefacilitet, er det som følge af direktivets artikel 2.4 muligt at opnå en fritagelse for at lave en havnesikringsplan (PSP), hvis havnens sikringsmæssige afgrænsning er sammenfaldende med havnefacilitetens afgrænsning (artikel 2.4 fritagelse).

Husk at havnefacilitetens afgrænsningen ikke må være for snæver

Det er vigtigt, at en havnefacilitets afgrænsning ikke bliver for snæver, men medtager alle relevante sammenbindende elementer, herunder særligt havnens vandområde og evt. navigationssystemer. Havnefaciliteten skal med andre ord være så stor, at den omfatter hele det område, der er indrettet til og letter kommerciel søtransport i relation til formålet med maritim sikring.

Vær også opmærksom på hvordan det sikres, at sikringsrelaterede oplysninger beskyttes mod uautoriseret adgang og udbredelse, da dette er en obligatorisk proceduremæssig fremgangsmåde i en havnesårbarhedsvurdering (PSA).

Der kan findes yderligere information om emnet i vores PSA-vejledning.

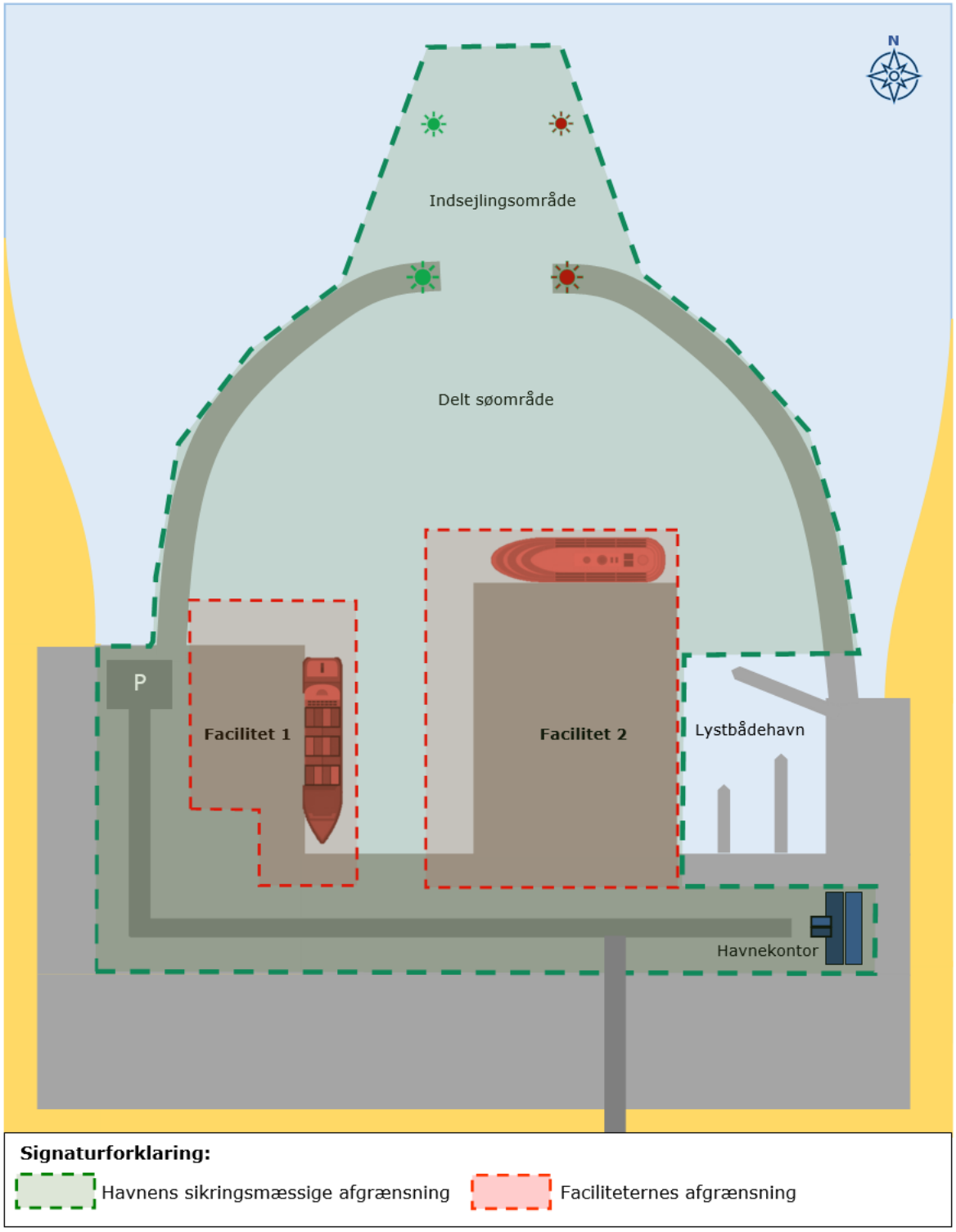
2.1 Oversigtskort over ejendom, infrastruktur og havnefacilitetens placering på havnen

Som bilag til ansøgningen vedlægges oversigtskort over havnen, der viser havnens placering i et større geografisk område, jf. nedenstående liste. Kortene skal indeholde en signaturforklaring samt tydeligt identificere og markere følgende:

- Havnens placering og sikringsmæssige afgrænsning.
- Faciliteternes placering og afgrænsning.
- Adgang fra land- og søsiden, f.eks. adgangs- og tilkørselsveje, ankerpladser, nærliggende hav- og søområder.
- Havnens indretning, f.eks. havnekontorets placering, bygninger, broer, jernbaner, veje, cykel- og gangstier.

- Sikringsudstyr på havnen, f.eks. hegn, porte, bomme.
- Andre relevante forhold, f.eks. offentlige anlæg, særligt adgangsbegrænsede områder.

Alle vedlagte kort indskrives i skemaet med angivelse af bilagsnummer samt navn. Efter skemaet indskrives relevante beskrivelser af havnen.

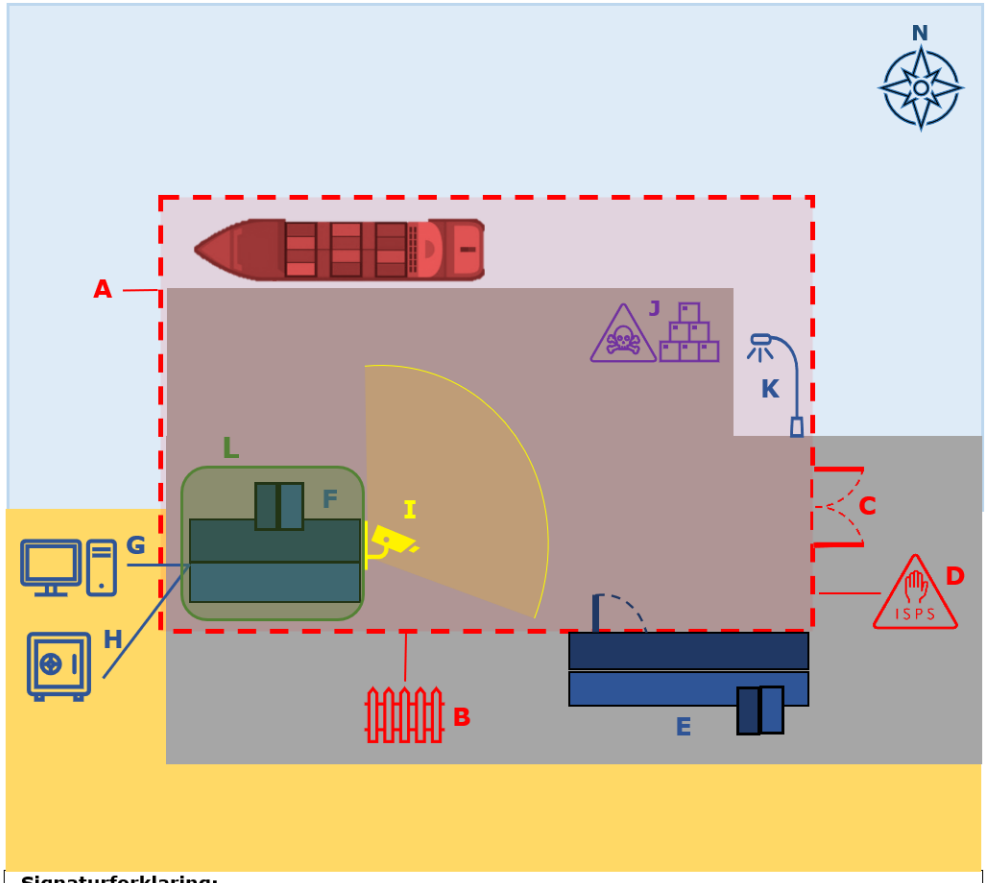


2.2 Oversigtskort over ejendom og infrastruktur på havnefaciliteten

Som bilag til ansøgningen vedlægges detaljerede oversigtskort over havnefaciliteten, der klart angiver de sikringsmæssige aspekter. Kortene skal indeholde en signaturforklaring samt tydeligt identificere og markere følgende:

- Facilitetens afgrænsning.
- Adgang fra land- og søsiden, f.eks. adgangs- og tilkørselsveje, indgange, adgangen fra havnen ind på facilitetens område, indsejlingen, manøvre- og fortøjningsområder.
- Facilitetens indretning, f.eks. havnekontorets placering, bygninger, broer, jernbaner, veje, cykel- og gangstier, lagerområder, lagerbygninger, godsterminaler, kaj- og passagerområder og udstyr til håndtering af gods/last.
- Sikringsudstyr på faciliteten, f.eks. permanent hegn, mobilhegn, porte, døre, mure, bomme, skilte, belysningsforhold, videokameraer, scannings- og røntgenudstyr
- Andre relevante forhold, f.eks. offentlige anlæg, særligt adgangsbegrænsede områder, opmarchområder, parkeringspladser, opbevaring af farligt gods eller farlige stoffer, placering af virksomheder og naboer til havnefaciliteten.

Havnefacilitetens afgrænsning skal tydeligt fremgå af kortet, herunder både grænser til søs og på land samt eventuelle særligt adgangsbegrænsede områder.



Signaturforklaring:

A: Facilitetens afgrænsning
B: Hegn opsat langs hele landsiden
C: Portåbning
D: ISPS-skiltning
E: Virksomhed X, del af perimetersikringen
L: Særligt adgangsbegrænset område
F: Havnekontoret
G: Server placeret på havnekontoret
H: Pengeskab placeret på havnekontoret
I: Videoovervågning
J: Oplag af farligt gods
K: Belysning

En havnefacilitet vil i udgangspunktet være at betragte som et område med adgangsbegrænsning. Derudover kan der være områder på eller med tilknytning til faciliteten, som direkte eller indirekte understøtter facilitetens maritime sikring. Sådanne områder kan på grund af deres sårbarhed have et yderligere lag af adgangsbegrænsning, og vil så betragtes som områder med særlig adgangsbegrænsning. Sådanne områder er i forordningen betegnet som "områder med adgangsbegrænsning", jf. f.eks. ISPS-kodens del A, pkt. 1.3.3. For at undgå misforståelser i forhold til den generelle adgangsbegrænsning til havnefaciliteten, er områderne hvortil der er behov for yderligere adgangsbegrænsning benævnt "særligt adgangsbegrænsede områder" i denne vejledning.

Et særligt adgangsbegrænset område kan f.eks. være et område, hvor der opbevares farligt gods, etableres midlertidig adgangskontrol i forbindelse med anløb af tenderbåde fra krydstogtskibe eller elektriske distributionssystemer. Det kan også være havnekontoret, da den maritime sikring ofte overvåges og styres herfra.

Bemærk, at afgrænsningen af havnefaciliteten ikke skal godkendes af TS. Styrelsen kan dog have bemærkninger til afgrænsningen, som ansøger skal forholde sig til. Det er vigtigt at holde sig for øje, at afgrænsningen ikke bliver for snæver.

Alle vedlagte kort indskrives i skemaet med angivelse af bilagsnummer samt navn. Efter skemaet indskrives relevante beskrivelser af havnefaciliteten.

2.3 Havnefacilitetens aktivitet

I dette afsnit beskrives aktiviteterne på havnefaciliteten, f.eks. skibsanløb, gods- og passageromsætning samt trafikmønstre.

2.3.1 Beskrivelse af forventet årlig skibstrafik på havnefaciliteten

Skemaet udfyldes i de felter, som har relevans for faciliteten dog med den undtagelse, at alle felter i kolonnen "*Antal anløb*" udfyldes jf. beskrivelse nedenfor.

	Beskrivelse
Antal anløb	Det forventede årlige antal skibsanløb fordelt på skibstyper. Alle felter i kolonnen udfyldes. Dersom faciliteten ikke anløbes af en bestemt skibstype skrives "*0*" i feltet. I nederste række "*Total*" opsummeres det samlede antal skibsanløb.
Antal passagerer	Det forventede årlige antal passagerer fordelt på skibstyper. I nederste række "*Total*" opsummeres det samlede antal passagerer.
Type af gods	Typen af gods som faciliteten håndterer. Her kan bruges de samme kategorier som fremgår på forsiden (vådbulk, skibsværft, containere, tørbulk, stykgods, passagerer eller andet) eller en mere præcis kategorisering, hvis dette er relevant.
Mængde	Den forventede årlige mængde gods (i tons) fordelt på skibstyper. Hvis godsmængden ikke er angivet i tons, skal den valgte enhed tydeligt fremgå.

Beskrivelse af kategorien "Ikke ISPS-skibe":

Dette felt udfyldes, hvis linjen "*Ikke ISPS-skibe*" i skema 2.3.1 er udfyldt.

Her beskrives, hvilke andre skibstyper som forventes at anløbe faciliteten. Det kunne f.eks. være krigsskibe, troppetransportskibe, andre statsskibe, lastskibe med en bruttotonnage på under 500, skibe uden mekanisk fremdrivning, træskibe af primitiv konstruktion, fiskeskibe eller skibe, der ikke anvendes i erhvervsmæssigt øjemed.

Beskrivelse af trafikmønster på havnefaciliteten:

Her beskrives f.eks. hvor skibene typisk kommer fra/til, og hvilken fast rutefart, der eventuelt udgår fra havnefaciliteten.

2.3.2 Beskrivelse af anden aktivitet på havnefaciliteten

Her beskrives anden relevant aktivitet på havnefaciliteten. Det kan f.eks. være:

- Håndteringen af tankanlæg, lastudstyr mv.
- Ventekaj, oplægningsplads mv.
- Godstrafik til/fra havnefaciliteten f.eks. jernbanetransport, tankbiler, containere mv.
- Skibsværfter eller andre værksteder
- Øvrig væsentlig aktivitet på havnefaciliteten og søområdet i nærheden af havnefaciliteten f.eks. fritidsskibe, fiskeskibe, indenrigsfærger, søredningsfartøjer, politi- og militære fartøjer mv.

2.4 Virksomhedsprofiler på havnefaciliteten

Dette afsnit indeholder en beskrivelse af virksomheder på havnefaciliteten, som ikke er en del af havnefacilitetens organisation. Beskrivelsen skal danne grundlag for udvælgelsen af, hvilke virksomheder der senere medtages i analysen i afsnit 5.1.

Der laves et skema for hver virksomhed. Skemaerne kopieres og indsættes efter behov. Der er desuden mulighed for at nummerere de enkelte skemaer i tekstfeltet i øverste venstre hjørne. Før skemaerne er der desuden mulighed for at skrive en tekst som supplement til de vedlagte virksomhedsprofiler.

Hvis der er mange virksomheder, kan man alternativt opliste de udvalgte virksomheder i et Excel dokument, som dækker de samme tekstfelter, eller kopiere alle skemaerne over i et bilag. I så fald knyttes der en bemærkning om dette i tekstfeltet.

Følgende oplysninger angives for hver virksomhed:

Tekstfelt	Beskrivelse
Navn	Navn på virksomheden
Adresse	Virksomhedens postadresse på havnefaciliteten
Beskrivelse af placering på faciliteten	Henvisning og placering på oversigtskort med evt. supplerende bilag jf. afsnit 2.2.
Antal medarbejdere	Antal medarbejdere i virksomheden
Aktiviteter	Virksomhedens aktiviteter og forretningsområder
Risikovirksomhed	Angiv, hvorvidt virksomheden er kategoriseret som en risikovirksomhed jf. gældende bekendtgørelse om kontrol med risikoen for større uheld med farlige stoffer (risikobekendtgørelsen) Kolonne 2 og 3 virksomheder skal altid risikovurderes i havnefacilitetens sårbarhedsvurdering.
Øvrige relevante forhold	Hvis der er øvrige forhold ved den enkelte virksomhed, som kan have indflydelse på sikringen af havnefaciliteten, skal dette også risikovurderes i sårbarhedsvurderingen. Det kunne f.eks. være, hvis virksomheden har en særlig økonomisk, strategisk, eller symbolsk betydning, ligger i perimeteren eller har et stort antal udefrakommende gæster. Et andet eksempel kunne være en butik, som sælger hårde hvidevarer. Butikken er beliggende uden for faciliteten, men varemodtagelsen af de hårde hvidevarer foregår inde på selve havnefaciliteten. Her angives også, hvis virksomheden har et anlæg indenfor elsektoren som er klassificeret (klasse 1, klasse 2 eller klasse 3) efter reglerne i gældende bekendtgørelse om beredskab for elsektoren (beredskabsbekendtgørelsen – el). Det kan også være relevant hvis der f.eks. er tale om en virksomhed med særlige sikringsaspekter. Det kunne f.eks. være oplag af brandfarlige væsker og gasser.

3 Eksisterende sikringsforhold

Dette afsnit indeholder en kort overordnet beskrivelse af eksisterende forhold med sikringsmæssig betydning på havnefaciliteten.

3.1 Liste over beredskabsplaner

I skemaet oplistes relevante beredskabsplaner herunder egne beredskabsplaner og beredskabsplaner fra andre myndigheder eller aktører.

Det kan f.eks. være beredskabsplaner i henhold til risikobekendtgørelsen[1], beredskabsbekendtgørelsen (el)[2] eller kommunale krisestyringsplaner for beredskabshændelser.

I første kolonne skrives navnet på beredskabsplanen. Herefter beskrives på et overordnet niveau beredskabstype, samarbejdende myndigheder og planens samspil med sikringen på faciliteten.

Det er relevant, at man er opmærksom på eventuelle sammenhænge med andre beredskabs- og evakueringsplaner, med henblik på senere at fastsætte relevante sikringstiltag i PFSP. Der bør således være en nærmere beskrivelse af interaktion og koordination med andre beredskabs- og krisestyringsplaner, så eventuelle konflikter og mangler identificeres.

3.2 Oversigt over sikringstiltag

3.2.1 Beskrivelse af fysisk sikring på havnefaciliteten

Her beskrives den fysiske sikring på havnefaciliteten. Den bør indeholde en kort overordnet beskrivelse af de enkelte elementer.

Det kan f.eks. være hegn, porte, døre, mure, bomme, bygninger, andre permanente barrierer, skilte eller belysningsforhold.

Det kan også være sikrings- og overvågningsudstyr samt sikrings- og overvågningssystemer såsom videokameraer, adgangskontrolsystemer, alarmsystemer, låsesystemer, vagtfunktioner eller scannings- og røntgenudstyr.

3.2.2 Beskrivelse af strukturel integritet på havnefaciliteten

Her beskrives den strukturelle integritet på havnefaciliteten.

Hvis en perimetersikring består af en bygning, så skal der være en beskrivelse af bygningens tilstand. Er bygningen f.eks. et forfaldent pakhus med løse vinduer og døre, kan dette være væsentligt at have med i sårbarhedsvurderingen.

Er perimetersikringen et hegn, kan hegnets strukturelle integritet beskrives som hegnets tilstand og udformning, ligesom kajens tilstand og udformning skal indgå i vurderingen.

3.2.3 Beskrivelse af personlige beskyttelsessystemer på havnefaciliteten

Her beskrives de personlige beskyttelsessystemer, som findes på faciliteten. Det bør indeholde en kort overordnet beskrivelse af de enkelte elementer.

[1] Bekendtgørelse om kontrol med risikoen for større uheld med farlige stoffer

[2] Bekendtgørelse om beredskab for elsektoren

Herved menes det udstyr, som facilitetens personale har med sig rundt i forbindelse med sikringsopgaver. Det kan f.eks. være uniformer, lygter, id-kort, mobiltelefoner, overfaldsalarmer, walkie-talkies, håndholdte VHF-radioer mv.

3.2.4 Beskrivelse af proceduremæssige fremgangsmåder på havnefaciliteten

Her beskrives de proceduremæssige fremgangsmåder på havnefaciliteten. Det betyder i praksis, at det skal være beskrevet, hvad personer i havnefacilitetens sikringsorganisation har af sikringsmæssige opgaver.

Afsnittet skal berøre alle, for havnefaciliteten, relevante emner, herunder f.eks. overvågning, adgangskontrol, håndtering af passagerer, gods og stores mv.

For en mere uddybende beskrivelse af proceduremæssige fremgangsmåder henvises til henholdsvis afsnit 5.9 om gods- og lasthåndtering, 5.14 om personale ved havnefaciliteten og 5.15 om eksterne samarbejdspartnere og leverandører.

Der er 7 obligatoriske proceduremæssige fremgangsmåder i en PFSA

De proceduremæssige fremgangsmåder **skal** fremgå af PFSA. Det vil derfor ikke være tilstrækkeligt at henvise til de proceduremæssige fremgangsmåder i en eksisterende sikringsplan.

Afsnittet **skal**, som minimum, indeholde en kort overordnet beskrivelse af følgende 7 obligatoriske proceduremæssige fremgangsmåder:

- Hvordan sikres det, at alle havnefacilitetens sikringsfunktioner virker tilfredsstillende?
- Hvordan kontrolleres adgangen til havnefaciliteten?
- Hvordan overvåges området, herunder forankrings- og kajområder?
- Hvordan overvåges særligt adgangsbegrænsede områder for at sikre, at kun bemyndigede personer har adgang hertil?
- Hvordan føres der tilsyn med håndteringen af last?
- Hvordan føres der tilsyn med håndtering af stores?
- Hvordan sikres det, at sikringsrelateret kommunikation er umiddelbar tilgængelig?

Afsnittet **skal** indeholde øvrige proceduremæssige fremgangsmåder, hvis de er relevante for havnefaciliteten (listen er ikke udtømmende):

- Hvordan sikres det, at sikringsrelaterede oplysninger beskyttes mod uautoriseret adgang og udbredelse?
- Hvordan håndteres sikringen fra OFF til ON og omvendt?
- Hvordan håndteres krydstogtsanløb?
- Hvordan håndteres bunkeroperationer?
- Hvordan håndteres ledsaget og uledsaget bagage?
- Hvordan håndteres køretøjer?
- Hvordan håndteres gående passagerer?
- Hvordan håndteres cyberangreb f.eks. på adgangskontrolsystemet eller videoovervågningen? (procedurer for nedbrud/angreb samt gendannelse).

3.2.5 Beskrivelse af radio- og telekommunikationssystemer, herunder computersystemer og -netværk på havnefaciliteten samt cyber security

Her beskrives radio- og telekommunikationssystemer, herunder computersystemer og -netværk på havnefaciliteten. Der forventes en kort overordnet beskrivelse af de enkelte systemer, herunder også hvilke eksisterende sikringstiltag i forhold til cyber security, som er taget i forhold til de enkelte systemer og deres fysiske placering.

Det kan f.eks. være mobiltelefoner, fastnettelefoner, nødkommunikationssystemer, dør- og porttelefoner, hardware, servere, routere, LAN, åbne trådløse netværk, software og trafikstyringssystemer for havnefartøjer og navigationshjælpemidler.

For en mere uddybende beskrivelse af cyber security henvises til afsnit 5.5.

3.2.6 Beskrivelse af relevant transportinfrastruktur på havnefaciliteten

Her beskrives relevant transportinfrastruktur på havnefaciliteten. Der forventes en kort overordnet beskrivelse af de enkelte elementer.

Afsnittet kan blandt andet indeholde en kort overordnet beskrivelse af:

- Adgang fra landsiden f.eks. adgangs- og tilkørselsveje, indgange, opmarcharealer og parkeringspladser.
- Adgang fra søsiden f.eks. ankerpladser, manøvre- og fortøjningsområder, nærliggende hav- og søområder, overvågning af søsiden, eller delt indsejling med andre maritime aktiviteter f.eks. fritidsskibe eller fiskeskibe.
- Udstyr til håndtering af gods/last, kraner, transportbånd, manifolde, pumper, mobile køretøjer, farligt gods og farlige stoffer, opbevaring af gods/last på faciliteten samt evt. overvågning af dette, lagerområder, lagerbygninger, godsterminaler, håndtering af bagage og stores til skibe.
- Broer, jernbaner, veje, cykel- og gangstier

3.2.7 Beskrivelse af offentlige anlæg på havnefaciliteten

Her beskrives offentlige anlæg på havnefaciliteten. Der forventes en kort overordnet beskrivelse af de enkelte elementer.

Det kan f.eks. være kraftværker, rørledninger til overførsel af last, skjulte rørledninger, vandforsyning, spildevandsledninger, transformatorstationer, nødstrømsanlæg, elmaster, søkabler og andre elektriske distributionssystemer, toldkontrol, brandstationer eller militære anlæg.

3.2.8 Beskrivelse af andre områder, der, hvis de beskadiges eller anvendes til ulovlig observation, indebærer en risiko for personer, ejendom eller operationerne i havnefaciliteten

Her beskrives andre områder, der, hvis de beskadiges eller anvendes til ulovlig observation, indebærer en risiko for personer, ejendom eller operationerne i havnefaciliteten. Det bør indeholde en kort overordnet beskrivelse af de enkelte elementer.

Det kan f.eks. være havnefartøjer, naboer til havnefaciliteten herunder ejendomme og bygninger i grænsefladen, kaj- og passagerområder eller andre omkringliggende områder, der kan benyttes i forbindelse med en sikringsrelateret hændelse til angreb/observation, offentlige anlæg, tankanlæg, toldkontrol, brandstationer, militære anlæg og andre områder med offentlig adgang.

4 Organisation

Dette afsnit indeholder en beskrivelse af havnefacilitetens generelle organisation og sikringsorganisation, herunder PFSO samt personalegrupper med/uden sikringsansvar.

Formålet med beskrivelsen af organisationen og personalegruppernes kompetencer er at afdække mulige sårbarheder med hensyn til medarbejdernes kompetencer. Det vil således blive afklaret, hvis der er uddannelsesmæssigt underskud, eller hvis der er behov for at supplere med yderligere kurser e.l.

Formålet er også at afdække de forskellige personalegruppers pålidelighed i relation til sikringsmæssige opgaver og beføjelser. Det kan derfor også give god mening, at havnen overvejer, om der er grund til at bede om f.eks. en straffeattest, hvis en medarbejder skal arbejde med og have indsigt i maritim sikring.

Der skal derfor i sårbarhedsvurderingen redegøres for personalegruppernes kompetencer i henhold til kravene i ISPS-koden. Dette kendskab skal sikres gennem den korrekte oplæring, som PFSO er ansvarlig for. ISPS-kodens del B, pkt. 18.1, 18.2 og 18.3 oplister en række eksempler på, hvad de respektive personalegrupper kan have af kompetencer, men oplistningen er ikke udtømmende.

Bemærk, at der i havnefacilitetssikringsplanen (PFSP) skal redegøres i detaljer for de uddannelsesmæssige krav og personalets kvalifikationer. I sårbarhedsvurderingen forventes det derfor, at beskrivelsen er på et overordnet niveau.

Herudover skal der i dette afsnit beskrives, hvor mange personer der er tilknyttet faciliteten, og hvor mange af disse, der har sikringsansvar. En sådan oplysning er f.eks. væsentlig for at kunne vurdere, om PFSA'ens anbefalinger til bedre sikring af faciliteten er mulige inden for de eksisterende rammer.

TS skal gøre opmærksom på, at jf. ISPS-kodens del A, pkt. 17.3 *"skal PFSO ydes den fornødne støtte til at opfylde de forpligtelser og dække de ansvarsområder, som PFSO pålægges i kapitel XI-2 (SOLAS) og denne del af koden (A-delen)"*.

4.1 Havnens generelle organisation

Vedlæg organisationsdiagram for havnen eller den selvstændige terminaloperatørs generelle organisation i et bilag til ansøgningen.

Organisationsdiagrammet forventes at vise ejerforhold, ansvarsstrukturer og andet, der kan have betydning for forståelse af havnefacilitetens organisatoriske struktur. Det vil f.eks. have betydning i forhold til at kunne vurdere, hvorvidt PFSO ydes den fornødne støtte til at opfylde de forpligtelser og dække de ansvarsområder, som PFSO pålægges.

Hvis organisationsdiagrammet ikke entydigt angiver ejerforhold og ansvarsstruktur i relation til maritim sikring, skal det beskrives i tekstfeltet.

4.2 Havnefacilitetens sikringsorganisation

Vedlæg organisationsdiagram for havnefacilitetens sikringsorganisation i et bilag til ansøgningen. Det skal fremgå, hvordan sikringsorganisationen hører hjemme i den generelle organisation.

Organisationsdiagrammet bør typisk have PFSO som den overordnede sikringsansvarlige for havnefaciliteten. PFSO kan have en række personer med sikringsansvar under sig, f.eks. assisterende PFSO og vagthavende PFSO. Eksterne firmaer kan også udgøre en del af sikringsorganisationen f.eks. skibsmæglere, stevedorer og vagtselskaber. Derudover er det relevant at medtage personale (internt eller eksternt) som varetager sikringsmæssige opgaver herunder også indenfor cyber security.

Der skal skrives en kort tekst som supplement til det vedlagte organisationsdiagram f.eks. hvordan sikringsorganisationen hører hjemme i den generelle organisation.

4.2.1 Havnefacilitetens sikringsansvarlige (PFSO)

	Beskrivelse
Navn	Navn på havnefacilitetens PFSO
Titel	Titel på havnefacilitetens PFSO
Uddannelse	PFSO bør som udgangspunkt have de kompetencer, der oplistes i ISPS-kodens del B, pkt. 18.1. Bemærk at listen er ikke udtømmende. Kompetencer indenfor cyber security kan også være relevant. Hvis faciliteten håndterer farligt gods, kan det desuden være relevant at supplere ovennævnte kvalifikationer i henhold til de vejledende afsnit om sikringsrelateret uddannelse i henholdsvis IMDG-kodens kapitel 1.4 samt IMSBC-kodens kapitel 11.

4.2.2 Personalegrupper med sikringsopgaver

	Beskrivelse
Funktion	Her indsættes de forskellige funktioner for både interne og eksterne personalegrupper f.eks. havnearbejdere, administrativt personale, skibsmæglere, stevedorer, vagtselskab mv.
Intern/ekstern	Angiv, hvorvidt der er tale om en intern eller ekstern personalegruppe. Ved eksternt personale menes personalegrupper, som ikke er en del af havnens generelle organisation. Det kan f.eks. være skibsmæglere, stevedorer eller eksterne vagtselskaber.
Antal	Angiv det omtrentlige antal personer med sikringsopgaver. Det vil sige personer, som har eller vil få specifikke sikringsopgaver i henhold til PFSP.
Sikringsrelateret uddannelse	Personer med specifikke sikringsopgaver kan have de kompetencer, der oplistes i ISPS-kodens del B, pkt. 18.2. Bemærk at listen ikke er udtømmende. Disse er de samme som angivet i pkt. 18.3 med en række tilføjelser. Blandt andet skal personale med sikringsopgaver have kendskab til sikringsrelateret kommunikation og teknikker til genkendelse af mistænkelige personer og genstande.

	Kompetencer indenfor cyber security kan også være relevant. Hvis faciliteten håndterer farligt gods, kan det desuden være relevant at supplere ovennævnte kvalifikationer i henhold til de vejledende afsnit om sikringsrelateret uddannelse i henholdsvis IMDG-kodens kapitel 1.4 samt IMSBC-kodens kapitel 11.

4.2.3 Personalegrupper uden sikringsopgaver

	Beskrivelse
Funktion	Her indsættes de forskellige funktioner for personalegrupper uden sikringsopgaver f.eks. rengøringspersonale, kantinemedarbejdere, reparatører, andre ansatte på virksomheder tilknyttet havnefaciliteten.
Antal	Angiv det omtrentlige antal personer uden sikringsopgaver. Det vil sige personer, som ikke har specifikke sikringsopgaver i henhold til PFSP.
Eventuel sikringsrelateret uddannelse	Personer uden sikringsopgaver kan have de kompetencer, der oplistes i ISPS-kodens del B, pkt. 18.3. Bemærk at listen ikke er udtømmende. Det kan f.eks. være relevant for denne gruppe at modtage træning indenfor cyber security herunder awareness og sikkerhedskultur. Der er ikke noget krav om uddannelse, men det er en fordel, at denne persongruppe ved, at de kan henvende sig til PFSO, hvis de observerer sikringsrelaterede hændelser eller mistænkelig adfærd i relation til sikring af havnen.

De vedlagte organisationsdiagrammer skal afspejle og være understøttet af de valgte funktionsbeskrivelser for de forskellige personalegrupper som fremgår i skema 4.2.1, 4.2.2 samt 4.2.3.

4.2.4 Beskrivelse af dagligt fremmøde på havnefaciliteten

I dette afsnit beskrives, hvordan bemandingen er på havnefaciliteten på de forskellige tidspunkter af døgnet, ugen eller året. Dette er særligt aktuelt, hvis der ikke er døgnbemanding.

4.2.5 Vurdering af personalegruppers pålidelighed

Her beskrives, hvis det skønnes relevant, forskellige personalegruppers pålidelighed i relation til sikringsmæssige opgaver og beføjelser. Ved personalegrupper menes både personale ved havnefaciliteten samt eksterne samarbejdspartnere og leverandører. Det kan f.eks. være relevant at indhente en straffeattest, hvis en medarbejder skal arbejde med og have indsigt i maritim sikring.

Hvis der ikke findes personalegrupper, hvor det f.eks. er relevant at indhente en straffeattest, skrives dette i feltet.

5 Identifikation af vigtig ejendom, infrastruktur, politikker og procedurer

Dette afsnit, som er det grundliggende element i analysedelen, indeholder en identifikation af vigtig ejendom, infrastruktur, politikker og procedurer for at identificere sårbare elementer på havnefaciliteterne.

Formålet med afsnittet er at identificere hvilke elementer, som skal overføres til trusselsmatrixen i afsnit 6.2. Eksempler på ejendomme og infrastruktur kan ses i ISPS-kodens del B, pkt. 15.7, og en række vejledende eksempler til identificeringen af sårbare elementer, når det drejer sig om havnefaciliteter kan ses i ISPS-kodens del B, pkt. 15.16.

I den henseende er det vigtigt at fokusere på, at formålet med maritim sikring er at beskytte den internationale skibstrafik og havnefaciliteter mod forsætlige ulovlige handlinger.

Det er med baggrund i formålet med maritim sikring, at elementerne vurderes i forhold til væsentlighed (V) og sårbarhed (S). Det betyder f.eks., at en virksomhed, som er vigtig for lokalområdet og havnefacilitetens drift, ikke nødvendigvis også er væsentlig (V) og sårbar (S) i relation til formålet med maritim sikring, da maritim sikring i udgangspunktet ikke har til formål at beskytte virksomheder på havnefaciliteten. Det er derfor udelukkende de elementer, der vurderes til både at være væsentlige (V) og sårbare (S) i relation til formålet med maritim sikring, som skal overføres trusselsmatrixen i afsnit 6.2.

Beskrivelsen i skemaerne (5.1 til 5.15) skal indeholde en god beskrivelse af de enkelte relevante elementer, specielt deres **anvendelse og betydning for havnefacilitetens sikring og drift i relation til formålet med maritim sikring**. Det er ikke intentionen, at dette afsnit skal være en gentagelse af de beskrivende afsnit 2, 3 og 4, men en fortsættelse! Afsnit 5 er den første del af analysen.

Beskrivelserne skal omfatte de relevante elementers anvendelse og betydning for havnefacilitetens sikring og drift i relation til formålet med maritim sikring

En PFSA skal afdække sikringsspørgsmål, der affødes af grænsefladen mellem skib og havnefacilitet samt havn og andre sikringsforanstaltninger. Det overordnede formål i PFSA er at se på risici på havnefaciliteterne. Det gøres ved at identificere og vurdere elementer, som er vigtige i forhold til havnefaciliteternes sikring og drift i relation til formålet med maritim sikring.

Endelig skal opmærksomheden henledes på, at sikring ikke blot er fysiske tiltag, men også kan være kommunikative, koordinerende og operative tiltag. Derfor skal også f.eks. manglende procedurer eller manglende uddannelse og træning tænkes ind i analysen.

Skemaerne skal således indeholde elementer, som er relevante for havnefacilitetens sikring uanset om det ligger på eller uden for havnefaciliteten.

Husk, at vurdering af konsekvens og sandsynlighed først foretages i afsnit 7.2 om risikovurdering

Alle elementer, som er relevante, indsættes i skemaerne (5.1 til 5.15). Derpå vurderes det, hvorvidt elementet er væsentligt (V) og sårbart (S) i relation til formålet med maritim sikring. Afkrydsning af "Ikke relevant" i skemaerne benyttes kun i tilfælde af, at de enkelte skemaer ikke er relevante for havnefaciliteten. Det kan f.eks. være tilfældet, hvis der ikke findes risikovirksomheder på havnefaciliteten. I dette tilfælde afkrydses "Ikke relevant" i skemaet 5.2 om risikovirksomheder.

Væsentligt (V)

Hvis det relevante element er væsentlig i relation til maritim sikring, afkrydses dette i kolonnen V, og det beskrives hvorfor elementet vurderes væsentlig (V).

Ved væsentligt menes, hvorvidt elementet har en værdi for havnefaciliteten i relation til formålet med maritim sikring. Væsentlighed refererer således til graden af relevans, om hvorvidt det valgte element har en værdi for havnefaciliteten i forhold til formålet med maritim sikring. Idet gode procedurer og veluddannede medarbejdere og leverandører har en værdi for havnefaciliteten, skal dette også tænkes ind under overskriften væsentligt.

Hvis et element ikke er væsentlig (V) i relation til maritim sikring, afkrydses der ikke i kolonne V, og det beskrives hvorfor elementet vurderes til ikke at være væsentlig (V).

Sårbart (S)

Hvis et element er vurderet som væsentlig (V) i henhold til ovenstående, skal der tages stilling til om elementet også er sårbart (S) i relation til formålet med maritim sikring.

Hvis et element vurderes sårbart i forhold til maritim sikring, afkrydses feltet i kolonne S og det beskrives hvorfor det er sårbart.

Ved sårbarhed menes, hvorvidt det har en negativ konsekvens for sikringen af havnefaciliteten i relation til formålet med maritim sikring, hvis der sker et nedbrud, bortfald eller konstateres en mangel. Sårbarhed refererer således til graden af skrøbelighed eller modtagelighed over for negative konsekvenser for sikringen af havnefaciliteten i relation til formålet med maritim sikring. Der er her vigtigt at vurderingen understøttes af argumenter for det valgte.

Hvis et element ikke vurderes som sårbart i forhold til maritim sikring, afkrydses feltet ikke og det beskrives hvorfor elementet ikke er sårbart.

Det er ikke nødvendigt at foretage en vurdering i forhold til sårbarhed, hvis elementet er vurderet til ikke at være væsentlig (V) i relation til maritim sikring.

Nedenstående kan hjælpe med at vurdere sårbarheden (S).

Nedbrud	**Bortfald**	**Mangler**
Vurdering af evne og ressourcer til at genskabe og reetablere efter nedbrud… Teknisk (IT-netværk/El mm.) Mennesker (pludseligt fravær) Andet (evt. afhængigheder) Tiltag (backup, serviceaftaler, redundans, substitution)	*Vurdering af evne og ressourcer til at opretholde sikringen ved bortfald…* Teknisk (fjernelse/ødelæggelse) Mennesker (udeblivelse/forhindring i fremmøde) Tiltag (substitution/udbedring)	*Vurdering af evt. manglende evner og ressourcer……* Teknisk (utilstrækkelig/kvaliteten) Procedurer (ufuldstændig/mangler) Mennesker (kompetencer/antal) Tiltag (Organisatorisk placering/ledelsesmæssig støtte/øvelse/uddannelse)

5.1 Ejendomme og bygninger mv.

Her identificeres relevante ejendomme og bygninger mv. på eller tæt ved havnefaciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Det er vigtigt, i samarbejde med politiet, at foretage en screening af hvilke ejendomme, bygninger, virksomheder mv. som er relevante at medtage i dette afsnit. Ejendomme med afgørende betydning for havnefaciliteter skal have særlig opmærksomhed i PFSA, med henblik på senere at fastsætte sikringstiltag i PFSP. For yderlige vejledning henvises til afsnit 2.4 om virksomhedsprofiler på havnefaciliteten.

Det kan f.eks. være havnekontoret, passagerterminalen, lagerbygninger, godsterminaler og virksomheder.

I vurderingen vil havnekontoret som udgangspunkt være at betegne som både væsentligt (V) og sårbart (S), selvom det ikke nødvendigvis er beliggende på faciliteten. Det kan f.eks. være, at videoovervågningen styres fra havnekontoret, at sårbarhedsvurderinger og sikringsplaner opbevares på havnekontoret, eller at det er her, man vil etablere en slags kommandocentral i sikringsøjemed.

Havnekontoret skal altid beskrives og analyseres i en PFSA

5.2 Risikovirksomheder

Her identificeres alle risikovirksomheder på havnefaciliteten. Herved forstås alle kolonne 2 og 3 virksomheder, som er klassificeret efter reglerne i risikobekendtgørelsen.

Kolonne 2 og 3 virksomheder på faciliteten vil altid være at betragte som både væsentlige (V) og sårbare (S), og skal derfor altid risikovurderes i afsnit 7.2.

Risikovirksomheder skal altid beskrives og analyseres i en PFSA

5.3 Perimetersikring, skilte og belysning

Her identificeres perimetersikring, skilte og belysning på havnefaciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Afsnittet kan blandt andet indeholde en vurdering af:

- Perimetersikring f.eks. hegn, porte, mure, bomme og andre permanente barrierer
- Bygninger i perimeteren
- Skilte om sikring
- Belysningsforhold

5.4 Sikrings- og overvågningsudstyr samt sikrings- og overvågningssystemer

Her identificeres relevant sikrings- og overvågningsudstyr samt sikrings- og overvågningssystemer på havnefaciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Afsnittet kan blandt andet indeholde en vurdering af:

- Sikrings- og overvågningsudstyr og sikrings- og overvågningssystemer, herunder også deres placering og dækning. Det kan f.eks. være videokameraer, termiske kameraer, adgangskontrolsystemer, nummerpladescannere, alarmsystemer, bevægelsessensorer, detektorer, sirener, højtalere, låsesystemer, fingeraftrykslæsere, ansigtsgenkendelse, scannings- og røntgenudstyr.
- Vagtfunktion f.eks. adgangskontrol, monitorering, rundering, patruljering, vagtselskaber og vagter.

5.5 Radio- og telekommunikationssystemer, herunder computersystemer og -netværk samt cyber security

Her identificeres relevante radio- og telekommunikationssystemer, herunder computersystemer og -netværk, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring. I vurderingen skal desuden indgå en beskrivelse af cyber security i forhold til de enkelte systemer og deres fysiske placering.

Afsnittet kan blandt andet indeholde en vurdering af:

- Radio- og telekommunikationssystemer, f.eks. mobiltelefoner, smartphones, tablets, walkie-talkies, fastnettelefoner, nødkommunikationssystemer og dør- og porttelefoner.
- Computersystemer og -netværk, f.eks. hardware, servere, routere, LAN og åbne trådløse netværk, og de tilknyttede fysiske og tekniske sikringstiltag, som er opsat til beskyttelse af disse.
- Software til computersystemer som styrer:
    - Sikrings- og overvågningssystemer f.eks. videoovervågning, termiske kameraer
    - Adgangskontrolsystemer f.eks. automatiske porte, nummerpladescannere
    - Alarmsystemer f.eks. bevægelsessensorer, detektorer, sirener
    - Identifikations- og autentificeringssystemer f.eks. låsesystemer, fingeraftrykslæsere, ansigtsgenkendelse
    - Evakueringssystemer f.eks. højtalere
    - Lasthåndteringssystemer samt tog- og lastbiltrafikovervågningssystemer
    - Billetkontrolsystemer

Cyber security

Drift, styring og sikringstiltag på en havnefacilitet er ofte afhængige af de tilknyttede IT-løsninger, og deres fortsatte funktion vil ofte være af afgørende betydning. Cyber security definerer den samlede mængde af foranstaltninger, som skal modvirke evt. trusler og understøtte til at funktionerne kan opretholdes.

Når der arbejdes med vurderingen af cyber security, anbefales det at afdække både organisatoriske, menneskelige og tekniske faktorer i forhold til formålet med at udfinde evt. sårbarheder. Det er her relevant at kigge på havnefacilitetens eksisterende sikringstiltag i relation til cyber security, som kan være af både forebyggende og afhjælpende karakter.

I nedenstående skema er opstillet typiske elementer inden for cyber security, som normalt anvendes til at skabe robusthed for kritiske operationer. Skemaet kan bruges som inspiration til at afdække og vurdere evt. mangler og potentielle sårbarheder. Det vil ofte være muligt at finde eksisterende IT-sikkerhedspolitikker, retningslinjer og understøttende funktioner i egen organisation og derved kan der typisk henvises til disse, hvis de er umiddelbar tilgængelige for relevante funktioner i sikringsorganisationen.

Sikringstiltag	Beskrivelse	Eksempler
Organisatoriske	Politikker	Kommunal IT-sikkerhedspolitik Virksomhedens IT-sikkerhedspolitik
	Ansvarsfordeling	Outsourcede opgaver IT-administrator IT-sikkerhedsansvarlig
	Retningslinjer	Rettighedsstyring Systemkrav og datakvalificering
Menneskelige	Uddannelse	Relevant viden om typiske cyberangreb alt efter funktion
	Awareness	Tiltag der kan fremme sikkerhedskulturen f.eks. kampagner om brug af USB-stik, e-mail/phishing og sms/smishing
	Handlekraft	Procedure for mistænkelig adfærd Procedure for rapportering
Tekniske	Netværkssikkerhed	Firewalls Regelmæssig softwareopdatering Segmentering af netværk
	Adgangskontrol	Logning og funktionsbestemte rettigheder Stærke kodeord
	Gendannelse	Backup systemer Test af systemer
	Fysisk sikring	Beskyttelse af relevant hardware og kabler mod uautoriseret adgang

Hvis IT-systemer er outsourcede, skal en vurdering af de eksterne leverandørers sikkerhedsniveau indgå, på samme måde som ved havnefacilitetens egne IT-systemer.

Der henvises i øvrigt til publikationer udgivet af ENISA (guidelines), ENISA (tool), International Maritime Organisation (IMO), Center for Cybersikkerhed samt EU-Kommissionens toolkit til cyber security og Guidance on how to treat cybersecurity at port facility and port level.

5.6 Trafikstyringssystemer og navigationshjælpemidler

Her identificeres relevante trafikstyringssystemer og navigationshjælpemidler, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Afsnittet kan blandt andet indeholde en vurdering af:

- Trafikstyringssystemer f.eks. udstyr på havnekontoret til hjælp for anløb af skibe, VHF/UHF-radio, radar, AIS-modtager
- Navigationshjælpemidler f.eks. fyr, båker, flydende afmærkning, broafmærkning og passagesignaler, racon, AIS-afmærkning og tågesignaler ved havne og broer.

Ovennævnte trafikstyringssystemer og navigationshjælpemidler er normalt beskrevet

- i danskehavnelods.dk, der indeholder oplysninger om havne og broer,
- i "Kort 1", der beskriver symboler, forkortelser og begreber i søkort eller
- i "Afmærkning af danske farvande", der beskriver forskellige typer af afmærkning.

I dette afsnit kan det også være relevant at foretage en vurdering i forhold til cyber security. For en mere uddybende beskrivelse af cyber security henvises til afsnit 5.5.

5.7 Adgang til havnefaciliteten fra landsiden

Her identificeres adgange fra landsiden til havnefaciliteten og til skibe, der er fortøjet på faciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Afsnittet kan indeholde en vurdering af f.eks. adgangs- og tilkørselsveje, indgange, opmarcharealer og parkeringspladser.

5.8 Adgang til havnefaciliteten fra søsiden

Her identificeres adgange fra søsiden til havnefaciliteten og til skibe, der er fortøjet/skal fortøjes på faciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Efter omstændighederne kan det også være ankerpladser, manøvre- og fortøjningsområder, nærliggende hav- og søområder, overvågning af søsiden, eller delt indsejling med andre maritime aktiviteter f.eks. fritidsskibe eller fiskeskibe.

Havne med kun en havnefacilitet (artikel 2.4 havn)

Det er vigtigt, at en havnefacilitets afgrænsning ikke bliver for snæver, men medtager alle relevante sammenbindende elementer, herunder særligt havnens vandområde. Havnefaciliteten skal med andre ord være så stor, at den omfatter hele det område, der er indrettet til og letter kommerciel søtransport i relation til formålet med maritim sikring.

Husk at havnefacilitetens afgrænsningen ikke må være for snæver

Der kan findes yderligere information om emnet i afsnit 5.8 i vores PSA-vejledning.

5.9 Gods- og lasthåndtering

Her identificeres relevant gods- og lasthåndtering samt passagerhåndtering, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Det kan f.eks. være udstyr til håndtering af gods/last, kraner, transportbånd, manifolde, pumper, rørledninger til overførsel af last og mobile køretøjer. Det kan også være opbevaring af gods/last på havnefaciliteten samt evt. overvågning af dette, håndtering af farligt gods og farlige stoffer, lagerområder, lagerbygninger, godsterminaler, håndtering af bagage og stores til skibe.

Havnefaciliteten er ansvarlig for sikring af last

Havnefaciliteten er ansvarlig for sikring af last og gods på facilitetens område. Det betyder f.eks., at det skal sikres, at uvedkommende ikke kan få adgang til godset/lasten, hvad enten det opbevares i kortere (før ombordkørsel) eller længere tid på faciliteten.

I dette afsnit identificeres og vurderes også relevante proceduremæssige fremgangsmåder vedrørende gods- og lasthåndtering samt passagerhåndtering.

Bemærk, at identifikation af relevante procedurer hænger sammen med beskrivelsen i afsnit 2.3 om havnefacilitetens aktivitet samt afsnit 3.2.4 om proceduremæssige fremgangsmåder på havnefaciliteten. I afsnit 2.3 og 3.2.4 bør det således være identificeret, hvorvidt havnefaciliteten har mulige sårbarheder vedr. procedurer for gods- og lasthåndtering samt passagerhåndtering.

Relevante ejendomme, bygninger og arealer som benyttes i forbindelse med gods- og lasthåndtering samt passagerhåndtering beskrives i afsnit 5.1 om ejendomme og bygninger mv.

Farligt gods og farlige stoffer

I vurderingen af farligt gods skal indgå, hvor ofte faciliteten håndterer farligt gods, mængden samt opbevaring. Derudover skal det beskrives, hvor faciliteten opbevarer farlige stoffer, som ikke er last.

Et område, hvor faciliteten opbevarer farligt gods og farlige stoffer, kan med fordel etableres som et særligt adgangsbegrænset område, jf. ISPS-kodens del B, pkt. 16.25, men det er ikke et krav.

Lagerbygninger, lagerområder og udstyr, som anvendes i forbindelse med farligt gods og farlige stoffer vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Farligt gods og farlige stoffer skal altid beskrives og analyseres i en PFSA

5.10 Broer, jernbaner og veje

Her identificeres alle broer, jernbaner og veje, dvs. hele den trafikale infrastruktur på havnefaciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Det kan f.eks. være broer, jernbaner, veje, cykel- og gangstier.

5.11 Kraftværker og vandforsyning

Her identificeres relevante kraftværker og vandforsyning på havnefaciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Det kan f.eks. være kraftværker, rørledninger, som ikke anvendes til lasthåndtering f.eks. vandforsyning og spildevandsledninger, transformatorstationer, nødstrømsanlæg, elmaster, søkabler og andre elektriske distributionssystemer.

5.12 Havnefartøjer

Her identificeres relevante havnefartøjer, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Det kan f.eks. være lodsbåde, slæbebåde, lægtere, pramme, havnefartøjer, turistbåde og havnerundfarter mv.

5.13 Andre arealer

Her identificeres andre relevante arealer på eller tæt ved havnefaciliteten, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Det kan f.eks. være ejendomme og bygninger i grænsefladen, kaj- og passageområder eller andre omkringliggende områder, der kan benyttes i forbindelse med en sikringsrelateret hændelse til angreb/observation, offentlige anlæg, tankanlæg, toldkontrol, brandstationer, militære anlæg og andre områder med offentlig adgang.

5.14 Personale ved havnefaciliteten

Her identificeres relevante elementer vedr. personale ved havnefaciliteten, herunder PFSO, personalegrupper med eller uden sikringsopgaver, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Bemærk i denne forbindelse, at manglende eller ufuldstændige procedurer eller mangel på uddannelse og/eller træning for personalet er væsentlige elementer at analysere i dette skema.

Derfor skal en PFSA også identificere sårbare elementer på faciliteten i forhold til organisatoriske og menneskelige faktorer i infrastruktur, politik og procedurer og uddannelse.

Identifikation af relevante elementer hænger sammen med beskrivelsen i afsnit 4 om organisation inklusive organisationsbilag samt afsnit 3.2.4 om proceduremæssige fremgangsmåder på havnefaciliteten. I afsnit 4 bør det således være identificeret, hvorvidt der er mulige sårbarheder med hensyn til interne personalegruppers kompetencer og pålidelighed.

I processen med at afdække, hvilke relevante elementer der bør medtages, kan følgende spørgsmål indgå i overvejelsen:

- Har personalet ved havnefaciliteten opgaver, som bevirker at de bør aflevere en straffeattest?
- Er der manglende eller ufuldstændige procedurer?
- Mangler personalet uddannelse i maritim sikring?
- Mangler personalet viden om cyber security?
- Har de ansatte kendskab til reglerne i ISPS-koden?
- Er der påvist sikringsproblemer under øvelser, og er der taget hånd om det?

- Er der, i forhold til personalet, sikringsproblemer i den daglige drift som følge af alarmer, indberetninger, anmeldelser, kontrolforanstaltninger mv?
- Vil tab af nøglemedarbejdere få konsekvenser?

5.15 Eksterne samarbejdspartnere og leverandører

Her identificeres relevante elementer vedr. eksterne samarbejdspartnere og leverandører, og de vurderes i forhold til væsentlighed (V) og sårbarhed (S) i relation til formålet med maritim sikring.

Ligesom for personalet i skema 5.14, er det også vigtigt i dette skema at have fokus på manglende eller ufuldstændige procedurer eller mangel på uddannelse og/eller træning.

Identifikation af relevante elementer hænger sammen med beskrivelsen i afsnit 4 om organisation inklusive organisationsbilag samt afsnit 3.2.4 om proceduremæssige fremgangsmåder på havnefaciliteten. I afsnit 4 bør det således være identificeret, hvorvidt der er mulige sårbarheder med hensyn til interne personalegruppers kompetencer og pålidelighed.

I processen med at afdække, hvilke relevante elementer, der bør medtages, kan følgende spørgsmål indgå i overvejelsen:

- Har eksterne samarbejdspartnere og leverandører ved havnefaciliteten opgaver, som bevirker at de bør aflevere en straffeattest?
- Er der manglende eller ufuldstændige procedurer?
- Er der leverancer, afhentning af gods mv. med eller uden opsyn?
- Har agenter og stevedorer sikringsopgaver?
- Har eksterne vagter og vagtselskaber sikringsopgaver?
- Mangler eksterne samarbejdspartnere og leverandører viden om ISPS og cyber security?
- Er der opsyn med håndværkere?

6 Trusler

Dette afsnit indeholder en beskrivelse af trusselsbilledet samt en vurdering af til- og fravalg af trusler og en sammenfatning af disse.

6.1 Vurdering af trusler

I dette afsnit beskrives det overordnede trusselsbillede på havnefaciliteten, hvorefter der på baggrund af trusselsbilledet foretages en vurdering af til- og fravalg af trusler.

Afsnit 6 er anden del af analysen. Det betyder, at intentionen med dette afsnit er, at man først på et overordnet niveau beskriver trusselsbilledet på havnefaciliteten ud fra en række relevante kilder, og herefter vurderer til- og fravalg af trusler, med udgangspunkt i de 10 fortrykte trusler i skema 6.1.1, og man må gerne supplere med andre relevante trusler.

Man skal altså analysere til- og fravalg af de enkelte trusler på baggrund af det beskrevne trusselsbillede.

Indhentning af information fra forskellige kilder er afgørende for at kunne vurdere hvilke trusler, som er relevante for havnefaciliteten, og det skal af beskrivelsen fremgå, hvilke kilder og grundlag, der er anvendt. Det kan f.eks. være de årlige rapporter fra Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste og Center for Cybersikkerhed samt dialog med det lokale politi mv.

I vurderingen af trusselsbilledet kan også indgå, hvilke personer eller grupper, som måtte have til hensigt at udføre forsætlige ulovlige handlinger mod havnefaciliteten, herunder en vurdering af deres tilstedeværelse, kapacitet, intention, historie, mål, motivation og handlemåder. Disse personer eller grupper kan f.eks. være fremmede efterretningstjenester, statssponsoreret terrorister, konkurrenter, kriminelle, cyberkriminelle, aktivister, terrorgrupper og insideree.

Der skal være sammenhæng mellem dette afsnit og skemaet i afsnit 6.1.1. Det betyder f.eks., at hvis man i dette afsnit har vurderet, at truslen ”hacking og kompromittering af IT-systemer” er relevant, så skal det også være markeret som relevant i skema 6.1.1.

6.1.1 Liste over trusler

I skemaet indsættes relevante trusler fra foregående afsnit. Skemaet indeholder 10 fortrykte trusler, som **altid** skal vurderes, men listen er ikke udtømmende og suppleres efter behov.

De 10 fortrykte trusler stammer således delvist fra ISPS-kodens del B, pkt. 15.11, hvor der er oplistet en række vejledende eksempler til identificeringen af trusler mod havnefaciliteter.

Andre eksempler på relevante trusler kan f.eks. være en bombetrussel mod skib ved faciliteten og uautoriseret adgang. Idet formålet med maritim sikring er at beskytte søfarten og havnefaciliteterne mod trusler om forsætlige ulovlige handlinger er det vigtigt, at den valgte relevante trussel indeholder et element af forsæt eller intentionel handling.

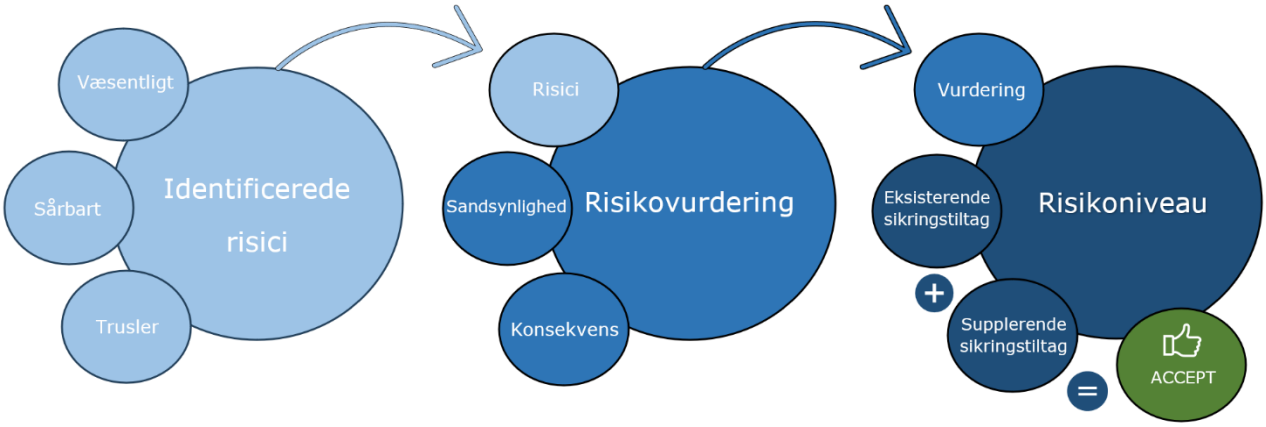
Ved uautoriseret adgang skal der ikke sondres mellem, om hensigten med adgangen er at foretage skade eller ej. Uautoriseret adgang vil altid udgøre en potentiel trussel. Hvis en lystfisker forvilder sig ind på en ISPS-facilitet, vil det også være muligt for personer med skadelige hensigter at få adgang.

6.2 Sammenfatning af væsentlige og sårbare elementer med relevante trusler

I trusselsmatrixen sammenfattes de elementer, som i afsnit 5 er vurderet til både at være væsentlige (V) og sårbare (S) i relation til formålet med maritim sikring, med de relevante trusler, som er identificeret under afsnit 6.1.

Formålet med afsnittet er at identificere de elementer, der er vurderet både væsentlige (V) og sårbare (S) og som derfor skal risikovurderes i afsnit 7.2. Der laves en risikovurdering i afsnit 7.2 for hver kryds i trusselsmatrixen i afsnit 6.2.1. Derudover indskrives de i listen over risikovurderinger i afsnit 7.1.

Der sættes et kryds ud for de elementer i trusselsmatrixen i afsnit 6.2.1, hvor der vurderes at være identificeret en risiko. Det gøres ud fra nedenstående model for identifikation af risici. Modellen beskriver de identificerede risici, som en gensidig afhængighed mellem trusler, væsentlighed (V) og sårbarhed (S).



Efterfølgende i afsnit 7.2 laves en risikovurdering af de identificerede risici. Dette gøres ved at vurdere den identificerede risiko i forhold til sandsynlighed og konsekvens. Ud fra denne vurdering tages herefter stilling til, hvorvidt de eksisterende sikringstiltag og supplerende sikringstiltag er tilstrækkelige til at kunne håndtere risikoniveauet på et acceptabelt niveau.

7 Risikovurdering af sårbar ejendom, infrastruktur samt sårbare elementer

Dette afsnit indeholder risikovurderinger samt en samlet oversigt over risikovurderingerne.

7.1 Liste over risikovurderinger

I skemaet indsættes, oplistes og nummereres alle risikovurderinger, som skal indgå i sårbarhedsvurderingen.

I feltet risikovurdering skrives navnet på den identificerede sårbarhed fra trusselsmatrixen i afsnit 6.2.1.

Antallet af krydser i trusselsmatrixen i afsnit 6.2.1. skal være identisk med antallet af risikovurderinger, som er oplistet i listen over risikovurderinger. Det vil sige, hvis der er 16 krydser i trusselsmatrixen, så skal der også være oplistet 16 (dertilhørende) risikovurderinger i skemaet.

Det er således ikke hensigten, at man puljer truslerne for at reducere antallet af risikovurderinger. Det betyder f.eks., at hvis man har identificeret 1 sårbarhed med dertilhørende 5 identificerede relevante trusler, så skal der også laves 5 risikovurderinger. Formålet med dette er at sikre, at alle de identificerede relevante trusler risikovurderes individuelt, uagtet at det ofte vil være de samme sikringstiltag, der tages i anvendelse.

7.2 Risikovurdering

Der skal foretages en risikovurdering af alle de trusler, som er relevante for de identificerede sårbarheder på havnefaciliteten. Det vil sige, at der skal udarbejdes risikovurderinger i overensstemmelse med listen over risikovurderinger i afsnit 7.1.

Formålet er at finde risikoniveauet for de enkelte trusler og evt. udpege nye eller revidere eksisterende sikringstiltag på havnefaciliteten.

7.2.1 Risikovurderingsmodel

Der er metodefrihed i forhold til, hvilken risikovurderingsmodel man anvender. I skabelonen er der stillet en model til rådighed, som frit kan anvendes. I dette afsnit gennemgås denne model i forhold til, hvordan den skal udfyldes.

Øverst i risikovurderingsskemaet udfyldes følgende:

	Beskrivelse
Nummer	Her indsættes nummeret fra listen over risikovurderinger i afsnit 7.1
Dato	Her indsættes datoen for hvornår risikovurderingen er blevet lavet i formatet (dag-måned-år)
Sårbarhed	Her indsættes den identificerede sårbarhed fra afsnit 6.2.1
Trussel	Her indsættes den identificerede relevante trussel fra afsnit 6.2.1

Efterfølgende skal hver af de identificerede sårbarheder på faciliteten vurderes i forhold til de identificerede relevante trusler i en matrix, som ses i risikovurderingsskemaet i afsnit 7.2.3. Dette gøres for at fastsætte risikoniveauet. Det er væsentligt, at den valgte trussel er relevant i forhold til den valgte sårbarhed. Det er f.eks. ikke meningsfuldt at vælge ”TV-overvågning”, som det sårbare element, og udsætte dette for truslen ”manipulation af lasten herunder smugling af våben”. Det vil i dette tilfælde f.eks. give mere mening at bruge truslen ”beskadigelse eller

ødelæggelse af havnefaciliteten f.eks. ved hjælp af sprængstofanordninger, ildspåsættelse, sabotage eller hærværk".

Risikoniveauet afhænger af to forhold:

- Hvad er konsekvensen hvis truslen indtræffer?
- Hvad er sandsynligheden for at truslen indtræffer?

Hvad er konsekvensen hvis truslen indtræffer?

Ved vurdering af hvor krydset skal sættes i matrixen i forhold til "konsekvens", det vil sige X-aksen, kan nedenstående skema benyttes.

Konsekvens	Beskrivelse
1 Begrænset	Ingen personskader og ingen dødsfald Minimale konsekvenser for økonomi eller operativ evne Minimal miljøpåvirkning, som har betydning for havnens drift Minimal tab af anseelse
2 Moderat	Mindre personskader og ingen dødsfald Mindre og rent lokale konsekvenser for økonomi og operativ evne Mindre miljøpåvirkning i lokalområde, som har betydning for havnens drift Mindre tab af anseelse
3 Alvorlig	Omfattende personskader og ingen dødsfald Store regionale konsekvenser for økonomi og operativ evne Lang tids miljøpåvirkning i lokalområde, som har betydning for havnens drift Større tab af anseelse
4 Meget alvorlig	Omfattende personskader og/eller flere dødsfald Nationale konsekvenser for økonomi og operativ evne Lang tids miljøpåvirkning over et større område, som har betydning for havnens drift Stort tab af anseelse
5 Kritisk	Meget omfattende personskader og/eller et stort antal dødsfald Store nationale eller internationale konsekvenser for økonomi og operativ evne. Varig miljøpåvirkning over et større område, som har betydning for havnens drift Meget stort tab af anseelse

Konsekvenser kan f.eks. være dødsfald, personskade, forringet operativ evne, miljøforurening som har betydning for havnens drift, økonomisk tab, tab af anseelse, sensitiv information offentliggøres, styrings- og informationssystemer kompromitteres, funktioners integritet tabes, vitale dele skades, tab af nøglepersoner, skade på infrastruktur og ejendele.

Når man skal vurdere konsekvensen af en hændelse, skal man ligge til grund, at hændelsen er indtruffet. Herefter vurderes, hvilken indvirkning (konsekvens), det vil have for faciliteten. I

ovenstående skema er der for hver graduering af konsekvens (1 til 5) oplistet fire forskellige typer af konsekvenser. Når man skal angive gradueringen af konsekvens i risikovurderingsskemaet, skal ikke alle typer af konsekvenser være opfyldt. Det betyder f.eks., at hvis konsekvensen vurderes til at være Alvorlig (3) på en af typerne (f.eks. større tab af anseelse), men Moderat (2) for de øvrige typer, så bliver den samlede vurdering af konsekvens dermed Alvorlig (3).

Hvad er sandsynligheden for at truslen indtræffer?

Ved vurdering af hvor krydset skal sættes i matrixen i forhold til "sandsynlighed", det vil sige Y-aksen, kan nedenstående skema benyttes. En nærmere beskrivelse af relevante personer eller grupper henvises til afsnit 6.

Sandsynlighed	Beskrivelse
I Meget usandsynligt	Der eksisterer ingen eller meget få personer, der har både ressourcer og motivation til at realisere en sikringshændelse, og de eksisterende sikringstiltag vurderes at være tilstrækkelige til at imødegå dette. Der er ingen indikationer til stede.
II Overvejende usandsynlig	Der eksisterer få personer eller grupper, der har både ressourcer og motivation til at realisere en sikringshændelse, og de eksisterende sikringstiltag vurderes at være tilstrækkelige til at imødegå dette.
III Sandsynligt	Der eksisterer nogle personer eller grupper, der har både ressourcer og motivation til at realisere en sikringshændelse, men pga. eksisterende sikringstiltag vurderes det at være muligt delvist at imødegå disse hændelser.
IV Overvejende sandsynligt	Der eksisterer flere personer eller grupper, der har både ressourcer og motivation til at realisere en sikringshændelse, og det vil kun kræve mindre forberedelse at omgå eksisterende sikringstiltag.
V Meget sandsynligt	Der eksisterer både flere personer og grupper med både ressourcer og motivation til at realisere en sikringshændelse, og de eksisterende sikringstiltag vurderes ikke at kunne imødegå disse hændelser.

I vurderingen af sandsynlighed tages hensyn til eksisterende sikringstiltag, som indskrives i feltet (eksisterende sikringstiltag) nederst i risikovurderingsskemaet.

Sammenfatning af risikovurderingen

Risikoniveauet kan accepteres, hvis man havner i det grå eller grønne felt. Hvis risikovurderingen viser, at risikoniveauet ikke kan accepteres (dvs. at man havner i gult, orange eller rødt felt i matrixen), skal der udpeges nye eller stærkere sikringstiltag. De nye udpegede eller stærkere sikringstiltag indskrives i feltet (forslag til yderligere sikringstiltag) nederst i risikovurderingsskemaet. Bemærk, at også eksisterende sikringstiltag på niveau 1 indskrives. Det skal beskrives om risikoniveauet herefter kan accepteres. Herefter tages der stilling til, hvorvidt disse nye eller stærkere sikringstiltag nedbringer risikoniveauet, så risikovurderingen ender i det grå eller grønne felt. Det vil sige, at risikoniveauet kan accepteres.

I skemaerne i afsnit 8 om konklusion og resume skal alle eksisterende og supplerende sikringstiltag indskrives.

7.2.2 Sikringstiltag

I vurderingen af hvilke sikringstiltag, som kunne være relevante i forhold til de identificerede sårbarheder, hvor risikovurderingen viser, at risikoniveauet ikke kan accepteres, kan der anvendes flere forskellige metoder for at imødegå dette.

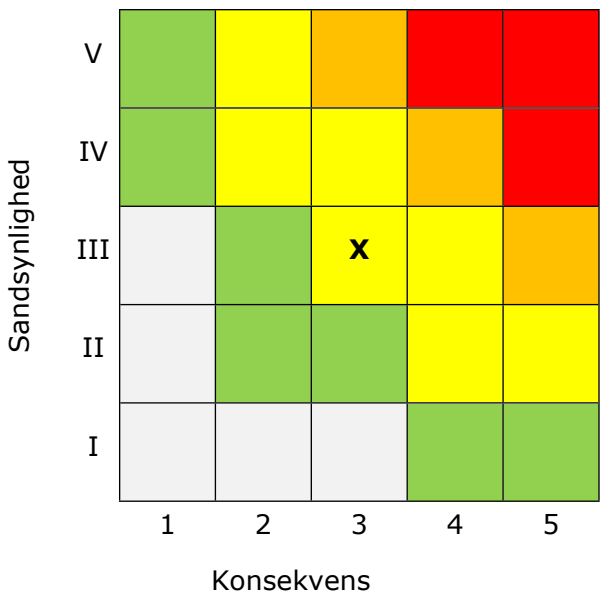
Sikringstiltagene kan være meget forskellige og kan indeholde alt fra proceduremæssige ændringer, uddannelse til fysiske sikringstiltag. Nedenstående skema oplister en række eksempler på forskellige sikringstiltag.

Sikringstiltag	Beskrivelse	Eksempler
Organisatoriske	Politikker	Kommunal IT-sikkerhedspolitik Virksomhedens IT-sikkerhedspolitik
	Ansvarsfordeling	Håndtering af mangel på ressourcer eller opbakning fra ledelsen Outsourcede opgaver f.eks. aftale med eksternt vagtselskab eller en IT-leverandør IT-administrator IT-sikkerhedsansvarlig
	Retningslinjer	Rettighedsstyring Systemkrav og datakvalificering
Menneskelige	Uddannelse	Eksterne ISPS-kurser Intern oplæring i organisationen herunder sidemandsoplæring Relevant viden om typiske cyberangreb alt efter funktion
	Awareness	Tiltag der kan fremme sikkerhedskulturen f.eks. øvelser, interne nyhedsbreve, posters med korte budskaber og kampagner. Det kan f.eks. være om brug af synligt id-kort, best practice, brug af USB-stik, e-mail/phishing og sms/smishing.
	Handlekraft	Ændring af proceduremæssige fremgangsmåder Procedure for mistænkelig adfærd Procedure for rapportering
Tekniske	Fysiske sikringstiltag	Hegn, porte, døre, mure, bomme, personlige beskyttelsessystemer f.eks. uniformer mv.
	Elektroniske sikringstiltag	Videokameraer, adgangskontrolsystemer, alarmsystemer, låsesystemer, scannings- og røntgenudstyr mv.
	Cyber security sikringstiltag	Firewalls, regelmæssig softwareopdatering, segmentering af netværk, logning og funktionsbestemte rettigheder, stærke kodeord, backup systemer, test af systemer, beskyttelse af relevant hardware og kabler mod uautoriseret adgang mv.

7.2.3 Eksempel på udfyldelse af en risikovurdering

Efterfølgende ses et eksempel på, hvordan en risikovurdering for sårbarheden *"Kajområdet"* og truslen *"Uautoriseret adgang"* kan se ud.

<table>
<tr><th colspan="2">RISIKOVURDERING</th></tr>
<tr><td>Nummer (jf. afsnit 7.1): 1</td><td>Dato: 1. januar 2025</td></tr>
<tr><td>Sårbarhed (jf. afsnit 6.2.1): Kajområdet</td><td>Trussel (jf. afsnit 6.2.1): Uautoriseret adgang</td></tr>
<tr><td>Konsekvens:
(Personer, økonomi, drift, miljø, anseelse)
1. Begrænset
2. Moderat
3. Alvorlig
4. Meget alvorlig
5. Kritisk

Sandsynlighed:
(Motivation, evne, kompleksitet, resurser)
I. Meget usandsynlig
II. Overvejende usandsynlig
III. Sandsynlig
IV. Overvejende sandsynlig
V. Meget sandsynlig</td><td> 
</td></tr>
<tr><td colspan="2">Risikoniveauet kan accepteres, hvis man havner i det grå eller grønne felt.

Hvis risikovurderingen viser, at risikoniveauet ikke kan accepteres (dvs. at man havner i gult, orange eller rødt felt i matrixen), skal der udpeges nye eller stærkere sikringstiltag.</td></tr>
<tr><td colspan="2">Eksisterende sikringstiltag: Kajområdet er indhegnet og der er kun adgang gennem porten. Porten står åben på hverdage mellem 07:00 – 16:00, men er låst i det øvrige tidsrum. Kajområdet overvåges af medarbejderne på havnefaciliteten på hverdage mellem 07:00 – 16:00. Hvis kajområdet forlades, aflåses porten.</td></tr>
<tr><td colspan="2">Forslag til yderligere sikringstiltag: Montering af kameraer med sensorer til overvågning i perioder, hvor kajområdet er ubemandet. Porten lukkes og der etableres adgangskontrol med kort/kode. Øvrig adgang kun kan ske efter henvendelse på havnekontoret. Med etablering af disse sikringstiltag nedbringes sandsynligheden til overvejende usandsynligt og krydset ender i det grønne område.</td></tr>
</table>

Konsekvensen vurderes som moderat (2) eller alvorlig (3), afhængig af om der er et skib ved kaj. Da der ikke laves en vurdering for kajområdet, når der ikke er et skib ved kaj, antager vi at konsekvensen er alvorlig (3).

Uautoriseret adgang til kajområdet anses som sandsynligt (III), da der indimellem sker bortvisning af personer, som ikke har et ærinde på kajområdet.

Risikovurderingen ender derfor i gul. Det betyder, at risikoniveauet ikke kan accepteres, og der skal evt. udpeges nye eller stærkere sikringstiltag.

I eksemplet er der først beskrevet de relevante eksisterende sikringstiltag. Herefter er der taget stilling til, hvilke nye eller stærkere sikringstiltag, som skal laves for at nedbringe risikoniveauet, så risikovurderingen ender i det grå eller grønne felt. Det vil sige, at risikoniveauet kan accepteres.

8 Konklusion og resume

Dette afsnit indeholder en konklusion samt et samlet resume af havnefacilitetssårbarhedsvurderingen.

Konklusion
I tekstfeltet skives en konklusion, som kort og præcist sammenfatter, hvad man har fundet ud af i havnefacilitetssårbarhedsvurderingen ud fra analysens fund og pointer. Det kan f.eks. være at man på baggrund af analysen kan konkludere, at de eksisterende sikringstiltag er tilstrækkelige, at det vil være nødvendigt at supplere de eksisterende sikringstiltag med en ny procedure eller supplerende uddannelse, eller at det har være nødvendigt at flytte den sikringsmæssige grænse i forhold til en tidligere PFSA. Udfaldsmulighederne er mange, men det er vigtigt, at konklusionen fastsættes ud fra analysens resultater i afsnit 5, 6 og 7. Konklusionen skal desuden hænge sammen med resumeet i det efterfølgende afsnit.

Hvis sårbarhedsvurderingen fører til, at faciliteten bør godkendes som en ON/OFF-facilitet, få en ESA eller en § 9-dispensation, skal denne konklusion klart begrundes i konklusionsafsnittet, jf. nærmere om undtagelsesformerne nedenfor.

Det er vigtigt, at man konkluderer i en konklusion. Det betyder f.eks., at man skal være opmærksom på, at man rent faktisk konkluderer, og ikke analyserer, eksemplificerer, stiller nye spørgsmål, diskuterer eller spekulerer osv. Derudover er det vigtigt, at man ikke introducerer ny viden i en konklusion.

Den gode konklusion er kendetegnende ved, at læseren blot behøver at læse de beskrivende afsnit og herefter konklusionen for at forstå hele analysen. Det er derfor vigtigt, at der er sammenhæng mellem de to afsnit.

Resume
Det samlede resume af havnefacilitetssårbarhedsvurderingen består af afsnit 8.1 samt 8.2. Resumeet skal minimum indeholde en beskrivelse af, hvordan vurderingen blev udført, samt en beskrivelse af hvert enkelt sårbarhedspunkt og sikringstiltag (modforanstaltning) som tages i anvendelse, jf. ISPS-kodes A-del pkt. 15.7.

8.1 Hvordan blev sårbarhedsvurderingen udført?

I dette afsnit beskrives hvordan og hvem som har udført sårbarhedsvurderingen.

8.2 Beskrivelse af sårbarhedspunkter og sikringstiltag

I skemaet indskrives de sårbarheder og sikringstiltag, som er blevet identificeret i risikovurderingerne i afsnit 7.

Sikringstiltagene gælder på sikringsniveau 1, altså normalsituationen. Forslagene baseres som nævnt på risikovurderingen, og kan indeholde alt fra proceduremæssige ændringer, uddannelse til fysiske sikringstiltag.

Der henvises i øvrigt til ISPS-kodens del A, pkt. 14.2 for en beskrivelse af de obligatoriske sikringsmæssige aktiviteter gældende for alle ISPS-faciliteter.

Beskrivelse af undtagelser

Hovedreglen er, at alle havnefaciliteter, som modtager skibe i international fart, skal udarbejde og implementere en sårbarhedsvurdering og en sikringsplan. Men de enkelte medlemsstater kan tillade at godkende ækvivalente sikringstiltag eller andre sikringstiltag med baggrund i en dispensation.

Hovedreglen om, at alle havnefaciliteter skal have en sikringsplan, kan for især små faciliteter med få skibsanløb være uforholdsmæssig i forhold til risikoen og dermed også uforholdsmæssigt bebyrdende. Derfor er der følgende muligheder for undtagelser, hvor havnefaciliteter kan opnå lempeligere vilkår.

ON/OFF havnefacilitet

Faciliteter med mindre end ca. 50 årlige anløb af ISPS-skibe kan ansøge om at få faciliteten godkendt som en ON/OFF-facilitet. Det betyder, at faciliteten skal opfylde alle kravene til en sikringsplan, men at den kan lade faciliteten være OFF, når der ikke er anløb af ISPS-skibe. Når faciliteten er OFF skal den ikke opfylde kravene til adgangskontrol, overvågning mv.

Grænsen for antal anløb er ikke fast, da det er vigtigt for TS at kunne udøve et vist skøn. Der har i Danmark hidtil været en praksis på maksimalt 50 årlige anløb af ISPS-skibe, og det vil være naturligt at betragte dette som en vejledende grænse. Derudover kan f.eks. facilitetens størrelse, kompleksitet og evt. sæsonrelateret operationer kunne indgå i betragtningen.

Der skal være en procedure i sikringsplanen, om hvordan faciliteten ændres fra OFF til ON tilstand. Det er i den forbindelse vigtigt, at der er en procedure for rensning af faciliteten forud for anløb af ISPS-skibe. EU-Kommissionen anbefaler, at rensning bør ske minimum 1 time før skibsanløb.

Hvis en facilitet er godkendt som en ON/OFF-facilitet, skal sikringstiltagene iværksættes på hele faciliteten, når sikringen aktiveres. Dette gælder også, selvom faciliteten desuden aktiverer et særligt adgangsbegrænset område på den del af faciliteten, hvor skibsanløb eller last befinder sig. I praksis skal der på faciliteter med et særligt adgangsbegrænset område dermed iværksættes adgangskontrol og overvågning for hele havnefaciliteten, når sikringen aktiveres. Afhængigt af PFSA og PFSP kan der desuden være krav om iværksættelse af yderligere sikring på det særligt adgangsbegrænsede område.

Når faciliteten er OFF, kan den modtage ikke ISPS-skibe uden restriktioner.

Det skal fremgå af forsiden, at der ansøges om godkendelse som ON/OFF-facilitet, og konklusionen i afsnit 8 skal indeholde en tydelig begrundelse herfor.

Ækvivalente sikringsarrangementer (ESA)

Havnefaciliteter med begrænsede eller specielle operationer, men med mere end lejlighedsvis trafik, kan på baggrund af en PFSA ansøge om at få tilladelse til at udarbejde et ækvivalent sikringsarrangement i stedet for en PFSP, jf. SOLAS XI-2 regel 12.2.

Baggrunden for at udarbejde ækvivalente sikringsarrangementer (ESA) er at give visse havnefaciliteter mulighed for at betjene ISPS-skibe, uden at de skal bære den fulde administrative, økonomiske og organisatoriske belastning, som for en fuldt implementeret ISPS-facilitet.

ISPS-koden beskriver et ækvivalent sikringsarrangement som: *"For visse specifikke havnefaciliteter med begrænsede eller specielle operationer, men med mere end lejlighedsvis trafik, kan det være hensigtsmæssigt at sikre overensstemmelse med sikringsforanstaltninger, der er ækvi-*

valente med dem, der er foreskrevet i kapitel XI-2 og i del A i denne kode. Dette kan navnlig være tilfældet for terminaler såsom dem, der er tilknyttet fabrikker eller kajpladser uden hyppige transaktioner." jf. ISPS-kodens del B, pkt. 4.27.

Hvad er begrænsede eller specielle operationer?

Selvom der står "*mere end lejlighedsvis trafik*" er det vigtigt at bemærke, at det ikke kun er anløbsfrekvensen der lægges vægt på, idet også typen af operationer vægtes.

Der skal altså tages udgangspunkt i, at havnefacilitetens drift eller operationer er begrænsede, men der kan også være tale om en begrænset periode – f.eks. sæsonrelateret. Med andre ord skal operationerne være enkle, simple eller periodeafgrænsede.

Grænsen for antal anløb er ikke fast. Det er vigtigt for TS at kunne udøve et vist skøn, men samtidig skal ESA ikke være en måde at omgå en fuld PFSP. Derfor vil 20 årlige anløb af ISPS-skibe være at betragte som en vejledende grænse.

Specielle operationer kan være anvendelse af faciliteten til andet end almindelig godshåndtering, f.eks. i forbindelse med anløb af tenderbåde fra krydstogtskibe, anlægs- eller ombygningsfasen af en havnefacilitet og kulturarrangementer eller lignende.

Ved anlægs- eller ombygningsfasen af en havnefacilitet vil antal anløb af ISPS-skibe typisk være højere end 20. Det vil her være den enkelte projektbeskrivelse som danner grundlag for den konkrete vurdering.

Krav til en ESA

Det fremgår af SOLAS XI-2 regel 12.2, at sikringstiltagene skal være mindst lige så effektive som i ISPS-kodens del A. Kommissionen har ved MARSEC Doc. 7608 anført, at en ESA som udgangspunkt skal opfylde ISPS-kodens del A, pkt. 14.2, og dermed kun gælder på sikringsniveau 1.

Sikringstiltagene skal være mindst lige så effektive som i ISPS-kodens del A. Det betyder, at de vejledninger, der nævnes i ISPS-kodens del B mht. sikringsforanstaltninger for en sikringsplan, og som vurderes relevante for faciliteten, skal medtages, f.eks. skal der være en vis form for uddannelse, træning og øvelser. Det betyder blandt andet, at PFSO og øvrigt sikringspersonale skal have modtaget undervisning og have den nødvendige viden. De skal være bevidste om deres ansvar og opgaver, som beskrevet i ESA'en tilsvarende kravet i en almindelig PFSP.

Øvelseskravet vil kunne variere i forhold til facilitetens anvendelse, men for at sikre en effektiv gennemførelse af havnefacilitetens ESA, skal der med jævne mellemrum gennemføres øvelser. For en facilitet, der er godkendt til 5-10 anløb af tenderbåde i en begrænset periode, kunne øvelseskravet f.eks. opfyldes ved, at der afholdes en stor øvelse før sæsonstart og en mindre øvelse i løbet af perioden.

En ESA er ikke underlagt de samme øvelses- og træningsregimer som en fuld sikringsplan

Det centrale er, at ordningen ikke må kompromittere sikringen på faciliteten, for skibet som anløber eller for andre havnefaciliteter som skibet anløber efterfølgende.

Det skal fremgå af forsiden samt konklusionen i afsnit 8, hvorfor faciliteten bør godkendes som en ESA.

En ESA skal som minimum opfylde følgende:

En ESA gælder kun på sikringsniveau 1

- ESA gælder kun for sikringsniveau 1.
- Havnefaciliteten må ikke anløbes af skibe, som er i sikringsniveau 2 eller 3.
- ESA skal være skriftlig.
- ESA skal beskrive de sikringstiltag, der anvendes for at imødegå punkterne i ISPS-kodens del A, pkt. 14.2.
- De beskrevne sikringstiltag skal være mindst lige så effektive, som hvis det havde drejet sig om en PFSP.
- Der skal være udpeget en PFSO samt en stedfortrædende PFSO.
- Havnefaciliteten skal være i stand til indføre sikringstiltagene hurtigt og effektivt ved anløb af ISPS-skib.
- Havnefaciliteten skal sikre, at den systematisk udfører en sikringsgennemgang f.eks. ved at gennemgå lokaliteterne (rensning) mv. førend den påbegynder ISPS-aktiviteter. Denne proces skal være nøje beskrevet i ESA'en som en integreret del af de foranstaltninger, der omfatter aktiviteterne i ESA'en.
- EU-Kommissionen anbefaler, at rensning sker minimum 1 time før skibsanløb.
- ESA skal omfatte sikringsprocedurer og foranstaltninger, som følges, når faciliteten betjener flere skibe, hvoraf nogle er underlagt forordningen og andre ikke er.
- Havnefaciliteten skal dokumentere, hvordan uddannelse, træning og afholdelse af øvelser gennemføres.
- TS skal godkende ESA på lige fod med PFSP.
- TS's forpligtelse mht. kommunikation (IMO/GISIS og til kommissionen) samt periodisk gennemgang af ESA er de samme som for en PFSP.
- Havnefaciliteten vil blive inspiceret på lige fod med andre faciliteter.

Bemærk, at der ikke kan udarbejdes en ESA for havnefaciliteter, som er dækket af en aftale indgået i henhold til SOLAS XI-2 regel 11 om alternative sikringsaftaler (ASA), jf. SOLAS XI-2 regel 12.2. En ASA er en bilateral aftale indgået mellem kyststater, som dækker korte faste internationale sejlruter mellem havnefaciliteter beliggende inden for deres respektive territorier.

Vær ligeledes opmærksom på, at hvis en havn indeholder flere havnefaciliteter, der betjener ISPS-skibe, influerer dette sandsynligvis på fastlæggelsen af havnens sikringsmæssige afgrænsning grundet tilstedeværelsen af elementer, der binder havnen sammen. Sådanne sammenbindende elementer kan f.eks. være fælles primær havneinfrastruktur, fælles vigtige havnetjenester eller fælles vandområder, jf. endvidere MARSEC dokument 5110 om Retningslinjer for fastlæggelsen af havnegrænser efter direktiv 2005/65/EF om bedre havnesikring samt afsnit 2.1 i PSA-vejledning om havnens sikringsmæssige afgrænsning.

Etablering af flere ESA'er i samme havn – uden at der samtidig er minimum én havnefacilitet med en PFSP - vil som hovedregel ikke kunne lade sig gøre, da der sandsynligvis vil forekomme sådanne sammenbindende elementer, der bevirker, at havnen vil skulle udarbejde en PSA og en PSP.

Derudover har Kommissionen i MARSEC Doc. 8708 (Interim Guidance on Maritime Security for Member States' Competent Authorities) samt MARSEC Doc. 7608 (Guidance on the use of Equivalent Security Arrangements (ESAs) for port facilities falling into the scope of Regulation (EC) 725/2004) lavet en vejledning om brug af ESA, som er tilgængelig for RSO'erne ved henvendelse til TS.

§ 9-dispensation

SOLAS XI-2 regel 2.2 og ISPS-kodens del A, pkt. 3.2 fastsætter, at de enkelte lande skal afgøre, i hvilken udstrækning ISPS-kodens del A skal anvendes på havnefaciliteter, der hovedsageligt betjener skibe i national fart, og som kun lejlighedsvis betjener skibe i international fart.

Bekendtgørelsens § 9 giver TS mulighed for at give dispensation for krav om udarbejdelse af en sikringsplan mod, at de sikringstiltag, der er beskrevet i sårbarhedsvurderingen (PFSA), implementeres ved hjælp af en DoS ved skibsanløb.

Idet der ikke udarbejdes en sikringsplan, og da den underliggende PFSA, som danner grundlag for udstedelse af DoS, udelukkende beskriver sikringstiltag på sikringsniveau 1, kan en havnefacilitet med en §-9 dispensation ikke anvendes på sikringsniveau 2 og 3.

Der kan ikke gives dispensation til havnefaciliteter som anløbes af passagerskibe.

Det er vigtigt, at PFSA'en detaljeret beskriver havnefacilitetens operationer, proceduremæssige fremgangsmåder og godstyper således, at styrelsen har et tilstrækkeligt oplyst grundlag til at træffe afgørelse om, hvorvidt der kan gives en §-9 dispensation.

Hvem kan søge om en § 9-dispensation?

En § 9-dispensation tildeles på baggrund af en PFSA og kan udelukkende tildeles en havn, som i øvrigt ikke har andre havnefaciliteter, og som har få anløb samt enkle og simple havneoperationer f.eks. sand, sten, salt, grus, korn. Grænsen for antal anløb er ikke fast, da det er vigtigt for TS at kunne udøve et vist skøn. Der har i Danmark hidtil været en praksis på maksimalt 5-10 årlige anløb af ISPS-skibe, og det vil være naturligt at betragte dette som en vejledende grænse. Selvom der er tale om meget få anløb er det vigtigt at bemærke, at det ikke kun er antallet af anløb der lægges vægt på, men også typen af operationer og liggetid.

Krav til en sikringserklæring (DoS)

Selvom havnefaciliteten har fået dispensation fra kravet om at udarbejde en sikringsplan, skal havnefaciliteten fortsat udføre sikringstiltag under skibsanløb. Der skal udarbejdes en DoS, mellem havnefacilitet og skib, som beskriver de sikringstiltag, som havnefaciliteten skal udføre under skibsanløbet. Der skal være en sammenhæng mellem indholdet i PFSA og de sikringstiltag, som er beskrevet i DoS'en.

En § 9-dispensation gælder kun på sikringsniveau 1

Udfyldt DoS vedlægges PFSA'en som et bilag.

Krav til en § 9-dispensation

Ved ansøgning om en § 9-dispensation vægtes følgende:

- Havnen har kun en havnefacilitet.
- Der kan ikke opnås dispensation for passagerskibe.
- Gælder kun for sikringsniveau 1.
- Havnefaciliteten må ikke anløbes af skibe, som er i sikringsniveau 2 eller 3.
- Der skal være udpeget en PFSO.
- Antallet af anløb
- Enkle og simple havneoperationer
- Liggetid

- Havnefaciliteten skal anvende DoS i forbindelse med anløb af ISPS-skib.
- En udfyldt DoS skal vedlægges PFSA.
- Dispensationen gives med vilkår.
- TS kan pålægge havnefaciliteten af indsende oversigt over skibsanløb.

Havnefaciliteter, der får en § 9-dispensation, bliver registreret i IMO/GISIS og får tildelt et IMO havnefacilitets nummer, men det vil fremgå, at faciliteten ikke er ISPS godkendt.

Beskrivelse af håndtering af større ændringer ved ombygning

Ved en større ændring forstås en ændring, der har **betydning** for havnefacilitetens sårbarhed, herunder større ændringer i havnefacilitetens fysiske struktur, organisation, eller hvis havnefaciliteten skal anvendes til andre formål end de, der er angivet i den godkendte sårbarhedsvurdering.

TS er opmærksom på, at havnefaciliteten og aktiviteterne ved havnefaciliteten løbende ændrer sig i ombygningsfasen.

Selve ombygningsfasen kan håndteres ved, at PFSA i planlægningsfasen af byggeriet gennemgås for at vurdere, hvorledes sikringstiltagene i PFSP løbende skal tilpasses for at tage højde for situationen i ombygningsfasen.

Ved større ændringer skal vurderingen af den gældende PFSA dokumenteres i et dokument udarbejdet af RSO og politiet og sendes til godkendelse hos TS. Herefter er en mulig løsning at udarbejde et bilag til PFSP, der beskriver sikringstiltagene, der iværksættes, når ombygningsarbejdet foregår, herunder når bygningsarbejderne er på stedet. En anden mulighed er udarbejdelse af en ESA, der gælder i ombygningsfasen.

PFSO skal løbende orientere TS om arbejdet for at sikre, at sikringstiltagene er tilstrækkelige.

Inden færdiggørelsen af byggeriet skal PFSA og PFSP godkendes på ny for at sikre, at tiltagene i PFSP er tilpasset den endelige udformning af havnefaciliteten.