VEILEDER FOR SIKRING

Veileder for sikring av bygg og infrastruktur i sykehusprosjekter

Rev. 1.2 26. oktober 2021

SYKEHUSBYGG

HELSE MIDT-NORGE HELSE VEST HELSE NORD HELSE SØR-ØST

Innholdsfortegnelse

Veileder for sikring av bygg og infrastruktur i sykehusprosjekter

Innholdsfortegnelse 1

Forord 3

Del 1. Sammendrag 5

Del 2. Hvorfor arbeide med sikring av bygg og infrastruktur for sykehus 11

2.1 Overordnede målsettinger med veilederen 14

2.2 Faglig avgrensning 14

2.3 Sikkerhetsloven 15

2.4 Sivilt beredskapssystem (SBS) 15

2.5 Grensesnitt mot andre deler av risikostyringen 15

2.6 Felles risikodefinisjon 16

Del 3. Sikring i sykehusprosjekter, steg for steg 19

3.1 Sikring i prosjektinnramming 19

3.2 Sikring i forbindelse med avklaring lokalisering 23

3.3 Sikring i konseptfasen, del 1 23

3.4 Sikring i konseptfasen, del 2 25

3.5 Sikring i forprosjekt 25

3.6 Sikring i detaljprosjekt og byggefase 27

3.7 Sikring i driftsfasen 29

Del 4. Metodebeskrivelser og verktøy 31

4.1 Helhetlig sikringsrisikovurdering (konseptfase, del 2/forprosjekt) 31

4.1.1 Etablere kontekst: Hva skal analyseres? 33

4.1.2 Identifisere risiko 38

4.1.3 Risikoanalyse 45
4.1.4 Risikoevaluering 50
4.1.5 Risikohåndtering 50
4.2 Innhold i en systembeskrivelse 50
4.3 Sjekkliste for sikring i prosjektinnramming 51
4.4 Arbeidsskjema for sammenlignende/komparativ risikovurdering (konseptfase, del 1) 54
4.5 Veiledning til ALARP-prinsippet 55
4.6 Innholdsfortegnelse for sikringskonsept 57
Del 5. Standard for grunnsikring i sykehus 59
5.1 Innledning 59
5.2 Bruk av dokumentet 61
5.3 Soneplan 61
5.4 Robusthetsmatrise 61
5.5 Grunnsikringskonsept for fysisk sikring 63
5.5.1 Soneinndeling 63
5.5.2 Områdesikring/perimetersikring 63
5.5.3 Krav til utvendige vegger, dører og vinduer 63
5.5.4 Krav til sikring av innvendige vegger, dører og vinduer 63
5.5.5 Elektroniske sikringsanlegg 63
5.5.6 Merking og skilting 64
5.5.7 Sikring av teknisk infrastruktur 64
5.5.8 Særlige sikringstiltak for utvalgte rom/områder 64
5.6 Grunnsikring – ansvarsmatrise prosjektering 64
Del 6. Vedlegg 67
Vedlegg A: Bakgrunn om risikobegrepet 67
Vedlegg B: Vold og trusler i helseinstitusjoner 71
Vedlegg C: Mer om generiske trusselscenarioer 75
Del 7. Litteraturliste 77

Forord

Dette prosjektet ble gitt til Sykehusbygg i Oppdragsdokument 2019.

Arbeidet startet opp 3. oktober 2018 og fem arbeidsmøter ble gjennomført med en ekspertgruppe fra RHF'ene fram til juni 2019.

Veilederen er ført i pennen av Jens Eirik Ramstad (sjef kvalitet, sikkerhet og samfunnsansvar i Sykehusbygg HF), Henrik Bjelland (PhD, seniorrådgiver systemsikkerhet og risikostyring i Multiconsult AS) og Stein Arne Meier (fagansvarlig sikkerhet i Sykehusbygg HF).

Fem arbeidsmøter med en ekspertgruppe oppnevnt av RHF'ene ble gjennomført. Vi takker medlemmene for et verdifullt bidrag.

Ketil Helgevold	Divisjonsdirektør	Stavanger universitetssykehus
Øystein Hoel	Leder stab brann, sikkerhet og beredskap	Nordlandssykehuset
Gry Strand	Sikkerhetssjef	Oslo Universitetssykehus
Mats Hobber	Sjef allmenteknisk avdeling	St.Olavs Hospital
Erlend Vandvik	Beredskapssjef	St.Olavs Hospital
Sigmund Stikbakke	Prosjektleder eiendomsforvaltning	Helse Sør-Øst

Styringsgruppen har bestått av:

Sigmund Stikbakke	Prosjektleder eiendomsforvaltning	Helse Sør-Øst
Lars Magnussen	Eiendomssjef	Helse Midt-Norge
Kjell-Einar Bjørklund	Bygg- og eiendomssjef	Helse Vest
Lars Alvar Mickelsen	Seksjonsleder drift og eiendom	Helse Nord

Ambisjonen er at Veilederen blir gjort gjeldende for alle større sykehusprosjekter.
Veilederen er godkjent i interregionalt AD-møte 25. oktober 2021

Trondheim 26. oktober 2021

Terje Bygland Nikolaisen
Prosjektansvarlig/Adm.dir

Jens Eirik Ramstad
Prosjektleder/Sjef kvalitet sikkerhet samfunnsansvar

Del 1. Sammendrag

Denne veilederen skal benyttes i alle sykehusprosjekter, store og små, og ved sikkerhetsoppgradering i eksisterende bygg og anlegg. Den skal sikre at lovpålagte og vesentlige sikkerhetsaspekter ivaretas på en systematisk måte. Videre skal veilederen bidra til å standardisere arbeidsprosesser, krav og løsninger som skal gi mer sikkerhet for pengene.

Veilederen er avgrenset til sikring mot **fysiske tilsiktede hendelser**, som kan føre til skade og tap på de verdiene som finnes på sykehus. Veilederen er et hjelpemiddel for å planlegge, prosjektere og bygge inn sikkerhet mot fysiske trusler i bygg og infrastruktur.

Sikring mot digitale angrep på eller via IKT-systemer («cybersecurity») er ikke omfattet av veilederen, men metodikken kan likevel være relevant også for dette temaet.

Fysiske angrep på informasjon eller informasjonssystemer omfattes av veilederen. Veilederen spesifiserer også krav til utarbeidelse av en informasjonssikkerhetsplan i prosjektets tidligfase.
Dette gjøres bl.a. for å unngå at beskyttelsesverdig informasjon om fysiskes sikringstiltak kommer på avveie i løpet av byggeprosjektet.

Veilederen består av fem deler som hver kan leses separat:

Del 1: Sammendrag

Del 2: Bakgrunn: hvorfor arbeide med sikring i sykehusprosjekter (HVORFOR)

Del 3: DEL 3: Sikring i sykehusprosjekter, steg for steg (HVA)

Del 4: Metodebeskrivelser og verktøy (HVORDAN)

Del 5: Standard for grunnsikring i sykehus

En kort beskrivelse av del 2 til 5 følger nedenfor.

Del 2 i Veilederen gir en nærmere beskrivelse av HVORFOR man bør styrke arbeidet med fysisk sikring av sykehus.

Helsesektoren er en utsatt sektor med hensyn til vold og trusler mot ansatte. Ved Stavanger Universitetssykehus er det for eksempel registrert i snitt ca. 1 200 hendelser pr år innenfor kategoriene trusler og vold i perioden 2014-2018. Dette er også en internasjonalt utfordring, som også beskrives som økende.

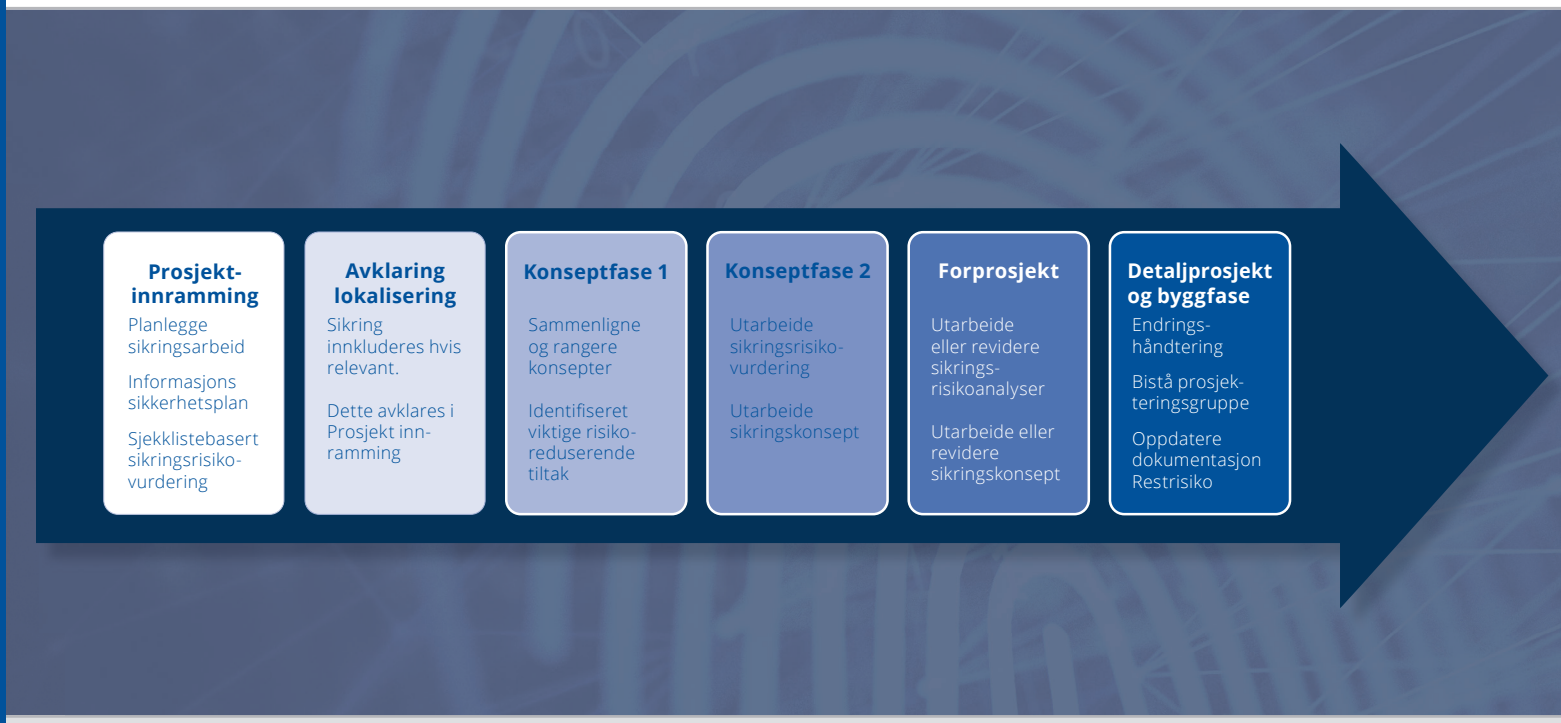
1

Etter 22. juli-hendelsen må man innse at viktige samfunnsfunksjoner, slik som sykehus, også kan bli gjenstand for angrep. Digitale angrep (f.eks. cyberangrep) kan også være et virkemiddel, hvor spesielt tap av integritet i pasientdata kan få alvorlige konsekvenser. Denne veilederen omfatter for øvrig ikke scenarioer knyttet til digitale angrep, men har fokus på fysiske angrep.

Etter 22. juli-hendelsen må man innse at viktige samfunnsfunksjoner, slik som sykehus, også kan bli gjenstand for angrep.

Del 3 i Veilederen beskriver HVA som anbefales gjennomført i planlegging og prosjektering (vurderinger og analyser), se figur 1 nedenfor. Hovedbudskapet er at forhold knyttet til fysisk sikkerhet må vurderes i tidlig fase, og at dette inngår i beslutningsgrunnlaget når eier skal bestemme lokalisering og velge konsept. Etter at konsept er valgt gjøres det en sikringsrisikovurdering for å vurdere hva som sikkerhetsmessig er

Bilde 1 Overskrifter fra norske nettaviser, som illustrerer noe av utfordringen denne veilederen kan bidra til økt risikobevissthet og bedre løsninger.



Figur 1. Prosjektfaser og arbeid med sikring.

«godt nok» med gitt lokalisering og funksjoner sykehuset skal romme. Dette foregår i forprosjekteringen og ender opp i tekniske beskrivelser som blir en del av anbudsgrunnlaget. Det anbefales at dette arbeidet gjennomføres i nært samarbeid med sykehusets egen sikkerhetsavdeling. Veilederen kan også brukes for å håndtere bygningsmessige endringer i driftsfasen.

Ved mindre endringer kan en komparativ sårbarhetsanalyse (jf. kap. 4.4) være tilstrekkelig, mens ved større endringer må det tas hensyn til at trusselbilde, verdier, etc. endres og en helhetlig sikringsrisikovurdering (jf. kap. 4.1) må gjennomføres.

Del 4 beskriver HVORDAN analysearbeidet skal gjennomføres i prosjektets ulike faser. Denne delen er skrevet for fagpersonell som skal gjennomføre analysene, i sykehusets sikkerhetsavdeling, hos byggherren/prosjektledelsen eller i prosjekteringsgruppen.
Det krever en viss forståelse for sikkerhetsfaget generelt og risikoanalyse/risikostyring spesielt (NS 5814, NS 5830-serien, herunder NS 5834 og ISO 31000) for å få fullt utbytte av denne delen av veilederen. Kjernen i del 4 er anbefalt metode for en **sikringsrisikovurdering** og oppdatering/detaljeringen av denne.

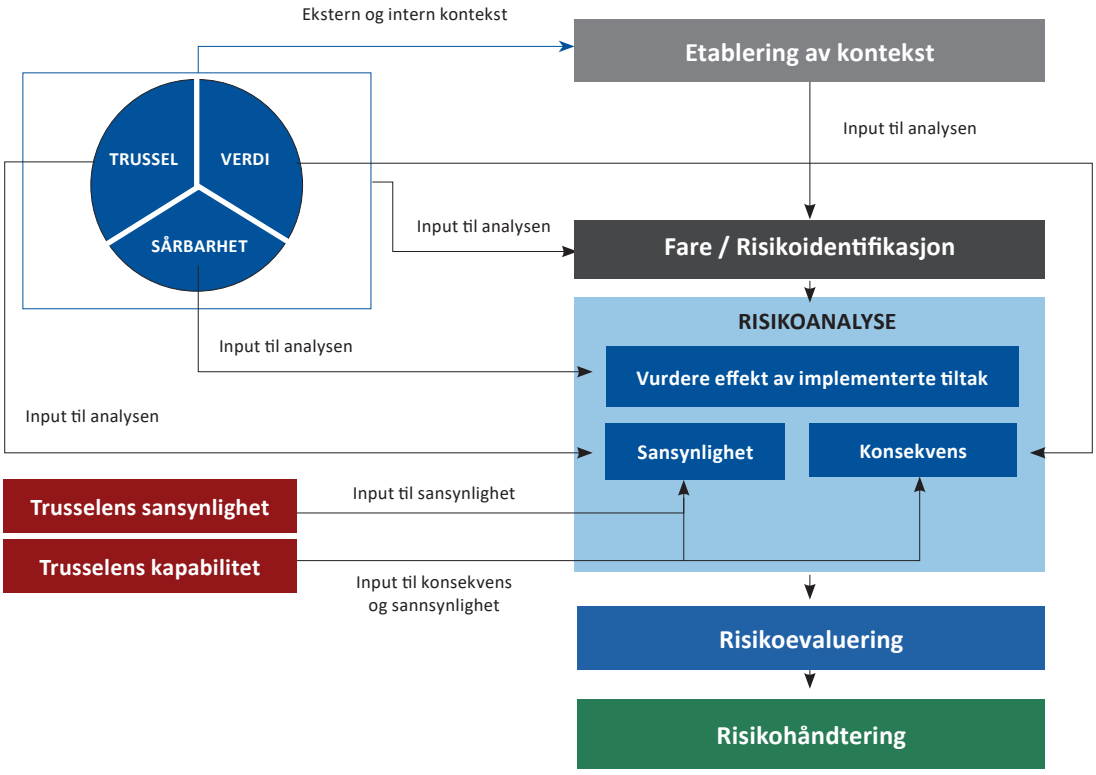
Verktøy og analysesteg er beskrevet i detalj, fra relativt enkle vurderinger i tidlig fase til den mer detaljerte sikringsrisikovurderingen som utarbeides i forprosjekteringsfasen. Oppfølgingen av sikringsrisikovurderingen vil utgjøre en viktig del av **byggherrens risikostyring.**

Figur 2 skisserer arbeidsprosessen, fra etablering av kontekst (dvs. avklare omfang og systemgrenser) til oppfølging av kartlagt risiko og vedtatte risikoreduserende tiltak. Den tar utgangspunkt i en tradisjonell risikovurdering, men stiller krav om at verdier, sårbarhet og trusler skal være en viktig del av i risikovurderingen.

Del 5 definerer hva som menes med et GRUNNSIKRINGSKONSEPT, altså hva RHF'ene og Sykehusbygg anser som et minimum av sikkerhet som skal bygges inn i nybygg og rehabiliteringsprosjekter. Sikringsrisikovurderingen vil avklare behovet for ytterligere sikringstiltak eller eventuelt en reduksjon av sikringstiltak.

Grunnsikringskonseptet inneholder også en beskrivelse av viktige verktøy innen prosjektering av robusthet og sikkerhet som soneplan og robusthetsmatrise, i tillegg til å spesifisere krav til arkitektoniske, fysiske og elektroniske sikringstiltak.

PROSJEKTFASER OG ARBEID MED SIKRING



Figur 2. Analyse av verdier, trusler og sårbarheter som grunnlag for risikovurderingen.

Del 2. Hvorfor arbeide med sikring av bygg og infrastruktur for sykehus

På et sykehus vil fysiske og organisatoriske sikringstiltak være sentrale i sikkerhetsstyringen. En viktig forutsetning for at menneskelige og organisatoriske tiltak skal fungere er at bygningsmessige utforming og sikringstiltak gir trygghet for at de ulike situasjonene kan håndteres på en god måte.

Dette gjelder først og fremst for de «daglige truslene». Samtidig kan det ikke utelukkes at alvorlige sabotasje- og terrorhandlinger vil kunne ramme norske sykehus i framtiden. Derfor er det viktig å ha en helhetlig og systematisk tilnærming til arbeidet med sikring mot tilsiktede handlinger gjennom alle faser av et sykehusprosjekt.
- Men hva er det sykehusene skal sikres mot?

Vold og trusler mot mennesker: pasienter, pårørende/besøkende og ansatte

Helsesektoren er en utsatt sektor med hensyn til vold og trusler mot ansatte (Wedervang-Resel m.fl. 2017; Hagen, 2019). Ved Stavanger Universitetssykehus er det for eksempel registrert i snitt ca. 1 200 hendelser pr år innenfor kategoriene trusler og vold i perioden 2014-2018 (Heie, 2019). Dette er også et internasjonalt problem, som også beskrives som økende. Trusler og vold er en kjent utfordring i psykiatri/rus-institusjoner, men vi ser at førstelinjetjenester, som akuttmottak for somatikken og legevakter, er utsatt. Enkelte avdelinger innen somatikken er også utsatt. Et eget kapittel (kap. 7) om trusler og vold i helsesektoren er tatt med i veilederen for å beskrive noe av det kunnskapsgrunnlaget som finnes.. Pasientens pårørende kan også være en volds- og trusselrisiko. Dette kan også ha sammenheng med situasjonen pasienten befinner seg i, og forekomme som en konsekvens av at pårørende ønsker pasientens beste. I praksis betyr dette at sikring av sykehus ikke i hovedsak kan basere seg på vanlige sikringsprinsipper som å etablere avstand og barrierer mellom trusler og verdier. For å ivareta samfunnsoppdraget, må sykehusets ansatte være tett på både pasienter og pårørende. Forebygging av volds- og trusselsituasjoner må de ansatte ha opplæring i, og det må finnes gode beredskapstiltak som bidrar til å redusere konsekvensene av uønskede situasjoner som oppstår.

Vi må sikre mot vold og trusler mot mennesker: pasienter, pårørende/besøkende og ansatte

Arbeidsmiljøloven (ASD, 2005) skal blant annet sikre et arbeidsmiljø som gir grunnlag for en helsefremmende og meningsfylt arbeidssituasjon, og gi full trygghet mot fysiske og psykiske skadevirkninger (§ 1–1). Regelverket krever at arbeidstaker skal, så langt det er mulig, beskyttes mot vold, trusler og uheldige belastninger som følge av kontakt med andre (§ 4–3).

Selv om det finnes mye kunnskap om trusler og vold, inkludert årsaker

og konsekvenser, er det generelt begrenset kunnskap om sammenhengen mellom trusler og vold og bygningsmessige forhold. For å kompensere for dette er det viktig at den tilgjengelige litteraturen som faktisk finnes nyttiggjøres, men også at ansatt-/brukerperspektivet får en plass i vurderinger av risiko for trusler og vold, samt i vurderinger av hvilke risikoreduserende bygningsmessige tiltak som skal anvendes.

Denne veilederen har som mål at ny kunnskap om forholdet mellom god design og risiko for vold og trusler spiller en rolle ved planlegging av nye og i driften av eksisterende sykehus. Risikovurderingene vil være en arena hvor denne typen kunnskap etterspørres. Gjennom økt etterspørsel etter kunnskap, er det også et håp at ny kunnskap utvikles gjennom målrettet forskningsarbeid. For å løse de reelle og store utfordringene sektoren opplever med dette, er det først og fremst behov for mer kunnskap om tiltak som kan forebygge at volds- og trusselsituasjoner oppstår.

Tap av operativ evne

I tillegg til risiko forbundet med volds- og trusselhendelser mot ansatte, er det også risiko knyttet til sykehuset som kritisk infrastruktur i samfunnet og som utvikler, bruker og forvalter av sensitiv informasjon, f.eks. pasientdata og forskningsresultater. Her er det større usikkerhet knyttet til hvilke trusselaktører man skal sikre seg mot, men tidligere hendelser viser at utfordringen er relevant og må håndteres.

I januar 2018 ble for eksempel Helse Sør-Øst rammet av et omfattende avansert og målrettet dataangrep (se for eksempel: Sykehuspartner, 2018). I mars 2019 ble Hydro utsatt for et omfattende dataangrep som påførte virksomheten et tap på ca. en halv milliard kroner (HelseCERT, ikke datert). Tidligere hendelser viser at norske virksomheter er utsatt for dataangrep og cybertrusler, og understreker viktigheten av å arbeide systematisk med sikring av informasjon og IKT-systemer.

Denne veilederen omfatter ikke vurdering av risiko eller tiltak mot digitale angrep på eller via IKT-systemer (cybertrusler). Samtidig må denne trusselen sees i sammenheng med fysisk sikring. Sykehusprosjektene må jobbe systematisk med informasjonssikkerhet fra prosjektinnrammingsfasen, og sørge for at det lages en informasjonssikkerhetsplan for prosjektet. Kompromittering av beskyttelsesverdig informasjon kan få konsekvenser for operativ evne senere, ved at en trusselaktør enklere kan angripe sårbare punkter.

Sabotasje- og terrortrusselen mot sykehus er ikke knyttet opp mot en gitt trusselaktør eller angrepsmetode. Sykehus har en egenverdi som kan rammes fysisk. Dette kan være angrep på mennesker som befinner seg på sykehuset, for eksempel gjennom væpnede aksjoner, bombeangrep, sabotere vannforsyning, angrep med farlig stoff m.m.
Cyberangrep kan også være et virkemiddel, hvor spesielt tap av integritet i pasientdata kan få katastrofale konsekvenser.
I tillegg til sykehusets egenverdi, har sykehus en instrumentell verdi. Dette betyr at sykehuset understøtter andre viktige funksjoner i samfunnet. Sabotasje og terror rettet mot sykehuset kan dermed være et virkemiddel for å oppnå effekter andre steder i samfunnet.

Sabotasje- og terrortrusselen mot sykehus er ikke knyttet opp mot en gitt trusselaktør eller angrepsmetode.

Tap av omdømme

Tillit er en viktig ressurs for et sykehus og helsesektoren generelt. I denne veilederen er derfor omdømme tatt med som en verdikategori som skal vurderes i en sikringsrisikovurdering.

2.1 Overordnede målsettinger med veilederen

Veilederen er utarbeidet som et hjelpemiddel for å arbeide systematisk med sikring av bygg og infrastruktur mot tilsiktede/ondsinnede uønskede handlinger i alle fasene av sykehusprosjekter og eksisterende bygninger. Dette omfatter å sørge for at tilsiktede handlinger blir en like naturlig del av risikostyrings- og designprosessen som utilsiktede hendelser, for eksempel brann, flom, ras og ekstremvind. Veilederen skal bidra til bevisstgjøring og at det tas risikoinformerte valg når sykehus bygges og/eller bygges om.

Veilederen skal bidra til at sikringsfaget integreres i planleggings- og prosjekteringsprosesser. På denne måten kan spørsmål om sikring behandles til riktig tid. Samtidig vil det muliggjøre nødvendige avklaringer mot andre fag og motstridene funksjonskrav. Et eksempel på dette kan være at krav som stilles til rømning ved brann, kan skape utfordringer knyttet til sikring av sykehuset mot tilsiktede handlinger.

Ikke alle norske sykehus skal dimensjoneres for å motstå forskjellige terrorscenarioer. Det er likevel hensiktsmessig å analysere muligheten for slike scenarioer, og gjøre et bevisst valg basert på analysen. Risikovurderingene skal være relevante, være et hensiktsmessig beslutningsunderlag og bidra til framdrift i sykehusprosjektet.

2.2 Faglig avgrensning

Veilederen er avgrenset til temaet sikring av sykehusets verdier mot fysiske trusler og angrep. Hovedfokus vil være på identifikasjon og beskrivelse av fysiske og elektroniske sikringstiltak rettet mot bygg og infrastruktur, men utelukker heller ikke organisatoriske/administrative tiltak.

Det er sykehusets mennesker, kontinuerlige drift (operativ evne) og omdømme som skal sikres, og som defineres som sykehusets verdier på et overordnet nivå. Selv om veilederen er rettet mot fysisk og elektronisk sikkerhet, vil mennesker, informasjon og informasjonssystemer være sentrale verdier/innsatsfaktorer som må behandles i risikovurderingene. Veilederen gir føringer for hvordan bygg og infrastruktur skal planlegges, prosjekteres og bygges for å sikre disse verdiene.

Veilederen spesifiserer krav til utarbeidelse av informasjonssikkerhetsplan i prosjektets tidligfase. Dette gjøres bl.a. for å unngå at beskyttelsesverdig informasjon om fysiske og elektroniske sikringstiltak kommer på avveie i løpet av prosjektet. Veilederen går ikke inn på hvordan prosjekter konkret skal arbeide med informasjonssikkerhet (prosjektsikkerhetsadministrasjon), personellsikkerhet (autorisasjon, sikkerhetsklarering m.v.), eller sikkerhet mot digitale trusler (cybersikkerhet) i sykehusets datanettverk. Den omfatter imidlertid fysiske angrep mot digitale systemer.

2.3 Sikkerhetsloven

Ny lov om nasjonal sikkerhet (sikkerhetsloven) trådte i kraft 1. januar 2019 (JBD, 2019). Behovet for ny sikkerhetslov begrunnes spesielt i teknologiutvikling og globalisering der strukturer er avhengig av hverandre. Lovens formål er å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Det forutsettes at virksomheter som er omfattet av loven må ta et større ansvar for å redusere sin sårbarhet og sikre seg mot angrep som kan skade nasjonale sikkerhetsinteresser. Som tidligere lov, gjelder ny lov hele helse- og omsorgsforvaltningen og helseforetakene. Loven er en fredstidslov og gjelder statlige, fylkeskommunale og kommunale organer, samt leverandører av varer og tjenester i forbindelse med en sikkerhetsgradert anskaffelse.
Sikkerhetsloven skal beskytte nasjonale sikkerhetsinteresser. Disse er i § 1-5 definert som: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser, bl.a. knyttet til samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.

Sikkerhetsloven definerer begrepet grunnleggende nasjonale funksjoner (GNF). Dette er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser. Aktører som av ulike årsaker ønsker å ramme norske sikkerhetsinteresser, vil kunne ha interesse av å forsøke å sette objekter, informasjonssystemer og infrastruktur ut av spill, enten ved å skade, ødelegge eller overta kontrollen over funksjonene disse utgjør. Enkelte objekter, informasjonssystemer og infrastrukturer vil derfor kunne være av en slik betydning for GNF at de klassifiseres som skjermingsverdige.

Det er Helse- og omsorgsdepartementet som skal peke ut og klassifisere skjermingsverdige verdier i sektoren. Det er det regionale helseforetaket som, på grunnlag av verdi- og skadevurderinger av den samlede virksomhet, foreslår potensielle skjermingsverdige verdier. Når departementet har fattet vedtak om eventuelle skjermingsverdige verdier skal ansvarlig virksomhet vurdere risiko og hvilke tiltak som skal iverksettes for å håndtere risikoen. Det er det regionale helseforetakets ansvar å avklare hvorvidt sykehusprosjekter omfatter skjermingsverdige verdier og informere de aktuelle prosjektene om dette.
Selv om spesialisthelsetjenesten i sum kan sies å understøtte en GNF, vurderer de regionale helseforetakene at det ikke er tilfelle for enkelt-helseforetak/-sykehus. Anbefalingen til Helse- og omsorgsdepartementet per nå er at sykehusenes funksjoner ikke er skjermingsverdige.
Selv om verdiene prosjektet omfatter vurderes å være utenfor sikkerhetslovens område er det likevel viktig at objekter, informasjonssystemer og infrastruktur risikovurderes og sikres på bakgrunn av andre hensyn.
Denne veilederen omfatter metodikk for sikringsrisikovurdering som kan benyttes uavhengig av om prosjektet omfattes av sikkerhetsloven eller ikke.

2.4 Sivilt beredskapssystem (SBS)

Sykehus er en del av virksomhetene som omfattes av Sivilt Beredskapssystem (SBS) (JBD, 2015). Virkeområdet for SBS er sektorovergripende kriser i fredstid forårsaket av alvorlige tilsiktede hendelser eller trusler om slike, kriser med sikkerhetspolitisk dimensjon og væpnet konflikt eller trusler om slike.

Ved iverksetting av tiltak fra nasjonalt nivå vil Helse- og omsorgsdepartementet videreformidle beslutning på graderte kommunikasjonskanaler.
En del av SBS omhandler forsterket egenbeskyttelse mot sikkerhetstruende virksomhet. Dette kapitlet i SBS er et lavterskel-verktøy for å heve sikkerhetsnivået i den enkelte virksomhet ved hjelp av en del forhåndsdefinerte tiltak når trusselbildet tilsier dette.

SBS opererer med fire beredskapstrinn: Alfa, Bravo, Charlie og Delta, som avhenger av det nasjonale trusselnivået. For sykehusene er det viktig å kunne trappe opp beredskapen med relevante påbyggingstiltak (utover grunnsikringen) i samsvar med gjeldende trusselnivå.
SBS spesifiserer anbefalte tiltak og føringer for hva sykehuset skal gjøre i en beredskapssituasjon.

De fleste tiltakene og føringene er knyttet til økt kontroll med egne områder, bygningsmasse og infrastruktur, samt kontroll med eksterne (besøkende, leverandører osv.). For lettere å kunne følge opp de ulike beredskapstrinnene på en effektiv måte, vil det være nyttig at sykehuset er tilrettelagt for dette i lokaliseringsarbeidet, planleggings- og byggefasen. Eksempler på tiltak som forutsetter planlegging og tilrettelegging tidlig er muligheten for å iverksette kontroll av kjøretøyer og besøkende til virksomhetens område, muligheten for å kontrollere all adgang til virksomhetens område og mulighet for å sette opp fysiske avsperringer på egen grunn for å forhindre tilkomst av kjøretøy.
Når det gjennomføres en sikringsrisikovurdering i samsvar med denne veilederen må det tenkes på at beredskapen skal kunne trappes opp i situasjoner med høyere beredskap. Beslutninger om lokalisering, tomtevalg, plassering på tomt, atkomstveier, innganger, bygningsmasse m.m. må ikke tas uten å vurdere mulighetene for å trappe opp beredskapen i samsvar med SBS.

2.5 Grensesnitt mot andre deler av risikostyringen

Risikostyring i sykehusprosjekter omfatter flere temaer, for eksempel brannsikkerhet, driftssikkerhet for teknisk infrastruktur, reguleringsrisiko, smittevern m.v. Risiko- og sårbarhetsanalyser (ROS-analyser) er et verktøy som brukes til å analysere utilsiktede uønskede hendelser, og generelt et kjent verktøy for

Et trusselscenario er en tenkt uønsket hendelse som kan oppstå som følge av tilsiktede handlinger på sykehuset.

risikovurderinger i Bygg-, Anlegg- og Eiendomssektoren (BAE).

I ROS-analysene som gjennomføres i et sykehusprosjekt er uønskede hendelser utgangspunktet for analysen. Eksempler på uønskede hendelser kan være «driftsstans som følge av strømbrudd», «oversvømmelse av atkomst-/utrykningsveier» eller «brann på sengeavdeling». Tilsiktede handlinger kan gjerne kan være årsaker til disse hendelsene. Temaet tilsiktede uønskede handlinger er derfor naturlig å diskutere i flere risikovurderinger som gjennomføres i et sykehusprosjekt. Det er viktig at relevante funn fra andre ROS-analyser nyttiggjøres i risikovurderingen for tilsiktede handlinger og motsatt.

De ulike risikovurderingene vil være underlag for hverandre. Funn fra alle risikovurderingene bør samles i ett felles risikoregister for sykehusprosjektet. I et helhetlig risikostyringsperspektiv vil dette være gunstig både med hensyn til prioritering av prosjektets begrensede ressurser og for å forenkle oppfølgingen ved at «alt er på ett sted».

2.6 Felles risikodefinisjon

Forutsetningen for å samle funn fra flere risikovurderinger i et felles risikoregister er at risikobildet i de ulike vurderingene presenteres på samme format. Risikovurderinger av tilsiktede uønskede handlinger har, ved publiseringen av NS 5830-serien, vært forbundet med «trefaktormodellen», hvor risiko er en funksjon av de tre faktorene verdier, trusler og sårbarhet (SN 2012; 2014). Vanlige ROS-analyser kjennetegnes ved at risiko er en kombinasjon av uønskede hendelsers sannsynlighet og konsekvenser (SN, 2008).

En viktig motivasjon for «trefaktormodellen» i NS 5830-serien er at den utelukker sannsynlighetsbegrepet i risikovurderingen. Nyere studier, hvor de aktuelle metodene og risikodefinisjonene sammenlignes, viser at sannsynlighetsbegrepet har en plass i risikovurderingen, uavhengig av hvilken metode som benyttes (FFI, 2015; FFI 2017). I ROS-analysene uttrykkes sannsynligheten eksplisitt, mens i trefaktormodellen brukes sannsynlighetsaspektet implisitt for eksempel når scenarioer inkluderes eller utelates fra analysen, eller når det settes sikringsmål.

Risikovurderinger står også sentralt i Sikkerhetsloven, som kom i oppdatert versjon i 2019, jf. kap. 2.3. Krav til virksomheters risikovurderinger av skjermingsverdige verdier gis i Virksomhetssikkerhetsforskriften § 12 (FD, 2019). Her følger det at virksomheten bl.a. skal ta hensyn til sannsynligheten for at sikkerhetstruende virksomhet kan inntreffe.

Usikkerhetsdimensjonen, uttrykt for eksempel gjennom sannsynligheter, er en sentral del av risikobegrepet. I denne veilederen legges det derfor til grunn at risiko er den todimensjonale kombinasjonen av konsekvenser og tilhørende usikkerhet (Aven, 2007; 2010). Usikkerhet kan her uttrykkes med bruk av sannsynligheter, men er ikke utelukket til det. Det vil også finnes usikkerhet i bakgrunnskunnskapen som analysen bygger på, som må uttrykkes kvalitativt.

Veilederen har for øvrig en sterk knytning til begrepene verdier, trusler og sårbarheter, og utelukker heller ikke bruk av f.eks. NS 5832 eller Helse Sør-Øst sin Veileder for sikringsrisikoanalyse i sykehusprosjekter (HSØ, udatert) der dette vurderes som hensiktsmessig.
Se Vedlegg A (kap. 6) for en mer omfattende redegjørelse om risikobegrepet.

2.7 Sentrale begrep/definisjoner

Sentrale begreper som er benyttet i denne veilederen er forklart nedenfor

Begrep	Definisjon
Analyseobjekt	Se forklaring under «systembeskrivelse».
Kritisk infrastruktur	Tjenester/systemer sykehuset er avhengig av for å kunne drifte forsvarlig. Hvilke systemer dette gjelder er individuelt og avhengig av hvilke funksjoner sykehuset har, samt redundans på systemene. Det vil være en viktig hensikt med risikoanalysen å identifisere hvilke systemer dette gjelder.
Fare	«Handling eller forhold som kan føre til en uønsket hendelse» (NS 5814:2008).
Intensjon	Refererer til en trusselaktørs «vilje og hensikt til å utføre en handling» (NS 5830:2012).
Kapasitet	Refererer til en trusselaktørs «evne, herunder ressurser, kunnskap og ferdighet, til å utføre en handling» (NS 5830:2012).
Konsekvens	«Mulig følge av en uønsket hendelse» (NS 5814:2008). En konsekvens knyttes til noe som er av verdi. I denne veilederen benyttes de tre verdikategoriene Liv og Helse, Operativ evne og Omdømme.
Risiko	I denne veilederen omtalles risiko som kombinasjonen av konsekvenser av trusselscenarioer med tilhørende usikkerheter. Risiko uttrykkes gjennom trusselscenarioer, sårbarheter, konsekvenser, trusselnivå (sannsynlighet) og usikkerhet.
Sannsynlighet	Grad av tro knyttet til om en uønsket hendelse, handling eller spesifiserte konsekvenser vil kunne inntreffe. I en risikoanalyse kan sannsynlighet uttrykkes på flere måter, f.eks. som et tall mellom 0 og 1 eller på en skala fra lav til høy.
Sikkerhet	Sikkerhet er en tilstand et system kan være i, hvor systemet evner å unngå skader og tap. Et sykehus er i en tilstand av sikkerhet (sikker tilstand) dersom det evner å unngå skader og tap under uvanlige tenkelige påkjenninger.
Trygghet	Pasienter, pårørende og ansattes opplevelse av at situasjonen er sikker. Merk at mennesker kan oppleve trygghet uten at systemet er i en sikker tilstand. Det er også mulig at mennesker opplever utrygghet i et system som er i en sikker tilstand. Et sykehus med høy grad av sikringspreg kan for eksempel oppleves mer utrygt enn et sykehus med lavere sikringspreg selv om sikkerhetsnivået objektivt sett er høyere ved det første sykehuset.

Begrep	Definisjon
Sikring	Bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger» (NS 5830:2012). Sikring kobles gjerne mot det engelske uttrykket «security» og kontrasteres gjerne mot det engelske uttrykket «safety».
Systembeskrivelse	En helhetlig beskrivelse av systemet som er gjenstand for en risikovurdering. Systemet omfatter geografiske, tekniske og organisatoriske avgrensninger, samt interne og eksterne avhengigheter/grensesnitt. I denne konteksten vil systemet omfatte sykehuset med tilhørende delsystemer. Systembeskrivelsen inkluderer en tydelig avgrensning mot systemets omgivelser. I andre sammenhenger brukes begrepet «analyseobjekt» (NS 5814:2008) med samme innhold. Vi bruker begrepet analyseobjekt for å skille mellom systemet som helhet og en konkret del av systemet som er gjenstand for analyse. Begrepet «delsystem» blir synonymt med analyseobjekt i denne sammenheng.
Sårbarhet	Manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning» (NS 5830:2012).
Trusselscenario	Tenkelig uønsket hendelse som kan oppstå som følge av tilsiktede handlinger på sykehuset.
Uønsket hendelse	«Hendelse som kan medføre tap av verdier» (NS 5814:2008). Uønskede hendelser oppstår ved at farer materialiserer seg, og har konsekvenser. Uønskede hendelser er derfor et naturlig startpunkt for å kartlegge et risikobilde, hvor man har anledning til å analysere forhold som leder til hendelsen, og konsekvensene som kan følge av hendelsen.
Verdi	NS 5830 definerer en verdi som «ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar nytte av ressursen». Verdier er et skalerbart konsept. Vi kan snakke om overordnede samfunnsverdier, eksempelvis nasjonale sikkerhetsinteresser, liv og helse og miljø. Vi kan også snakke om objekter, gjenstander, informasjon osv som verdier. I andre sammenhenger kan dette omtales som innsatsfaktorer som er nødvendige for å ivareta overordnede samfunnsverdier.

Del 3. Sikring i sykehusprosjekter, steg for steg

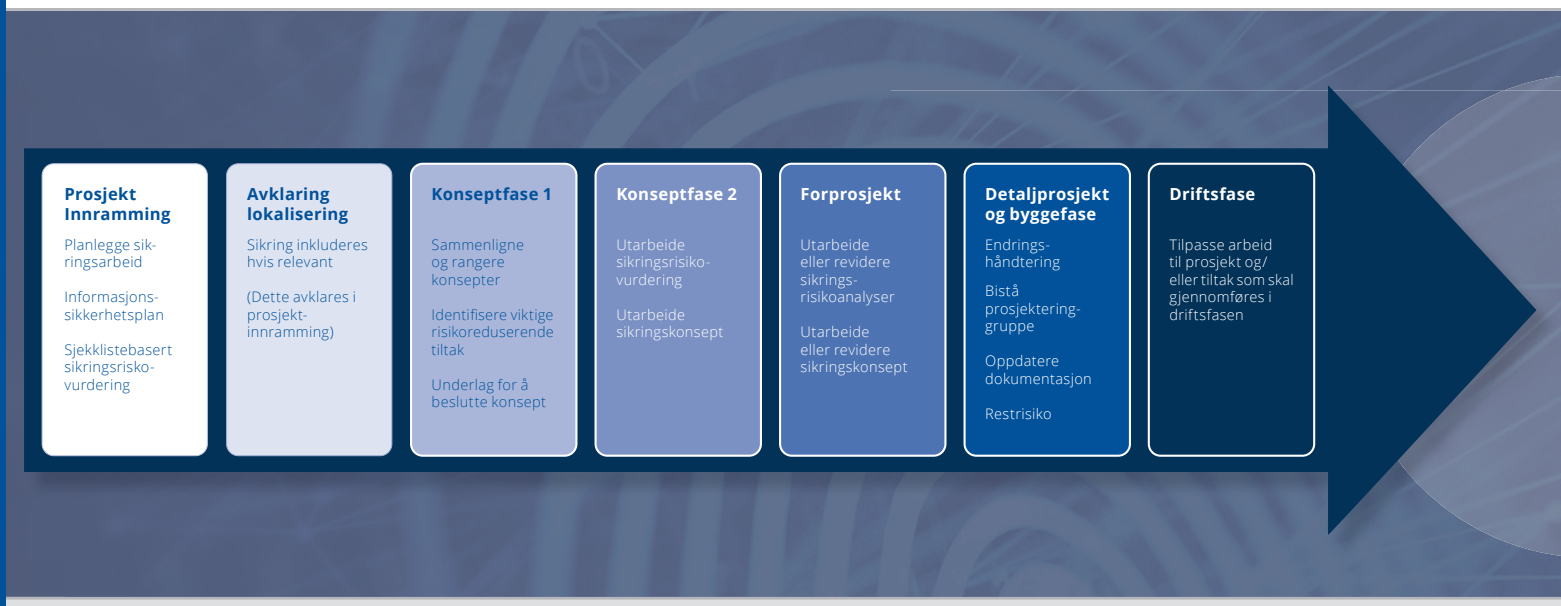
Veilederen er utarbeidet for brukes i alle faser av alle norske sykehusprosjekter, store og små. Veiledningen er bygget opp med utgangspunkt i Veileder for tidligfasen i sykehusprosjekter (Sykehusbygg, 2017) og prosjektfasene som beskrives i denne. I tillegg gis det føringer for påfølgende prosjektfaser, utover tidligfaseveilederens omfang, og driftsfasen.

Formålet med dette er å sikre at risikovurderingene integreres i prosjektet og tilpasses de beslutninger som skal tas i de ulike fasene.
Det er laget egne kapitler for de enkelte fasene. Variasjoner rundt behov i konkrete prosjekter er sannsynlig. Det presiseres derfor at arbeidet med sikring og risikovurderinger må tilpasses prosjekt og fase i de konkrete tilfellene.

3.1 Sikring i prosjektinnramming

Formålet med prosjektinnrammingen er å utarbeide styringsdokument for prosjektet og et mandat for konseptfasen. Styringsdokumentet skal på et overordnet nivå beskrive hvordan tidligfasen skal gjennomføres i samsvar med mål og strategier beskrevet i utviklingsplanen.
Sikringsarbeidet i prosjektinnrammingen må innrettes slik at det danner et godt grunnlag for arbeid med sikring i påfølgende faser. I praksis omfatter dette en grov, sjekklistebasert kartlegging av risiko. Dette inkluderer en kartlegging av overordnede verdier/funksjoner, generiske trusselscenarioer og vurdere betydning for lokalisering.

Det er også viktig å vurdere prosjektets behov for informasjonssikkerhet allerede i denne fasen. Dersom prosjektet skal forholde seg til skjermingsverdig informasjon, planlegge objekter eller infrastruktur som understøtter grunnleggende nasjonale funksjoner, eller omfatte annen beskyttelsesverdig informasjon, må det legges en plan for hvordan informasjonen i prosjektet skal tilvirkes, behandles og lagres. Vurderingen vil også omfatte vurderinger rundt sikkerhetsgradering av personell, autorisasjon av personell, anskaffelser, bruk av informasjonssystemer, håndtering av bygningsinformasjonsmodeller (BIM) m.m.



Figur 4. Prosjektsteg og arbeid med sikring.

Hovedleveranser fra fasen:	Styringsdokument for prosjektet som avklarer hvordan tidligfasen skal gjennomføres.
Input til fasen	• Nasjonal helse- og sykehusplan, regional plan, utviklingsplan • Overordnet prosjektbeskrivelse, prosjektmål m.m. • Sjekkliste for sikring i prosjektinnramming (se kap. 4.3). • Eier og brukers driftserfaringer. • Nasjonale og/eller virksomhetsspesifikke trusselvurderinger. • Det regionale helseforetakets vurdering av om prosjektet omfatter skjermingsverdige verdier. • Eventuelle regionale risiko- og sårbarhetsanalyser (ROS) på fylkes- eller kommunenivå.
Aktiviteter	
Prosjekteier (HF eller RHF)	• Bruker/prosjekteier er gjerne samme aktør i denne fasen. • Vedta output fra sikringsprosessen. • Inkludere oppsummering om sikring i styringsdokument og mandat.
Bruker (HF, sykehusapotekene, universiteter m.m.)	Sikringsrådgiver/kontaktperson for sikring (ev. sikring drift) fra HF bistår utøvende i arbeidet med sikring i prosjektinnrammingen.
Prosjektgruppe (HF, RHF eller Sykehusbygg m/sikringsrådgiver)	Gjennomgå sjekkliste for sikring i prosjektinnramming (se kap. 4.3): Verdikartlegging: identifisere funksjoner med sikringsbehov. • Særegne trusler for sykehusprosjektet (sjekk mot kap. 4.1.2.1). • Spesielle sårbarheter knyttet til planlagt prosjekt. • Definere kritikalitetsnivå for plan for informasjonssikkerhet: normal, hevet (f.eks. unntatt offentlighet eller referanse til beskyttelsesinstruksen), høyt/sikkerhetsloven). Utarbeide plan for sikringsrisikostyring i prosjektet avhengig av verdi-, trussel- og sårbarhetsbildet.

PROSJEKTFASER OG ARBEID MED SIKRING

Offentlige myndigheter	Forespørsel til lokalt politi om det er noe spesielt man bør legge til grunn for prosjektet.
Output: leveranser fra prosjektgruppe	Enkelt notat som oppsummerer arbeidet med sikring: • Overordnet prosjekt-/systembeskrivelse (jf. kap. 4.2) • Identifiserte verdier, trusler, sårbarheter (jf. sjekkliste kap. 4.3) • Anbefalinger til arbeid med sikring videre i prosjektet med omfang-sestimater • Input til plan for overordnet risikostyring i prosjektet • Anbefaling om informasjonssikkerhetsplan for prosjektet iht valgt kri-tikalitetsnivå og plan for samspill med regionale IKT-foretak/enheter.
Forventet arbeidsvolum (størrelsesorden)	Prosjekteier/bruker: 40 timer Prosjektgruppe/utførende: 60 timer Off. myndigheter: < 8 timer
Kommentarer	Prosjektgruppe bør utføre en enkel vurdering av om sikkerhetskonsep-tet påvirker lokalisering, eller motsatt (jf. sjekkliste i kap. 4.3).

Sårbarhet er definert som manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning

3.2 Sikring i forbindelse med avklaring lokalisering

Hovedformålet med denne fasen er å utrede og avklare lokalisering for bygget. Arbeidet skal generelt bygge på utviklingsplan, godkjent mandat for avklaring av lokalisering og godkjent styringsdokument for tidligfasen.

Fasen skal resultere i en konsekvensutredning (KU) etter Plan og bygningsloven (ved behov). Det skal også leveres en utredning av lokalisering av bygget hvor man har bestemt lokalisering, men ikke nødvendigvis tomt. For øvrig er bl.a. følgende underlag relevant: tilgjengelighetsvurderinger, kostnadsanalyser og økonomiske effekter, reguleringsmessige forhold, risikovurderinger m.m.

Det er ikke forhåndsdefinert aktiviteter knyttet til sikring i forbindelse med avklaring av lokalisering i denne veilederen. Årsaken til dette er at avklaring av lokalisering er prosesser som kan gå over svært lang tid og er ulike fra gang til gang. Risikovurderinger er for øvrig et viktig underlag for denne fasen.
Vurderinger av sikringsrisiko må innrettes slik at det kan nyttiggjøres i helhetlige risikovurderinger som gjennomføres i denne fasen. Videre er det sentralt å stille seg spørsmål om sikringskonseptet kan påvirke lokalisering, eller om lokalise ring kan påvirke sikringskonseptet. Dette skal også vurderes i prosjektinnrammingsfasen, hvor det eventuelt vil anbefales konkrete oppfølgingsaktiviteter i forbindelse med avklaring lokalisering.

Forhold knyttet til opptrapping av beredskap i samsvar med Sivilt Beredskapssystem (SBS) er viktig å sjekke ut i forbindelse med avklaring av lokalisering. Se sjekkliste for sikring i prosjektinnramming for nærmere føringer for dette arbeidet, jf. kap. 4.3.
Det er også hensiktsmessig å revurdere behovet for informasjonssikkerhet i prosjektet.

3.3 Sikring i konseptfasen, del 1

Hovedformål med konseptfase del 1 er å utvikle et hovedprogram og gjennomføre alternativutredning. Etter endt fase skal det tas en beslutning på anbefalt alternativ for utdypning i konseptfase del 2.

Sikringsarbeidet i konseptfase del 1 må innrettes slik at de ulike alternativenes styrker og svakheter med hensyn på sikring belyses.

Det må legges opp til en sammenlignende/komparativ form på risikovurderingene. Risikovurderingene skal bidra til at det velges hensiktsmessig tomt og sykehuskonsept, mest mulig i tråd med prosjektets målsetninger.

Arbeidet har tre hovedmål:

1. Rangere ulike alternativer/konsepter med hensyn sikringsutfordringer.
2. Identifisere viktige/kostnadsdrivende risikoreduserende tiltak tilknyttet hvert alternativ/konsept.
3. Danne grunnlag for sikringsarbeidet i etterfølgende faser.

Det må etableres en hensiktsmessig systembeskrivelse for hvert konsept (jf. kap. 4.2) og foreta en sammenlignende/komparativ analyse av de ulike konseptene (jf. kap. 4.4). Systembeskrivelsen må være så detaljert at den gir grunnlag for å identifisere vesentlige forskjeller mellom konseptene.

Hovedleveranser fra fasen:	Hovedprogram og alternativvurdering
Input til fasen	Notat om sikring fra prosjektinnramming Plan for arbeid med sikring i prosjektet fra prosjektinnramming Informasjonssikkerhetsplan basert på anbefaling fra prosjektinnramming
Aktiviteter	
Prosjekteier (HF eller RHF)	Vedta output fra sikringsprosessen. Inkludere oppsummering om sikring i konseptrapport.
Bruker (HF, sykehusapotekene, universiteter m.m.)	Sikringsrådgiver/kontaktperson for sikring (ev. sikring drift) fra HF bidrar med erfaringer. Utvalgt personell fra teknisk og tillitsvalgt og verneombud fra klinisk drift deltar i den komparative risikovurderingen.
Prosjektgruppe (HF, RHF eller Sykehusbygg m/sikringsrådgiver)	Gjennomgang av verdi- og trusselliste fra prosjektinnramming. Oppdatere med ny informasjon. Avklare og dokumentere fasetilpasset systembeskrivelse for konseptene (lokalisering, driftskonsept, tekniske løsninger). Innhente erfaringer fra drift. Gjennomføre komparativ risikovurdering basert på forhåndsdefinerte scenarioer (se kap. 4.4). Hensikt: • Avdekke vesentlige forskjeller mellom alternativene. • Identifisere overordnede sikringstiltak (med betydning for konseptvalg). • Danne grunnlag for sikringsarbeidet i neste fase. • Samhandling og koordinering mot øvrige involverte fag.
Offentlige myndigheter	Forespørsel til lokalt politi om oppdateringer knyttet til trusselsituasjonen. Vurdere avklaringer mot andre myndigheter (strålevern, smittevern, dsb, kommune m.m.).
Output: leveranser fra prosjektgruppe	Dokument som dokumenterer arbeidet med sikring, evt sikring som et eget punkt i alternativvurderingen. Kapittel (sammendrag) om sikring til konseptrapport.
Kommentarer	Systematisk gjennomgang av hvert alternativ for å identifisere sårbarheter basert på et sett med forhåndsdefinerte scenarioer. Gjennomføres som en forberedt gruppeprosess/idémyldring med etterarbeid og rapportering. Riktige deltakere og god prosessledelse er nøkkelord for god kvalitet (se kap. 4.1.1 for veiledning til planlegging av prosessen).

3.4 Sikring i konseptfasen, del 2

Hovedformål med konseptfase del 2 er å utdype hovedprogram for valgt hovedalternativ med detaljerte skisser og tilhørende kalkyler og utredninger. Etter endt fase skal konseptrapporten og eventuelt rapport fra ekstern kvalitetssikring (for prosjekter > 500 mill.) behandles. Det skal tas et endelig valg om hvilket konsept/alternativ som skal bearbeides videre i forprosjektfasen, gi grunnlag for lånesøknad til departementet, og eventuelt godkjenning etter spesialisthelsetjenesteloven.

Målet med prosjektsteget er å detaljere ut valgt hovedkonsept og skape mer trygghet rundt kalkylen. Arbeidet med sikring må bidra til dette. Sikringsarbeidet i konseptfase del 2 bør omfatte en sikringsrisikovurdering. Sikringsrisikovurderingen utføres i samsvar med kap. 4.1, og at denne er grunnlag for å lage et sikringskonsept, jf. kap. 4.6. Målet er å identifisere vesentlige risikoforhold og risikoreduserende tiltak som må tas med i planlegging og prosjektering av andre faggrupper. Sikringskonseptet er en beskrivelse av organisatoriske, menneskelige og fysiske/tekniske tiltak som anbefales for å oppnå et akseptabelt risikonivå for sykehuset.

3.5 Sikring i forprosjekt

Målet med forprosjektet er å bearbeide det valgte konseptet til et nivå hvor gjennomførbarhet og kostnader er bestemt, slik at en investeringsbeslutning

Hovedleveranser fra fasen:	- Konseptrapport med følgende vedlegg: hovedprogram; alternativvurdering; skisser og modeller av anbefalt alternativ med tilhørende kalkyler; forslag til mandat for forprosjekt m.m.
Input til fasen	- Notat om sikring fra prosjektinnramming og komparativ analyse fra konseptfase del 1. - Plan for arbeid med sikring i prosjektet fra prosjektinnramming. - Informasjonssikkerhetsplan basert på anbefaling fra prosjektinnramming. - Beskrivelse av valgt hovedkonsept.
Aktiviteter	
Prosjekteier (HF eller RHF)	- Vedta output fra sikringsprosessen. - Beslutte sikringskonsept basert på anbefalingene fra sikringsprosessen.
Bruker (HF, sykehusapotekene, universiteter m.m.)	- Vedta output fra sikringsprosessen. - Beslutte sikringskonsept basert på anbefalingene fra sikringsprosessen.
Prosjektgruppe (HF, RHF eller Sykehusbygg m/sikringsrådgiver)	- Utarbeide detaljert systembeskrivelse, jf. kap. 4.2. - Implementere standardiserte grunnsikringstiltak, jf. kap. 5. - Gjennomføre sikringsrisikoanalyse, jf. kap. 4.1. - Samhandling og koordinering mot øvrige involverte fag. - Utarbeide sikringskonsept basert på sikringsrisikovurderingen, jf. kap. 4.6.
Offentlige myndigheter	- Forespørsel til lokalt politi om oppdateringer knyttet til trusselsituasjonen. - Vurdere avklaringer mot andre myndigheter (strålevern, smittevern, dsb, kommune m.m.).
Output: leveranser fra prosjektgruppe	- Helhetlig sikringsrisikovurdering, jf. kap. 4.1. - Sikringskonsept, jf. kap. 4.6.
Kommentarer	

kan tas på riktig grunnlag. Valgt sikringskonsept vil ha en del avgjørelser, som bæresystem og plassering av funksjoner, som legger føringer for det videre arbeidet med sikring.
Tidlig i forprosjektet vurderes å være «siste frist» for å gjennomføre en helhetlig sikringsrisikovurdering for å ha en reell påvirkningskraft på løsninger. I valg av entrepriseform og tildelingskriterier bør kompleksitet og gjennomføringsrisiko av sikringstiltakene være en del av beslutningsunderlaget. Hvis det er utarbeidet en helhetlig sikringsrisikovurdering i konseptfasen bør denne oppdateres i forprosjektet. En detaljering av sikringsrisikovurderingen fra konseptfasen kan også være hensiktsmessig for å understøtte valg av konkrete løsninger. Tilsvarende oppdateres sikringskonseptet, og sikringsmål kan eventuelt revurderes og forankres hos prosjekteier.

Sikringsarbeidet i forprosjekt har fokus på valg av løsninger og nivå/klasser av sikringsprodukter, samt tilhørende kostnader og tverrfaglige konsekvenser. Løsninger og konsekvenser må omforenes med nødvendige brukerrepresentanter som sikkerhetsansvarlig, tillitsvalgte/ombud, ledere og driftsorganisasjon. Eventuelle tiltak som kan komme i konflikt med vernede eller fredede fasader, interiør og landskap må gjennomgås med relevante myndigheter.
Hovedleveranser i et forprosjekt vil være sikringsplaner med fokus på nivå for fysisk sikring, TVO-dekning, sone- og robusthetsplaner, funksjonsbeskrivelser m.m. Spesielt for resepsjoner og mottak med flere brukergrupper og bruksmåter er det viktig at funksjonsbeskrivelser gjennomgås med brukers sikkerhetsansvarlige, og at tilstrekkelig plass og teknisk infrastruktur etableres for de tiltak som omfattes av konseptet.

Hovedleveranser fra fasen:	- Forprosjektrapport med følgende vedlegg: Romfunksjonsprogram; brutto- og netto utstyrsprogram; beskrivelser og modeller på romnivå, og detaljering av bygningsmessige og tekniske løsninger; overordnet IKT-program. - Mandat for neste fase.
Input til fasen	- Sikringskonsept fra konseptfasen - Konseptrapport med underliggende delutredninger m.m.
Aktiviteter	
Prosjekteier (HF eller RHF)	- Investeringsbeslutning
Bruker (HF, sykehusapotekene, universiteter m.m.)	- Sikringsrådgiver/kontaktperson for sikring (ev. sikring drift) fra HF godkjenner funksjonsbeskrivelser. - Utvalgt personell fra teknisk og tillitsvalgt og verneombud fra klinisk drift kommer med innspill for å forankre løsninger og funksjonsbeskrivelser.
Prosjektgruppe (HF, RHF eller Sykehusbygg m/sikringsrådgiver)	- Samhandling, koordinering, - Valg av løsninger og klasser for sikringstiltak. - Oppdatering og/eller detaljering av sikringsrisikovurdering og sikringskonsept, eller utarbeide detaljert sikringsrisikovurdering hvis dette ikke er gjennomført i konseptfasen. - Samhandling og koordinering mot øvrige involverte fag. - Arbeid med sikringsplaner, funksjonsbeskrivelser og bistand til kalkyle for sikringstiltak.
Offentlige myndigheter	- Forespørsel til lokalt politi om oppdateringer knyttet til trusselsituasjonen. - Vurdere avklaringer mot andre myndigheter (strålevern, smittevern, dsb, antikvariske myndigheter, kommune m.m.).
Output: leveranser fra prosjektgruppe	- Forespørsel til lokalt politi om oppdateringer knyttet til trusselsituasjonen. - Vurdere avklaringer mot andre myndigheter (strålevern, smittevern, dsb, antikvariske myndigheter, kommune m.m.).
Kommentarer	

3.6 Sikring i detaljprosjekt og byggefase

Formålet med detaljprosjektfasen er å detaljere ut prosjektet til et entydig nivå som muliggjør en kvalitetssikret utførelse for entreprenør i byggefasen. Selv om mulighetene for å påvirke sikringsnivå i positiv retning er begrenset i disse fasene, er tett involvering av sikringsrådgiver i prosjekteringsgruppen med tanke på oppfølging og bistand viktig for et godt sluttresultat. Sikringsarbeidet i detaljprosjekt vil omfatte kvalitetetssikring av tilbuds- og arbeidsunderlag fra arkitekt og rådgivende ingeniører, tverrfaglig kontroll av sikringsløsninger, avviksbehandling av detaljerte løsninger og verifikasjon av sikringsplaner. Det vil også være hensiktsmessig at sikringsrådgiver er involvert i evaluering av tilbydere.

Fravik i detaljeringen kan oppstå fra forskriftskrav, tverrfaglige og praktiske tilpasninger, kostnadspress, samt tilpassing til eksisterende forhold i forbindelse med rehabiliteringsprosjekt. Måloppnåelse må dokumenteres, og ved avvik må sikringsrisikovurderingen og sikringskonsept oppdateres og godkjennes av beslutningstaker.
I byggefasen vil sikringsarbeidet bestå av godkjenning av tilbudte løsninger og produkter fra entreprenør, kontroll av dokumentasjon av klasser og ytelser, samt avviksbehandling av utførelsen. Fravik i byggefasen kan f.eks. oppstå ved at byggbarhet ikke er tilstrekkelig vurdert i detaljeringen, tilpassing til eksisterende forhold, eller menneskelige feil i utførelsen. For å oppdage og dokumentere fravik er det nødvendig at sikringskompetanse er tilstede på byggeplassen, enten ved kompetente byggeledere eller befaringer av sikringsrådgivere.

Ved overlevering leveres «som bygget»-dokumentasjon på sikringsplaner, sikringsrisikovurderinger og måloppnåelse av sikringskonsept/restrisikorapport. Dette danner grunnlaget for tiltak i driftsfasen som administrative rutiner og beredskapsplaner, og er også viktig underlag for fremtidige prosjekt.

Hovedleveranser fra fasen:	- Detaljprosjekt: Produksjonsunderlag for entreprenør. - Byggeprosjekt: Ferdig bygg med innhold.
Input til fasen	- Forprosjekt
Aktiviteter	
Prosjekteier (HF eller RHF)	- Godkjenning av oppdaterte sikringsrisikovurderinger og sikringskonsept
Bruker (HF, sykehusapotekene, universiteter m.m.)	- Brukerrepresentanter bidrar ved behov for avklaringer.
Prosjektgruppe (HF, RHF eller Sykehusbygg m/sikringsrådgiver)	- Oppfølging og kvalitetssikring av prosjekteringsgruppe og utførende. - Bistå i utarbeidelse av detaljer: vinduer, vegger, dører, innfesting, ventilasjon, m.m. - Gjennomføre sårbarhetsanalyser/-beregninger og utarbeide notater knyttet til spesifikke løsninger/produkter etter behov fra prosjekteringsgruppen. - Kontakt med leverandører av sikringsprodukter. - Oppdatering av analyser og sikringskonsept.
Offentlige myndigheter	- Forespørsel til lokalt politi om oppdateringer knyttet til trusselsituasjonen.
Output: leveranser fra prosjektgruppe	- Oppdaterte (as built) sikringsplaner og konsept. - Måloppnåelse/restrisikorapport som grunnlag for beredskapsplanlegging i driftsfasen.
Kommentarer	

3.7 Sikring i driftsfasen

Fra et sikringsperspektiv er målet med fasen at bruker opplever gevinster ved tilfredsstillende sikringsnivå og effektiv drift. En riktig grunnsikring kan eksempelvis redusere vaktbehov.

Basert på etablerte kvalitets- og risikostyringsprinsipper bør implementerte tiltak evalueres og måles kontinuerlig. Ideelt sett bør også prosjekteringsgruppen og sikringsrådgivere få tilbakemelding på hvor hensiktsmessige tiltakene er i daglig drift. Dette bør derfor legges inn som en del av evalueringsprosess for prosjekter.

Som et resultat av risikostyringsprosessen, eller om det oppstår som behov for endringer i bygningsmassen, organisering m.v., må sikringsmessige konsekvenser vurderes. Et minstekrav, og en hensiktsmessig start, er at det utføres en sikringsrisikovurdering som er tilpasset endringen som ønskes gjennomført. Ved mindre endringer kan en komparativ sårbarhetsanalyse (jf. kap. 4.4) være tilstrekkelig, mens ved større endringer må det tas hensyn til at trusselbilde, verdier, etc endres og en helhetlig sikringsrisikovurdering (jf. kap. 4.1) må gjennomføres.

Ved utførte endringer må «som bygget»-leveranser som f.eks. soneplaner oppdateres. Ved avhending av bygningsmasse, tekniske systemer, utstyr m.m., må det finnes en oversikt over sensitive installasjoner og informasjon, og etableres en plan for sanering av disse.

I driftsfasen er veilederen særlig relevant i følgende situasjoner, som omtales nærmere nedenfor:

- Tilstandskartlegging
- Situasjoner med hevet risikonivå i driften
- Særskilte sikringsprosjekter
- Ombyggings- og/eller rehabiliteringsprosjekter

Tilstandskartlegging
For mange sykehus vil det bli aktuelt å vurdere og beskrive sikkerhetstilstanden. Denne veilederen spesifiserer både en metode for risikovurdering og et minimum grunnsikringsnivå. Metoden for risikovurdering kan, på et selvstendig grunnlag, brukes til å kartlegge og prioritere trusselscenarioer og potensielle tiltak for å redusere risiko.

Samtidig vil også beskrivelsen av minimum grunnsikringsnivå kunne benyttes til å vurdere avvik på egne sykehusbygninger.

Begge metodene kan gi relevant informasjon for beslutningstaker med hensyn til blant annet:

- Sykehusets og/eller spesifikke bygningers sikkerhetsnivå.
- Behov for bygningsmessig og/eller organisatoriske tiltak.
- Hvilke bygninger som bør prioriteres med hensyn til sikkerhetsmessig oppgradering eller annen bruk.

Der det velges å utføre en sikringsrisikovurdering anbefales det å starte med en gjennomgang av sjekklisten for prosjektinnrammingsfasen, jf. kapittel 4.3. Deretter kan det gjennomføres en sikringsrisikovurdering for utvalgte analyseobjekt/verdier etter metoden beskrevet i kapittel 4.1.

Situasjoner med hevet risikonivå i driften
I alle virksomheter vil risikonivået variere med tiden. Sykehusets sikringskonsept, som er summen av fysiske, elektroniske og organisatoriske tiltak, skal være så robust at det håndterer risikonivået som følger av normale driftsvariasjoner. I tillegg til normale driftsvariasjoner vil det oppstå situasjoner med særlig hevet risikonivå. Dette er situasjoner som kan kreve særskilte risikoreduserende tiltak, utover tiltak som ligger i det ordinære sikringskonseptet og vanlig drift. Hva som regnes som en situasjon med særlig hevet risiko er avhengig av hva sykehuset har planlagt og organisert seg for i utgangspunktet. For enkelte syke-

hus kan en situasjon med utkobling av adgangskontrollanlegget kreve en særskilt risikogjennomgang og ekstraordinære tiltak. For andre sykehus håndteres denne situasjonen gjennom normal drift og i henhold til standard prosedyrer.

Veilederen kan brukes til å planlegge for situasjoner med hevet risikonivå i driften, slik at sykehuset er bedre forberedt dersom situasjonen oppstår. En mulig fremgangsmåte er å starte med å kartlegge mulige situasjoner som kan oppstå. Dette kan være situasjoner med økt bygningsmessig og eller organisatorisk sårbarhet, høyere trusselnivå og/eller flere viktige verdier samlet på sykehuset.

Deretter gjennomføres det en risikovurdering for de aktuelle situasjonene. Dersom sykehuset allerede har en risikovurdering, er det interessant å se på hvilke endringer i risikobildet som oppstår i de identifiserte situasjonene.

Særskilte sikringsprosjekter

Av ulike årsaker vil det være aktuelt for sykehus å gjennomføre særskilte sikringsprosjekter. Dette kan være at en regelverksendring fører til nye krav til bygningsmassen, ønsker om risikoreduksjon knyttet til erfarte uønskede handlinger, utvikling av god praksis i sektoren, resultat av egne risikovurderinger (jf. Pkt. om tilstandskartlegging ovenfor) m.m. I denne situasjonen er gjerne risikoproblemet kjent, der utgangspunktet for arbeidet er en foreliggende sikringsrisikovurdering.

Målet med prosjektet er å finne riktige risikoreduserende tiltak, altså risikohåndtering. Sikringskonseptet for sykehuset er summen av bygningsmessige, elektroniske og organisatoriske tiltak. I denne typen situasjoner er det viktig å finne en riktig balanse mellom ulike tiltaksstrategier. Kan risiko reduseres ved å gjøre endringer/forsterkninger i organisatoriske tiltak, kreves bygningsmessige endringer, eller begge deler?
Dersom det allerede er utført en sikringsrisikovurdering, vil det være hensiktsmessig å starte med å evaluere relevante forslag til risikoreduserende tiltak fra denne. Løser de foreslåtte tiltakene problemet? Hvis ikke, må det gjennomføres en kartlegging av andre potensielle risikoreduserende tiltak. Forslag til risikoreduserende tiltak evalueres etter prinsippene beskrevet i kap. 4.1.4.

Ved evaluering av foreslåtte risikoreduserende tiltak, må disse sees i sammenheng med risikobildet som er beskrevet i forkant av prosjektet. I etterkant av prosjektet er det hensiktsmessig at risikovurderingen, og risikobildet for sykehuset, oppdateres med de nye tiltakene implementert.

Ombyggings- og/eller rehabiliteringsprosjekter

Når sykehuset skal gjennomføre en bygningsmessig endring som organiseres i et ombyggings- og/eller rehabiliteringsprosjekt, brukes veilederen i utgangspunktet på samme måte som i et nybyggprosjekt. Hvis prosjektet følger Sykehusbyggs vanlige prosjektfaser, organiseres også sikringsarbeidet i de samme fasene, som beskrevet i kap. 3.1 - 3.6.

I mindre prosjekter, med annen faseinndeling, må sikringsarbeidet organiseres basert på skjønn. De viktigste leveransene fra sikringsarbeidet er 1) risikovurdering og 2) sikringskonsept. Risikovurderingen må tilpasses de beslutninger som skal tas i prosjektet.

Hvis omfanget av eventuelt sikringsarbeid er slik at det gjennomføres som et prosjekt, er det viktig å være klar over at rehabiliteringsprosjekter generelt, og spesielt med tanke på sikring, erfaringsmessig har høyere gjennomføringsrisiko enn nybyggprosjekter. Det er da viktig at det etableres tilstrekkelig prosjektorganisasjon og risikostyring fra starten av, og at Sykehusbyggs fasenorm (tidligfaseveilederen) følges fullt ut.

Del 4. Metodebeskrivelser og verktøy

Verdier, sårbarhet og trusler vil være sentrale elementer i risikovurderingen. Konsekvensenes, det vil si tapets, størrelse vil være avhengig av systemets verdi. Hvorvidt konsekvenser/tap realiseres ved en hendelse, er avhengig av systemets sårbarhet ovenfor det aktuelle scenarioet. Trusler vil være de underliggende årsakene til at konsekvenser/tap kan oppstå.

4.1 Helhetlig sikringsrisikovurdering (konseptfase, del 2/forprosjekt)

Her beskrives anbefalte steg i en helhetlig sikringsrisikovurdering, basert på risikoperspektivet som er valgt (Se tekstboks til høyre og vedlegg A, kap. 6). Prosessen anbefales gjennomført i sin helhet i konseptfase del 2, eller alternativt tidlig i forprosjektet.

Deler av prosessen er relevant for andre prosjektfaser. Dette gjelder for eksempel veiledning til planlegging av prosessen, føringer for systembeskrivelse, beskrivelse av trusselscenarioer m.m. Se kap. 3.1 og 3.3 for veiledning til anvendelse i prosjektinnramming og konseptfase del 1.

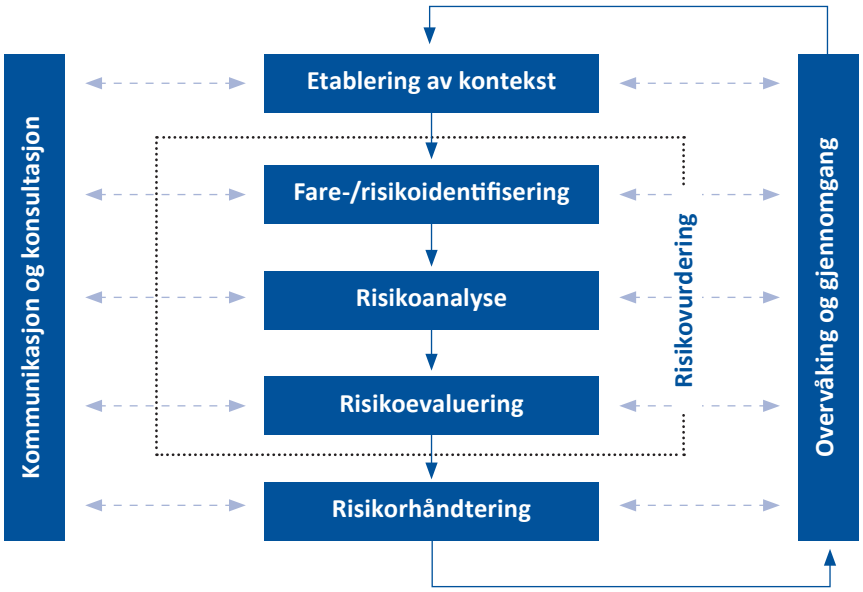
Veiledningen tar utgangspunkt i en vanlig risikostyringsprosess, slik den er beskrevet i ISO 31000 (ISO, 2018), jf. Figur 5.

Risiko er kombinasjonen av hendelser (A) med konsekvenser (C) og tilhørende usikkerheter (U) (Aven, 2007; 2010).

A som alle tenkelige trusselscenarioer som kan oppstå på et sykehus.

C er alle mulige konsekvenser av trusselscenarioene.

U er et uttrykk for at det er usikkerhet knyttet til om scenarioene vil oppstå, konsekvenser hvis scenarioet oppstår og tilgjengelig bakgrunnskunnskap



Figur 5 Risikostyringsprosessen (ISO 31000:2018).

Figur 6 illustrerer trinnene i risikostyringsprosessen anvendt på sikringsområdet. Trefaktormodellen (verdi, trussel, sårbarhet) er integrert i den tradisjonelle risikostyringsprosessen slik vi kjenner den fra ISO 31000 og NS 5814. Dette bidrar til at sikringsutfordringer får sin naturlige plass i den generelle risikostyringen i helseforetakene.

I de påfølgende kapitlene gis det en nærmere veiledning til hva som inngår i de ulike stegene i risikostyringsprosessen, relatert til sykehusprosjekter. For en omfattende innføring i sikringsrisikostyring henvises det til for eksempel Talbot & Jakeman (2009). Se også York & MacAlister (2015) for kunnskapsgrunnlag og praktisk tilnærming til sikring av sykehus (USA).

4.1.1 Etablere kontekst: Hva skal analyseres?

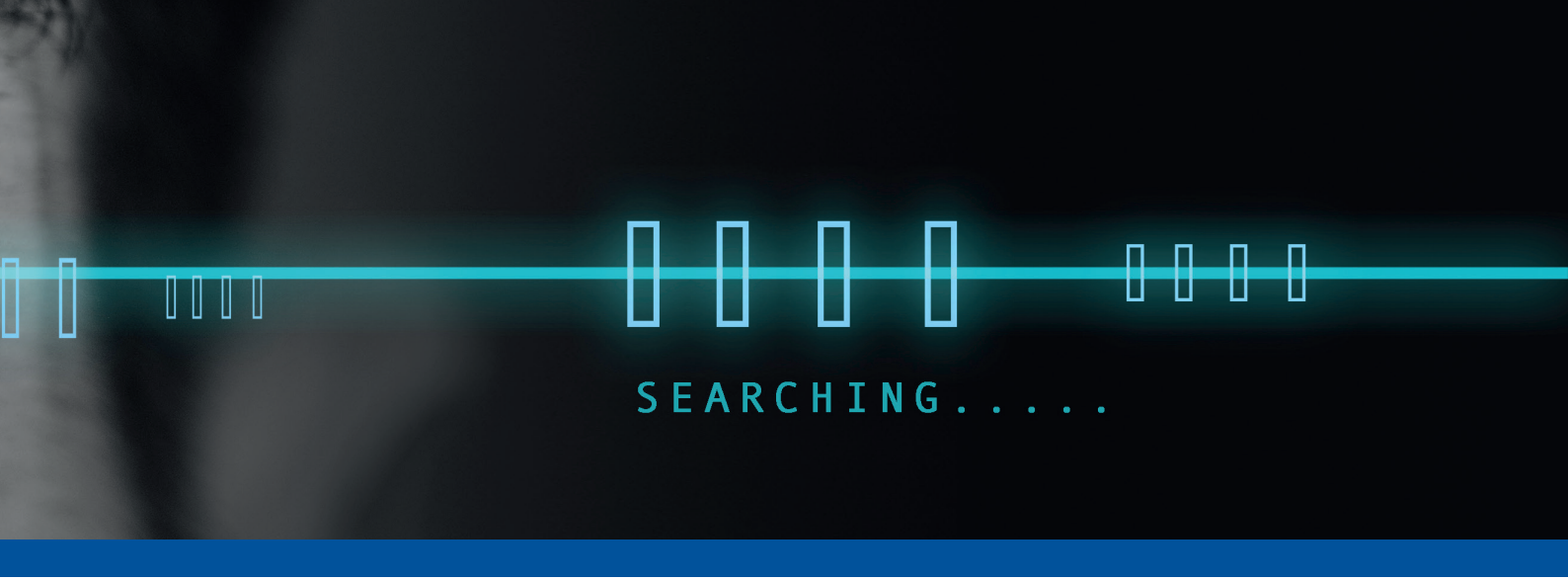
Risikostyringsprosessen må alltid tilpasses slik at den passer med beslutningsprosessene i prosjektet. Risikovurderingene må behandle beslutningsrelevante tema og innpasses i tid slik at de blir et reelt beslutningsunderlag. For å sikre integrasjon med resten av prosjektet må det lages en plan for risikovurderingen, der hovedaktiviteter og milepæler er definert. Planen er også viktig for å sikre forankring hos beslutningstakere.

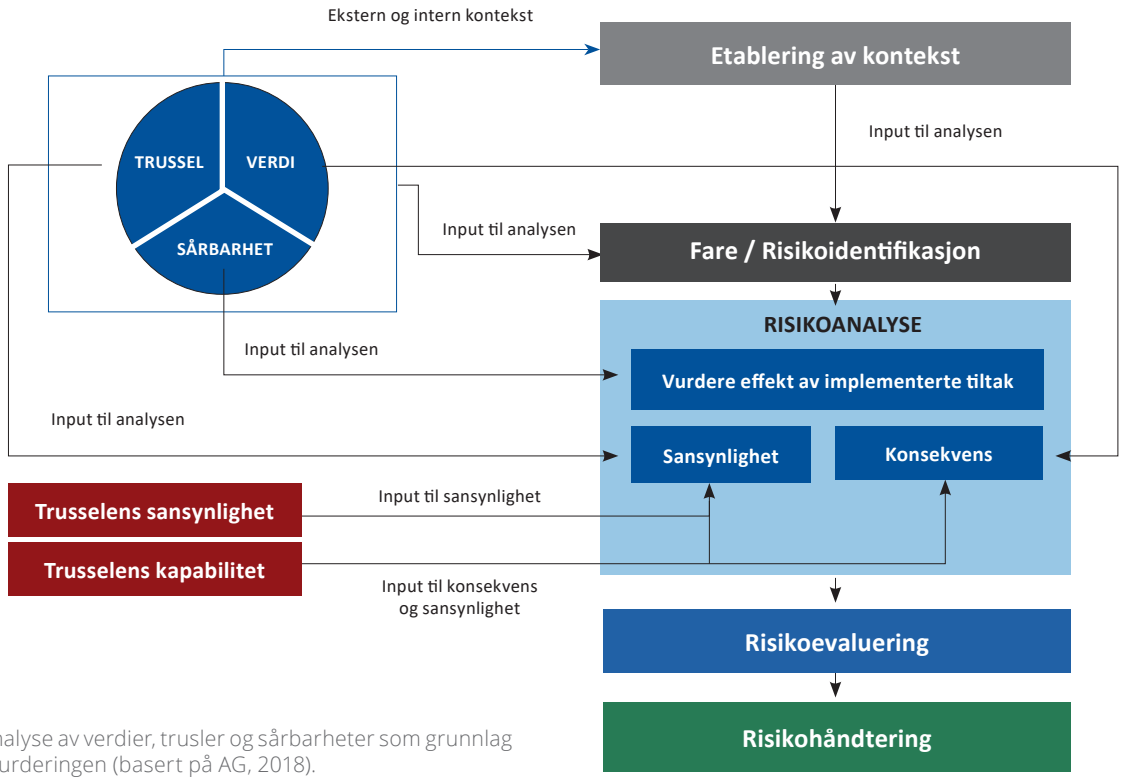
De viktigste aktivitetene i fasen «etablering av kontekst» er:

Definere formål og omfang av risikovurderingen

- Avklare ressurser som skal involveres i risikovurderingen
- Informasjonsinnhenting
- Systembeskrivelse

Prosjektets omfang og fase bestemmer hvordan arbeidet med sikring legges opp, jf. kap. 3. Samtidig må det gjøres en selvstendig vurdering av om veiledningens





Figur 6. Analyse av verdier, trusler og sårbarheter som grunnlag for risikovurderingen (basert på AG, 2018).

anbefalinger er dekkende for prosjektets behov.

Følgende spørsmål er relevante å stille seg:

- Hvilken prosjektfase skal sikringsrisikovurderingen gjennomføres?
- Hvilke spørsmål står i fokus i prosjektfasen?
  - Valg mellom ulike lokasjoner?
  - Valg mellom ulike tomter på en valgt lokasjon?
  - Utredning og valg mellom ulike sykehuskonsepter?
  - Romprogrammering og valg av bygning tekniske kvaliteter?
- Etablering av produksjonsunderlag (detalj-prosjektering) for bygging av sykehuset?
- Hvilke rammebetingelser ligger til grunn for analysen?
  - Tilgjengelig tid?
  - Tilgjengelige ressurser (økonomisk, kapasitet og kompetanse)?
  - Gjeldende regelverk (lov, forskrift og standarder)?
- Er beslutningskriterier for risiko definert og for-ankret i prosjektledelsen?
  - Er det definert prosjektspesifikke sikrings-mål, dvs beskrivelser av ønsket tilstand under og etter tenkelige uønskede handlinger?

Risikovurderinger handler om å sette tilgjengelig kunnskap i system for å si noe om hva vi bør forberede oss på i fremtiden

Organisering

Risikovurderinger handler om å sette tilgjengelig kunnskap i system for å si noe om hva vi bør forberede oss på i fremtiden. Anbefalinger for fremtiden må baseres både på det vi har lært av fortiden og evnen til å forestille oss utviklingstrekk og potensielle/tenkelige scenarioer.

I denne veiledningen er det valgt å beskrive en vanlig arbeidsmetode for risikovurderinger. Risikovurderingen bygges opp med tre faser som er jevnbyrdige med hensyn til tids-/ressursbruk: planleggingsfase, analysefase med analysemøter og etterarbeidsfase:

- **Planleggingsfasen** omfatter aktivitetene som beskrives i kap. 4.1.1 (Etablere kontekst). Rammer og formål med risikovurderingen og involvering av ressurser avklares. Informasjon om prosjektet og problemstillingen samles inn og systematiseres og tilgjengelig gjøres for deltakerne slik at de kan forberede seg godt til analysefasen.
- **Analysefasen** omfatter aktivitetene som beskrives i kap. 4.1.2, 4.1.3 og 4.1.4. Fasen omfatter å identifisere risikoelementer, analysere og klssifisere risikoelementene og evaluere og prioritere disse opp mot beslutningskriterier for risiko. Innspill på analysemøter kan ses på som hypoteser eller påstander, som må testes i etterkant. Oppfølgingen omfatter kvalitetssikring av innspill, kommunikasjon og avklaringer med analysedeltakere eller andre ressurser og eventuelle detaljanalyser ved behov.
- **Etterarbeidsfasen** omfatter å utarbeide dokumentasjon og kommunisere resultatene. Dette omfatter utarbeidelse av rapport som dokumenterer risikovurderingen, samt å utarbeide en rapport for «Sikringskonsept» med resultater som er spesielt viktig for prosjektet å forholde seg til. Et fullverdig sikringskonsept utarbeides gjerne ikke før konsept er avklart (konseptfase, del 2). I de tidligste fasene kan «sikringskonseptet» gjerne være et kapittel/sammendrag i hovedleveransen i prosjektet, tilpasset prosjektets modenhet og formål.

Rolle	Beskrivelse
Prosessleder/ fasiltator	- Ansvar for å planlegge, gjennomføre, dokumentere og kommunisere resultatene fra arbeidet med risikovurderinger og sikringskonsept i prosjektet. Ansvar for å lede prosess og analysemøter. I dette inngår f.eks. å innlede med bakgrunnen for problemstillingen og møter; informere om metode og hvordan møter skal gjennomføres; sørge for at alle deltakerne blir involvert; sørge for at uklare innspill tydeliggjøres; utfordre deltakerne til å skille mellom påstander og fakta. - Sørger for at mest mulig tilgjengelig kunnskap avdekkes gjennom møtene, samt at deltakerne utfordres til å tenke kreativt og fremtidsrettet.
Loggfører	- Ansvar for å dokumentere alt som har relevans for problemstillingen som kommer opp i et analysemøte. Dette omfatter loggføring av innspill, men også beskrivelse av bakgrunnskunnskap, forutsetninger, antakelser og begrunnelser for innspillene. Loggføreren skal støtte prosesslederen og støttes av prosesslederen. - I enkelte tilfeller, som i mindre analysemøter, vil prosesslederen kunne ivareta rollen som loggfører.
Deltakere i analyse-gruppen (arbeidsgruppe)	- Deltakerne i analysegruppen er de som forventes å sitte med nøkkelen til å løse problemet som behandles i risikovurderingen. Sammensetningen av analysegruppen må derfor tilpasses problemstillingen som skal diskuteres. Antall deltakere i analysegruppen bør begrenses så langt som problemstillingen tillater, både av hensyn til ressursbruk og for å oppnå effektive møter. - Utover faglig kompetanse og engasjement forventes det at deltakere i analysegruppen er forberedt til analysemøtet, deltar aktivt i prosessen, er lojal ovenfor instruksjoner fra prosessleder, evner å tenke «utenfor boksen» og evner å forenkle komplekse problemstillinger på en kortfattet og presis måte.
Referansegruppe	- Risikovurderinger tar opp mange utfordringer, som igjen kan påvirke hverdagen til pasienter, pårørende og ansatte i spesialisthelsetjenesten. Behovet for involvering og høringsprosesser er ofte stort. En referansegruppe kan benyttes til dette formålet. Referansegruppen er ikke en del av utførelsen av risikovurderingene, men skal holdes orientert om arbeidet. Prosjekteier har ansvaret for å utnevne referansegruppen og bidra til å planlegge hvordan referansegruppen skal involveres i prosessen.

Tabell 2. Vanlige roller i gjennomføringen av møter i forbindelse med risikovurderinger

Informasjonsinnhenting

Forut for risikovurderingen er det viktig å samle inn relevant informasjon om prosjektet og problemstillingen risikovurderingen skal svare ut. Tilgjengelig informasjon vil være avhengig av prosjektfasen.

Nyttige informasjonskilder:

- Relevante lover, forskrifter, veiledninger og interne instrukser.
- Tilgjengelige oppdaterte åpne trusselvurderinger fra for eksempel Politiets Sikkerhetstjeneste (PST), Nasjonal Sikkerhetsmyndighet (NSM) og Forsvarets e-tjeneste.
- Trusselvurderinger fra lokalt politi via politidistriktets næringskontakt.
- Kart over aktuelle områder/omgivelser for lokalisering av sykehus, inkl. oversikt over for eksempel atkomstveier, beredskapsinstitusjoner, industri, offentlig kommunikasjon m.m.
- Kart over kommunal infrastruktur fram til aktuelle tomter, herunder vann- og avløpsanlegg, strømforsyning, fiber/IKT.
- Tegninger: Oversiktsplaner, plantegninger, utomhusplaner, belysningsplaner, kraftforsyning.
- Rom- og funksjonsprogram.
- Tidligere risikovurderinger, for eksempel for samme sykehus eller lignende sykehus.
- Tidligere robusthetsmatriser som spesifiserer krav til materialkvalitet, produkter, tekniske systemer m.m. i sykehus.
- Statistikk over uønskede hendelser fra Sykehusene (informasjon fra avvikssystem, hendelsesregister hos vakttjeneste e.l.).
- Lokalkunnskap og erfaringer fra eksisterende driftsorganisasjon og befaringer på lokasjon/tomt eller lignende sykehus. Fagpersoner må presentere sine erfaringer og bidra aktivt.
- Relevant forskningslitteratur.

Systembeskrivelse og verdivurdering

Se kapittel 4.2 for veiledning til innhold i en systembeskrivelse. Systembeskrivelsen er viktig i forbindelse med sikring og risikovurderinger av særlig to årsaker:

1. Systembeskrivelsen definerer hva man gjennomfører en risikovurdering av.
2. Systembeskrivelsen er grunnlag for verdivurdering.

Systembeskrivelsen som analysegrunnlag

En systembeskrivelse er en beskrivelse av systemet som skal risikovurderes. Systemet må omfatte geografiske, tekniske og organisatoriske avgrensninger. I denne konteksten vil systemet omfatte sykehuset med tilhørende delsystemer. Systembeskrivelsen inkluderer også en tydelig avgrensning mot systemets omgivelser. I mange sammenhenger brukes også begrepet «analyseobjekt» (NS 5814:2008).

Systembeskrivelsen er avhengig av prosjekt og prosjektfase. Det overordnede kravet til beskrivelsen er at den må være så omfattende at den kan brukes til å identifisere relevante risikoforhold. I de tidligste prosjektfasene vil systembeskrivelsen være overordnet og inneholde få detaljer. Fokuset vil være på egenskaper ved ulike lokasjoner eller sikringsrelevante forskjeller med ulike sykehuskonsepter. Når det skal gjennomføres en sikringsrisikovurdering i forprosjektet må det lages en detaljert systembeskrivelse.

Systembeskrivelsen som grunnlag for verdivurdering

Systembeskrivelsen er en beskrivelse av verdier, dvs ressurser som ved uønsket påvirkning kan medføre negative konsekvenser for sykehuset og/eller samfunnet. Enkelte ressurser har en egenverdi som er viktig å beskytte. Dette gjelder for eksempel menneskers liv og helse og beskyttelsesverdig informasjon, for eksempel pasientdata.

Andre ressurser har instrumentell verdi for sykehuset, dvs at ressursene er innsatsfaktorer for å kunne utfø-

re andre funksjoner. For å kunne gjøre en vurdering av den instrumentelle verdien av en ressurs er det nødvendig å se ressursens rolle i det systemet den er en del av. Et sykehus er for eksempel en ressurs for å ivareta funksjonen akutt psykisk helsevern for barn og ungdom i en region. Dersom det ikke finnes redundans på denne funksjonen i regionen, dvs flere avdelinger for akutt psykisk helsevern, vil den instrumentelle verdien til sykehuset være høyere enn om det fantes reell redundans. Beskrivelser av både interne og eksterne avhengigheter er derfor viktig for å kunne gjøre gode verdi-/konsekvensvurderinger i risikovurderingen.

Verdivurderingen identifiserer og tildeler kritikalitet for alle ressurser/innsatsfaktorer (noe som har verdi for enheten, inkludert ansatte, informasjon, informasjonssystemer, materiell, andre fysiske verdier eller støtteprosesser) som er kritiske for kontinuerlig drift av enheten/funksjonen.

I veilederen er det valgt å definere følgende overordnede verdikategorier for sykehus:

- **Mennesker (liv og helse):** Sykehus skal ivareta personsikkerhet og trygghet.
- **Operativ evne:** Sykehus skal kontinuerlig ivareta sine samfunnsviktige funksjoner. I praksis handler dette om sykehusets evne til å opprettholde tjenester for diagnostikk og behandling.
- **Omdømme:** Sykehus skal ivareta regelverk, bestemmelser og god praksis innen sikkerhetsstyring.

I «trefaktormodellen» (jf. SN, 2014; HSØ, udatert) er verdivurderingen et utgangspunkt for risikovurderingen. Dette forutsetter at det gjennomføres en egen verdi- og skadevurdering. I denne veilederen er det valgt å forenkle metoden på dette punktet ved å forhåndsdefinere sykehusfunksjoner og bygningsdeler som skal eksponeres for definerte trusselscenarioer, jf. Tabell 3.
På denne måten identifiseres verdier gjennom konsekvensvurderingen, dvs. at trusselscenarioene brukes til å kartlegge verdier. Grunnlaget for å gjøre en god konsekvensvurdering etableres i systembeskrivelsen, En separat verdi- og skadevurdering er altså ikke en nødvendig forutsetning for å gjennomføre en risikovurdering etter denne veiledningen. Dersom det likevel foreligger en slik verdi- og skadevurdering vil denne være et godt grunnlag for å gjennomføre konsekvensvurderingen.

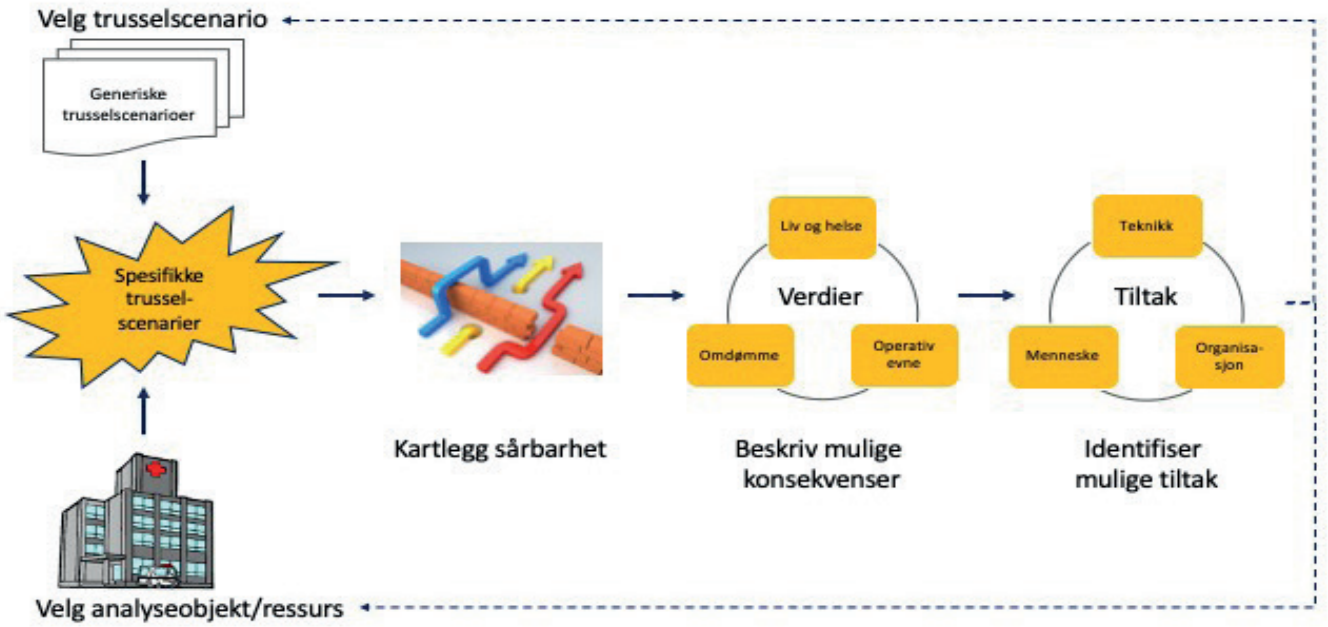
4.1.2 Identifisere risiko

Målet med denne fasen er å identifisere og kartlegge risikoforhold og mulige risikoreduserende tiltak. Et grunnleggende konsept og verktøy denne veilederen bruker til dette formålet er generiske trusselscenarioer (uønskede hendelser). Scenarioene kalles generiske fordi de anses som allmenngyldige for å vurdere sikkerhet mot tilsiktede handlinger i sykehusprosjekter.

De generiske scenarioene forutsettes brukt i alle faser av et sykehusprosjekt, som et utgangspunkt for å identifisere sårbarheter ved planlagt lokalisering, tomtevalg, landskapsplanlegging, bygningsutforming og teknisk infrastruktur, avhengig av prosjektets fase. Mer detaljer om trusselvurdering og utledning av generiske trusselscenario finnes i Del 6 Vedlegg C.

De generiske trusselscenarioene er knyttet opp mot spesifikke sykehusfunksjoner, bygninger og teknisk infrastruktur (verdier) i Tabell 2. Innenfor hver sykehusfunksjon vil det finnes mer konkrete verdier (ressurser/innsatsfaktorer), som er nødvendige for å ivareta sykehusfunksjonen.

Når et generisk trusselscenario kobles sammen med en slik ressurs eller innsatsfaktor innenfor et valgt analyseobjekt, får man et spesifikt trusselscenario. For hvert spesifikke trusselscenario kartlegges sårbarhet, mulige konsekvenser og risikoreduserende tiltak. Dette er illustrert i Figur 7, som er en overordnet prosessbeskrivelse for fasen Identifisere risiko.



Figur 7. Prosessbeskrivelse for fasen Identifisere risiko.

Det settes ingen begrensninger på hvilke trusselscenario som kan diskuteres eller hvilke risikoreduserende tiltak som kan foreslås i denne fasen. Rangering av scenarioer og konsekvenser gjøres i neste steg, kap. 4.1.3 Risikoanalyse.

Figur 8 gir en overordnet beskrivelse av arbeidsoppgavene innenfor hovedstegene i denne fasen, dvs. trusselvurdering, verdivurdering, sårbarhetsvurdering og etablering av risikoregister. Trusselvurdering og scenarioutvikling

Trusselvurdering og scenarioutvikling

En trusselvurdering skal identifisere kilden til en fare og brukes i virksomhetens risikovurdering. Trusler vurderes ved å fastslå trusselaktøren sin intensjon om å skade, ødelegge eller forstyrre, og med hvilken kapasitet (evne og ressurser til å gjennomføre en handling). Veilederen definerer 11 trusselscenario som forventes å være et minimum av scenarioer som behandles i et sykehusprosjekt. På bakgrunn av trusselvurderingen og verdivurderingen etable-

GENERISKE TRUSSELSCENARIOER SOM SKAL VURDERES I ALLE SYKEHUSPROSJEKTER

1. Trusler og fysisk vold mot mennesker på sykehuset
2. Hærverk/skadeverk på utstyr, bygning m.m.
3. Tyveri av utstyr, eiendeler, medisiner, informasjon m.m.
4. Fremsettelse av trusler om alvorlig handling mot sykehuset
5. Selvskading på sykehuset
6. Rømning fra sykehuset (psykisk helsevern, demens, barn m.m.)
7. Frihetsberøvelse av mennesker på sykehuset (gisselsituasjon, kidnapping m.m.)
8. Offentlig uro (f.eks. demonstrasjon) på sykehusets eiendom
9. Fysisk angrep (uautorisert tilgang) på digitale systemer: informasjonstyveri, sabotasje
10. Planlagt og målrettet fysisk angrep mot personer (for eksempel terrorhandlinger)
11. Planlagt og målrettet fysisk angrep mot kritisk funksjon eller infrastruktur (for eksempel sabotasjehandlinger)

TRUSSEL VURDERING

- Kritisk gjennomgang av scenarioliste.
- Supplere/redusere scenarioliste iht. behov i prosjekt/-fase.

VERDI-VURDERING

- Selvstendig verdivurdering.
- Kontrollere liste over trusselscenarioer/verdier mot selvstendig verdivurdering.
- Supplere/redusere liste over trusselscenarioer/verdier tilpasset systembeskrivelsen/prosjektet.

SÅRBARHETS-VURDERING

- Kartlegge sårbarheter ved systemet med utgangspunkt i trusselscenarioene.
- Kartlegge konsekvensene av trusselscenarioene.
- Kartlegge mulige risikoreduserende tiltak.

RISIKOREGISTER

- Samle informasjonen fra risikoidentifikasjonen i et risikoregister.

Figur 8. Arbeidsoppgaver under fasen «Identifisere risiko»

ID	Uønsket hendelse/scenario	Bygning generelt[1]	Uteområde	Somatikk sengepost	Somatikk poliklinikk	Psykiatri sengepost	Psykiatri poliklinikk	Psykiatri sikkerhet	Akuttmottak og legevakt	Prehospital (bygg)	Kontor og adm.	Medisinsk laboratorietjeneste	Bildediagnostikk (radiologiske tjenester)	Forskning	Teknisk infra., inkl. tekniske rom	Annet?
1	Trusler og fysisk vold mot mennesker på sykehuset	1	1	2	1	3	3	3	3	1	1	3	3	1		
2	Hærverk/ skadeverk på utstyr, bygning m.m.	2	2	1	1	3	3	3	3	1	1	3	3	1	1	
3	Tyveri av utstyr, eiendeler, medisiner, informasjon m.m.	1	1	1	1	1	1	1	1	1	1	2	2	3	3	
4	Fremsettelse av trusler om alvorlig handling mot sykehuset	3														
5	Selvskading på sykehuset		2	2	1	3	3	3	3			1	1			
6	Rømning fra sykehuset			2	1	3	2	3	2							
7	Frihetsberøvelse på sykehuset			2	2	3	3	3	3	1	1	2	2	1		
8	Offentlig uro (f.eks. demonstrasjon) på sykehusets eiendom	2	2													
9	Fysisk angrep (uautorisert tilgang) på digitale systemer: informasjonstyveri, sabotasje[2]										2			3	3	
10	Planlagt og målrettet angrep mot personer	3	3	1	1	2	2	2	3	1	1	1	1	1		
11	Planlagt og målrettet angrep mot kritisk funksjon eller infrastruktur			2	2	2	2	2	3	1	1	1	1	2	3	
	Andre relevante scenarioer?															

Tabell 3 Sikring av sykehusfunksjoner (verdier) i lys av generiske trusselscenarioer.

1. Funksjonen «Bygning generelt» benyttes for å fange opp scenarioer som kan oppstå i grensesnittet mellom ute og inne, eller mellom ulike funksjoner som er nevnt spesifikt i tabellen.
2. Digitale trusler (cyberangrep) er del av omfanget for denne veilederen. Det anbefales likevel at det gjøres en vurdering av hvilken betydning et slikt scenario kan få for bygg og teknisk infrastruktur.

res det et sett med spesifikke trusselscenarioer mot gitte verdier, som samlet forventes å kunne benyttes til å gi et representativt risikobilde for virksomheten. Et spesifikt trusselscenario inneholder beskrivelse av en trusselaktør (pasient, ansatt, terrorist, osv.), handlingsmåte (slag/spark, knivangrep, kjøretøy, drone, osv.), og er koblet til et gitt sted eller funksjon. Det er naturlig at arbeidet i dette steget starter med en kritisk gjennomgang av scenariolisten. Listen suppleres med flere scenarioer der dette er relevant. Scenarioer som ikke er relevante for prosjektet eller prosjektfasen tas bort. Den som er ansvarlig for sikringsrisikovurderingen må identifisere spesifikke trusselscenarioer med utgangspunkt i listen over generiske trusselscenarioer.

Ved innføring av nye scenarioer bør disse også defineres som uønskede hendelser. Det er også viktig å ha et bevisst forhold til scenarioets detaljeringsnivå. Et svært detaljert/spesifisert scenario vil for eksempel være langt mindre sannsynlig enn et mer overordnet scenario. Det viktigste er likevel at analysen inkluderer scenarioer som bidrar til å underbygge de beslutninger som skal tas.

Konsekvens-/verdivurdering

I konsekvensvurderingen skal analysegruppen kartlegge potensielle konsekvenser av trusselscenarioene. Tabell 3 gir en oversikt over relevante sykehusfunksjoner og steder, som utgjør verdier på et overordnet nivå. Basert på systembeskrivelsen og verdivurderingen må denne oversikten oppdateres. Finnes det flere viktige sykehusfunksjoner og/eller trusselscenarioer som burde stå på listen? I et forprosjekt er det gjerne nødvendig å gå mer detaljert til verks på etablering av analyseobjekter for å få fram tiltak på riktig detaljnivå.

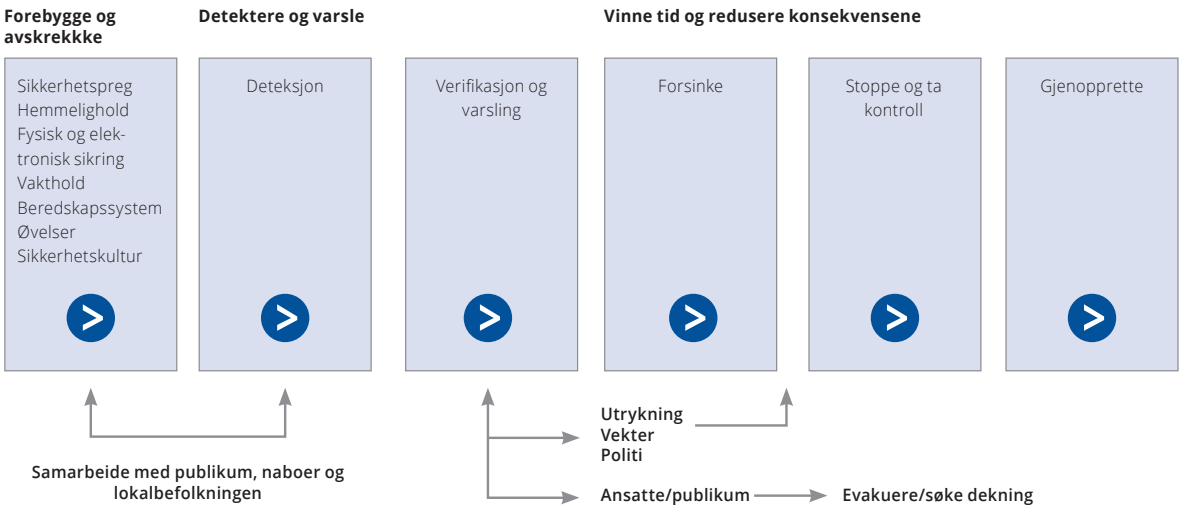
I Tabell 3 er det spesifisert en tilnærming til sikring for de ulike trusselscenarioene for ulike sykehusfunksjoner. Tallkodene som benyttes i tabellen har følgende betydning:

1. Basis grunnsikringskonsept forutsettes tilstrekkelig for å håndtere risiko
2. Grov scenariobasert sikringsrisikovurdering (jf. kap. 4.4)
3. Detaljert sikringsrisikovurdering (jf. kap. 4.1)

Sårbarhetsvurdering

Sårbarhet er generelt definert som «manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen» (SN, 2008). Sårbarhet er en graduell egenskap ved et system, dvs at den kan være lav, høy eller et sted imellom. I sårbarhetsvurderingen er målet derfor å kartlegge og beskrive graden av sårbarhet et system (lokasjonen, tomt, sykehuset, sykehusavdeling/-funksjon, delsystem m.v.) har ovenfor definerte trusselscenarioer.
I et system med høy sårbarhet vil det være enkelt for en trusselaktør å gjennomføre og lykkes med sine handlinger, om det så er å angripe en ansatt, bortføre et barn eller sabotere en viktig teknisk infrastruktur (vann, avløp, strøm, IKT). Hvis sykehuset har redundante tekniske infrastrukturer vil ikke handlingen nødvendigvis få store konsekvenser. Hvis sykehuset klarer å detektere at et barn er kidnappet, verifiserer handlingen, stenger ned avdelinger og sørger for rask reaksjon fra vektertjeneste eller politi vil også konsekvenser begrenses.

Sårbarheten vurderes som en kombinasjon av systemets iboende motstandsevne/robusthet (barrierer mellom trusselaktøren og verdiene), og systemets evne til å gjenopprette funksjonsevne etter en uønsket handling. Sistnevnte handler om i hvilken grad og hvor raskt virksomheten vil kunne gjenopprette viktige funksjoner dersom den uønskede handlingen ikke har latt seg stanse. I praksis skjer dette gjennom å erstatte eller reparere verdier/ressurser som er tapt eller ødelagt, eller å utnytte eventuell redundans i systemet. I vold- og trusselsituasjoner er det sårbarheten for de involverte menneskene (verdiene) som



Figur 9. Helhetlig sikring. Forebygge, avskrekke, forsinke, detektere, verifisere, varsle, utrykning, stoppe/ta kontroll og gjenopprette. Figur hentet fra Sikringshåndboka (NKSB, 2016: 18).

må vurderes, og ikke sykehussystemet i sin helhet.

Ved klassifisering av systemets robusthet og systemets evne til å gjenopprette funksjonsevne er det etablert en tredelt skala, hhv lav, middels og høy.
Rangering gjøres skjønnsmessig av analysegruppen for hvert spesifiserte trusselscenario. Dette kan gjøres direkte, basert på klassene i Tabell 4, eller på bakgrunn av en diskusjon av følgende sjekkpunkt:

1. Systemets robusthet/motstandsevne:

- **Barrierer:** Hvilke barrierer er etablert som vil yte motstand mot trusselaktøren i det aktuelle trusselscenarioet? Eksempelvis fysiske, elektroniske, organisatoriske og/eller menneskelige barrierer.
- **Barriereytelse:** Har den spesifiserte trusselaktøren kapasitet til å forsere sikkerhetstiltakene? En stor og bevæpnet psykiatrisk pasient har for eksempel stor kapasitet ovenfor en kropslig underlegen sykepleier.
- **Deteksjon:** Hvilke deteksjonsmuligheter fins, og vil hendelsen bli verifisert? Finnes det for eksempel voldsalarm eller videoovervåkning som vil kunne fange opp en hendelse?
- **Reaksjonsmuligheter:** Hvilke rutiner finnes for reaksjon når en hendelse inntreffer? Vil reaksjonsstyrken rekke fram i tide til å stanse trusselaktøren? Finnes det for eksempel en vektertjeneste eller en beredskapsplan som sørger for bistand fra andre avdelinger ved hendelse?
- **Sikkerhetskultur:** Hvordan er sikkerhetskulturen i virksomheten? Er virksomheten (eller tilsvarende virksomhet) kjent for å gjennomføre risikovurderinger, følge opp sikkerhetsrutiner og tenke sikkerhet i alle ledd?

2. Systemets evne til å gjenopprette funksjonsevne:

- **Redundans:** Er det etablert redundans for de viktigste funksjonene eller verdiene? Finnes det for eksempel flere systemer eller ressurser som kan ivareta samme funksjon, eller kan dette enkelt skaffes eksternt?
- **Beredskapsplaner:** Finnes det beredskapsplan for trusselscenarioet?

	Systemets robusthet	**Høy (3)**	**Middels (2)**	**Lav (1)**
Systemets evne til å gjenopprette funksjonsevne og/eller verdi	Høy (3)	**SVÆRT LAV**	**LAV**	**MODERAT**
	Middels (2)	**LAV**	**MODERAT**	**HØY**
	Lav (1)	**MODERAT**	**HØY**	**SVÆRT HØY**

SÅRBARHETS-KATEGORI	**BESKRIVELSE (basert på FEMA, 2011).**
SVÆRT HØY (5)	Ekstremt utsatt, ingen fysisk beskyttelse og/eller lang nedetid. Det finnes én eller flere store svakheter som gjør verdien ekstremt utsatt for en trusselaktør eller fare. Ingen redundans og fysisk beskyttelse og verdien/enheten i sin helhet vil være ute av funksjon i meget lang tid etter et angrep.
HØY (4)	Finnes en eller flere store svakheter som gjør verdien svært utsatt for en trusselaktør eller fare. Begrenset redundans og fysisk beskyttelse og verdien/enheten i sin helhet vil være ute av funksjon i lang tid etter et angrep.
MODERAT (3)	Finnes en viktig svakhet som gjør verdien noe utsatt for en trusselaktør eller fare. Mangelfull redundans og fysisk beskyttelse. Viktige deler av en enhet eller annen utsatt verdi kan være ute av funksjon i betydelig tid.
LAV (2)	En mindre svakhet er identifisert som gjør enheten/verdien litt utsatt for en trusselaktør eller fare. God redundans og fysisk beskyttelse slik at en hendelse kun vil ha en svært begrenset betydning for driften og/eller den utsatte verdien.
SVÆRT LAV (1)	Ingen kjente svakheter som kan utnyttes av en trusselaktør. Sterk redundans og fysisk beskyttelse slik at en hendelse har liten/ingen betydning for driften og/eller den utsatte verdien.

Tabell 4 Veiledende klassifisering av sårbarhet for trusselscenarioer.

Identifikasjon av sikringsrisiko omfatter å utarbeide en tydelig og omfattende liste over tenkelige uønskede trusselscenarioer.

Dette gjøres ved å kartlegge kritikaliteten til organisasjonens verdier (verdivurdering), vurdere potensielle risikokilder (trusselvurdering) og hvordan verdiene er beskyttet, forberedt eller organisert for å motstå trusselen (sårbarhetsvurdering).

Samlet risikoidentifikasjon

I denne veilederen er det etablert et sett med verdier og generiske trusselscenarioer som skal vurderes. Dette fremgår av Tabell 3 Konsekvens-/verdivurdering.

Stegene i analysen fremgår av analyseskjema i Tabell 5, og beskrives som følger:

1. **Velg analyseobjekt.** I tidligfase kan dette være én av flere lokasjoner. I en helhetlig risikovurdering (konseptfase, del 2 eller tidlig forprosjekt) vil dette typisk være geografiske eller funksjonelle avgrensninger, som sykehusfunksjoner/-avdelinger, bygninger, uteområder eller teknisk infrastruktur.
2. **Velg generisk trusselscenario fra Tabell 3.**
3. **Identifiser spesifikke trusselscenarioer.** Spesifikke trusselscenarioer er scenarioer som er spesielt for det enkelte prosjekt/system. Spesifikke trusselscenarioer er en kombinasjon av valgt trusselaktør og relevante verdier (ressurser, innsatsfaktorer) innenfor det valgte analyseobjektet.
4. **Beskriv systemets sårbarhet** i relasjon til det spesifikke trusselscenarioet og velg en sårbarhetsklasse i samsvar med Tabell 3.
5. **Beskriv mulige konsekvenser** av det spesifikke trusselscenarioet innenfor kategoriene «liv og helse», «operativ evne» og «omdømme». Her skal det tas utgangspunkt i en representativ konsekvens gitt scenarioet. Deretter må det legges vekt på å beskrive usikkerheten i utfallsrommet.
6. **Identifiser mulige risikoreduserende tiltak**. I denne fasen skal det legges vekt på at dette er mulige risikoreduserende tiltak. Det skal ikke tas stilling til hvilke tiltak som skal implementeres eller ikke.
7. **Gjenta steg 2-6 til alle generiske trusselscenarioer er analysert for det valgte analyseobjektet.**
8. **Gjenta steg 1-7 for et nytt analyseobjekt til alle analyseobjektene er analysert.**

Informasjonen samles i et analyseskjema, jf. Tabell 5.

ID	Generisk trusselscenario	Spesifikt trusselscenario (trusselaktør og verdi)	Beskrivelse av systemets/ analyseobjektets sårbarhet	Sårbarhets-klasse	Beskrivelse av konsekvenser for: Liv og helse Operativ evne (pasientbehandling og diagnostisering) Omdømme	Mulige risikoreduserende tiltak
Analyseobjekt 1: Psykiatri poliklinikk						
1A	Trusler og fysisk vold mot personer på sykehuset.	Psykisk ustabil pasient angriper sykepleier med kniv.	Ingen fysiske barrierer. Ansatte har voldsalarm. Videoovervåkning i fellesarealer. Vektertjeneste.	**HØY**	Stor fare for alvorlig skade og/eller omkomne. Liten fare for langvarig nedsatt operativ evne. Vil medføre nasjonal media-oppmerksomhet.	Fluktveier fra behandlingsrom. Utadslående dører i behandlingsrom.
1B		Pårørende til pasient er misfornøyd med behandling og truer med fysisk vold.	[kvalitativ beskrivelse]	**MEGET LAV til MEGET HØY**	[kvalitativ beskrivelse]	[kvalitativ beskrivelse]
1C		...				
Analyseobjekt 2: Psykiatri sengepost						
2A	Trusler og fysisk vold mot personer på sykehuset.	Psykisk ustabil pasient angriper sykepleier med kniv.	[kvalitativ beskrivelse]	**MEGET LAV til MEGET HØY**	[kvalitativ beskrivelse]	[kvalitativ beskrivelse]
2B		Pårørende til pasient er misfornøyd med behandling og truer med fysisk vold.	[kvalitativ beskrivelse]	**MEGET LAV til MEGET HØY**	[kvalitativ beskrivelse]	[kvalitativ beskrivelse]
2C		...				
Analyseobjekt 3: Teknisk infrastruktur						
3A	Planlagt og målrettet fysisk angrep mot kritisk funksjon eller infrastruktur.	Misfornøyd ansatt saboterer avløpssystemet.	[kvalitativ beskrivelse]	**MEGET LAV til MEGET HØY**	[kvalitativ beskrivelse]	[kvalitativ beskrivelse]
3B		Terrorgruppe plasserer bilbombe inntil sykehusets trafostasjoner.	[kvalitativ beskrivelse]	**MEGET LAV til MEGET HØY**	[kvalitativ beskrivelse]	[kvalitativ beskrivelse]

Tabell 5 Veiledende klassifisering av sårbarhet for trusselscenarioer.

4.1.3 Risikoanalyse

Risikoanalyse inkluderer vurdering av sannsynlighet og konsekvenser for hvert identifiserte trusselscenario og fastsette risikonivå.

Målet med risikoanalysen er å:

A. Definere konsekvensene av et trusselscenario og tilhørende usikkerhet. Dette oppnås ved å vurdere:

I. Sannsynlighet: grad av tro knyttet til at scenarioet inntreffer, basert på all tilgjengelig bakgrunnskunnskap (f.eks. frekvensdata, ekspertvurderinger, forskningsrapporter, offentlige nasjonale trusselvurderinger, lokale trusselvurderinger m.m.).

II. Konsekvens: Hvordan verdier/virksomheten påvirkes dersom hendelsen inntreffer (konsekvenser kan uttrykkes kvalitativt eller kvantitativt og kan være sikker eller usikker og ha positiv eller negativ effekt). Det kan være flere mulige utfall av en hendelse (usikkerhet i konsekvensbildet).

III. Usikkerhet i bakgrunnskunnskap: Beskrivelse av kunnskapsstyrke for den bakgrunnskunnskapen som er benyttet for fastsettelse av sannsynligheter og konsekvenser. Dette har i praksis betydning for vekten sikringsrisikovurderingen skal tillegges, sammenlignet med annet beslutningsunderlag, når beslutninger om sikring skal tas

B. Etablere et risikobilde for virksomheten, f.eks. presentert gjennom en risikomatrise. Det overordnede risikonivået bestemmes ved å kombinere sannsynlighets- og konsekvensvurderingen.

Ved fastsettelse av sannsynligheter og konsekvenser for trusselscenarioene må informasjonen fra forrige steg (risikoidentifikasjonen) benyttes. Dette er illustrert i Figur 6 i kapittel 4.1.
Verdi-, trussel- og sårbarhetsvurderingen er det sentrale grunnlaget for risikoidentifikasjonen. Videre er trusselvurderingen, herunder trusselaktørens intensjon og kapasitet, et viktig grunnlag for sannsynlighetsvurderingen. Verdivurderingen er grunnlaget for konsekvensvurderingen. Sårbarhetsvurderingen gir grunnlag for å vurdere effekten av planlagte/besluttede tiltak, og er et viktig grunnlag for fastsettelse av både sannsynlighet og konsekvenser for trusselscenarioene.

Trusselnivå for trusselscenario

Tabell 6 gir en beskrivelse av fem trusselnivåer og hvordan de kan forstås. Trusselnivåene uttrykker analysegruppens grad av tro om trusselscenarioet vil inntreffe i løpet av sykehusbyggets normerte levetid, her definert som 50 år.

Tabell 6 kan brukes direkte til å bestemme trusselnivå. Alternativt kan trusselnivå bestemmes ved å se nærmere på:

1. Fremtidsperspektivet: Trusselaktørens egenskaper knyttet til kapasitet og intensjon.
2. Historisk trusselnivå.

Først gjøres det en vurdering av trusselaktørens egenskaper ved å vurdere trusselaktørens intensjon og kapasitet ovenfor den definerte verdien, jf. Tabell 7. Deretter gjøres det en vurdering av historisk trusselnivå, dvs hvor ofte hendelsen har inntruffet historisk sett i sykehussektoren. Kombinasjonen av dette gir en samlet klassifisering av sannsynlighet for trusselscenarioet, jf. Tabell 7.

Trusselnivå	Beskrivelser	Sannsynlighet for å inntreffe i løpet av normert levetid (50 år)
Svært lavt (1)	Kjenner ingen tilfeller. Det er svært lite sannsynlig at hendelsen vil skje i løpet av sykehusets levetid.	Mindre enn 5 %
Lavt (2)	Har hørt om enkelttilfeller. Det er mindre sannsynlig at hendelsen skjer, enn at den skjer, i løpet av sykehusets levetid.	5 % – 30 %
Moderat (3)	Kjenner enkelttilfeller fra egen erfaring. Det er omtrent like sannsynlig at hendelsen skjer som at den ikke skjer, i løpet av sykehusets levetid.	30 % - 70 %
Høyt (4)	Kan inntreffe (mange tilfeller i vår bransje). Det er mer sannsynlig at hendelsen skjer, enn at den ikke skjer, i løpet av sykehusets levetid.	70 % - 95 %
Svært høyt (5)	Må forventes å inntreffe. Det er meget stor sannsynlighet for (nesten sikkert) at hendelsen vil skje i løpet av sykehusets levetid.	Over 95 %

Tabell 6 Trusselnivå for trusselscenarioer

Trusselnivå i et fremtidsperspektiv bestemmes på bakgrunn av trusselaktørens egenskaper knyttet til kapasitet og intensjon. En aktør med stor kapasitet forventes å kunne være tilstede hvor som helst. Aktørens målvalg kobles til aktørens intensjon. Målvalg handler om trusselaktørens valg av akkurat ditt objekt blant en rekke potensielle mål.

Historisk trusselnivå kobles til erfaringene med tilsvarende, eller lignende, handlinger i sykehus. Noen handlinger, f.eks. at ansatte blir angrepet av pasienter skjer ofte/daglig i norske sykehus. Andre handlinger, for eksempel terroraksjoner mot sykehus, finnes det ingen erfaring med i Norge, men vi kjenner eksempler fra andre vestlige land.

Intensjon	Kapasitet		
	Lav (1)	Betydelig (2)	Stor (3)
Lav (1)	**Svært lavt**	**Lavt**	**Moderat**
Betydelig (2)	**Lavt**	**Høyt**	**Høyt**
Sterk (3)	**Moderat**	**Svært høyt**	**Svært høyt**
Beskrivelse av kategorier			
Intensjon			
Sterk (3)	Det forutsettes at aktøren har stor vilje til og/eller ønske om handling. Det konkrete sykehuset og tilhørende verdier/enheter antas å være et relevant målvalg for aktøren hvis flere valg eksisterer.		
Betydelig (2)	Det forutsettes at aktøren har vilje til og/eller ønske om handling. Det konkrete sykehuset eller tilhørende verdier/enheter antas ikke å være primært målvalg for aktøren hvis flere målvalg eksisterer, men det kan ikke utelukkes.		
Lav (1)	Det forutsettes at aktøren i utgangspunktet ikke har vilje til og/eller ønske om handling.		
Kapasitet			
Stor (3)	Aktøren forutsettes å ha stor tilegnet, antatt eller demonstrert evne ovenfor den aktuelle verdien. Aktøren forutsettes å ha betydelige taktiske og operative ressurser.		
Betydelig (2)	Aktøren forutsettes å ha moderat tilegnet, antatt eller demonstrert evne ovenfor den aktuelle verdien. Aktøren forutsettes å ha begrensede taktiske og operative ressurser.		
Lav (1)	Aktøren forutsettes å ha begrenset tilegnet, antatt eller demonstrert evne ovenfor den aktuelle verdien. Aktøren forutsettes å ha begrensede taktiske og operative ressurser.		

Tabell 7 Vurdering av trusselnivå basert på trusselaktørens egenskaper (fremtidsperspektivet)

	Trusselnivå i et fremtidsperspektiv				
Historisk trusselnivå	Meget lavt (1)	Lavt (2)	Moderat (3)	Høyt (4)	Svært høyt (5)
1: Kjenner ikke til lignende hendelse i sykehus, men har skjedd i andre virksomheter i vestlige land.	**1 Svært lavt**	**1 Svært lavt**	**2 Lavt**	**3 Moderat**	**4 Høyt**
2: Har skjedd på lignende Sykehus/enheter i andre vestlige land, men kjenner ikke til hendelse på norske sykehus.	**1 Svært lavt**	**2 Lavt**	**3 Moderat**	**4 Høyt**	**5 Svært høyt**
3: Skjer av og til på enheter/ avdelinger i norske sykehus.	**2 Lavt**	**3 Moderat**	**4 Høyt**	**5 Svært høyt**	**5 Svært høyt**
4: Skjer jevnlig på enheter/ avdelinger i norske sykehus.	**3 Moderat**	**4 Høyt**	**4 Høyt**	**5 Svært høyt**	**5 Svært høyt**

Tabell 8. Vektet trusselnivå basert på trusselaktørens egenskaper og historisk trusselnivå.

To eksempler på bruk av metoden:

Trusselscenario A: Voldshandling, hvor en psykotisk pasient (uten våpen) angriper en ansatt på en lukket avdeling for psykisk helsevern.

Pasientens intensjon om å utføre vold mot den ansatte (verdien) vurderes som «betydelig». Tilsvarende vurderes pasientens kapasitet ovenfor den ansatte (verdien) som «betydelig». Den ansatte og pasienten vurderes å være relativt jevnbyrdige kapasitetsmessig.
Ser vi på statistikk for denne typen handling, finner vi at denne typen hendelser skjer jevnlig i norske sykehus. Kombinasjonen av trusselnivå i et fremtidsperspektiv og historisk trusselnivå gir trusselnivå «svært høyt».

Her ser vi at det historiske trusselnivået bidrar til å heve trussel-/sannsynlighetsnivået fra «høyt» til «svært høyt».

Trusselscenario B: Terrorangrep med kjøretøybombe mot resepsjonsområdet i et sykehus.
Intensjonen for aktuelle trusselaktører (terrorister) vurderes som «lav» ovenfor norske sykehus slik vi vurderer situasjonen i Norge i dag. Det vil si at vi ikke forventer at trusselaktørene vil rette sine handlinger mot dette sykehuset. Det finnes mer naturlige målvalg for trusselaktørene.
Kapasiteten til eventuelle trusselaktører vurderes for øvrig som «stor». Når vi ser på statistikken finner vi ikke denne typen handlinger i norske sykehus, men lignende scenarioer har skjedd ved sykehus i andre vestlige land (York & MacAlister, 2015:53).

Kombinasjonen av trusselnivå i et fremtidsperspektiv og historisk trusselnivå gir trusselnivå «moderat».

Konsekvensvurdering

Tabell 9 gir et eksempel på konsekvensklassene innenfor verdikategoriene «liv og helse», «operativ evne» og «omdømme». Informasjon og klassifiseringen fra sårbarhetsvurderingen er et viktig grunnlag for å vurdere konsekvensklasse (se figur 6).

Nivå	Beskrivelse, liv og helse	Beskrivelse, operativ evne	Beskrivelse, omdømme
Katastrofal (5)	Flere omkomne.	Sykehuset kan ikke utføre sine oppgaver innenfor enkelte eller flere områder som følge av en uforutsett hendelse. Umiddelbart fare for tap av flere liv pga følgehendelser.	Meget store politiske og nasjonalt destabiliserende konsekvenser. Tap av all tillit, som fører til at pasienter og henvisende instanser velger bort sykehuset. Sykehuset settes under administrasjon.
Svært høy (4)	Svært store skader på èn eller flere personer som medfører lengre sykefravær, varige mèn og/eller død.	Alvorlig svikt eller stans i en eller flere lovpålagte livsviktige medisinske tjenester. Fare for tap av liv pga følgehendelser.	Omdømmet for sykehussektoren er omfattende skadet, alvorlig fravær av tillit. Pasienter og henvisende instanser starter å velge bort sykehuset.
Høy (3)	Store skader på èn eller flere personer som medfører lengre sykefravær og/eller varige mèn.	Tjenesten blir utført, men med betydelig svekket kvalitet. Det er brudd på retningslinje/prosedyre som kan sette liv og helse i fare.	Omdømme skades alvorlig, nasjonal negativ mediedekning, redusert tillit. Brudd på god praksis, som kan sette liv og helse i fare.
Moderat (2)	Skader på èn eller flere personer som medfører sykefravær og/eller behov for behandling i etterkant.	Kvalitetsforringelse på tjenesten. Noen tjenester kan ikke utføres innen akseptabelt tidsrom. Indikasjoner på at retningslinje/ prosedyre ikke følges i tilstrekkelig grad. Langvarig situasjon medfører store utfordringer knyttet til behandling av pasienter, men ingen umiddelbar fare for tap av liv pga følgehendelser.	Omdømme kan alvorlig skades. Kortvarig og lokal negativ eksponering. Kan medføre redusert tillit.
Lav (1)	Ubetydelige til mindre skader på personer. Medfører ikke sykefravær eller behov for behandling i etterkant.	Tjenesten blir vanskelig eller uvanlig arbeidskrevende å utføre. Langvarig situasjon kan medføre utfordringer knyttet til behandling av pasienter, men ingen fare for tap av liv pga følgehendelser.	Ubetydelig negativ eksponering.

Tabell 9. Konsekvensklasser for "liv og helse", "operativ evne" og "omdømme".

ID	Generisk trussel-scenario	Spesifikt trussel-scenario (trusselaktør og verdi)	Trussel-nivå (iht Tabell 6)	Konsekvensklasse: representativ konsekvens for trussel-scenarioet (iht. Tabell 9)			Beskrivelse av usikkerhet
				Liv og helse	Operativ evne	Omdøm-me	
Analyseobjekt 1: Psykiatri poliklinikk							
1A	Trusler og fysisk vold mot personer på sykehuset.	*Psykisk ustabil pasient angriper sykepleier med kniv.*	***MODE-RAT***	***SVÆRT HØY***	***LAV***	***MODE-RAT***	*Svært farlig situasjon hvor flere ansatte og pasienter med små variasjoner i scenarioeti kan bli alvorlig skadet eller drept. Usikkerhet knyttet til triggere for scenarioet og tilgang på våpen. Vold mot ansatte skjer regelmessig på avdelinger for psykisk helsevern, men sjeldnere med kniv/våpen slik dette scenarioet beskriver. Sterkt kunnskapsgrunnlag (statistikk) knyttet til hendelsen.*
1B		*Pårørende til pasient er misfornøyd med behandling og truer med fysisk vold.*	VELG: SVÆRT LAVT til SVÆRT HØYT	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	[kvalitativ beskrivelse]
1C							
Analyseobjekt 2: Psykiatri sengepost							
2A	Trusler og fysisk vold mot personer på sykehuset.	*Psykisk ustabil pasient angriper sykepleier med kniv.*	VELG: SVÆRT LAVT til SVÆRT HØYT	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	[kvalitativ beskrivelse]
2B		*Pårørende til pasient er misfornøyd med behandling og truer med fysisk vold.*	VELG: SVÆRT LAVT til SVÆRT HØYT	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	[kvalitativ beskrivelse]
2C							
Analyseobjekt 3: Teknisk infrastruktur							
3A	Planlagt og målrettet fysisk angrep mot kritisk funksjon eller infrastruktur.	*Misfornøyd ansatt saboterer avløpssystemet.*	VELG: SVÆRT LAVT til SVÆRT HØYT	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	[kvalitativ beskrivelse]
3B		*Terrorgruppe plasserer bilbombe inntil sykehusets trafostasjoner.*	VELG: SVÆRT LAVT til SVÆRT HØYT	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	VELG: LAV til KATA-STROFAL	[kvalitativ beskrivelse]

Tabell 10 Analyseskjema risikoanalyse (eksempler vist med kursiv tekst)

Samlet risikoanalyse og beskrivelse av usikkerhet

En samlet risikoanalyse består av følgende steg:

1. Angi trusselnivå for hvert spesifikke trusselscenario. Informasjon fra sårbarhetsvurderingen er relevant å benytte ved fastsettelse av trusselnivå.
2. Angi konsekvensklasse for hhv «liv og helse», «operativ evne» og «omdømme». Informasjon fra sårbarhetsvurderingen er relevant å benytte ved fastsettelse av konsekvensklasse.
3. Beskriv usikkerhet, for eksempel i utfallsrommet for mulige konsekvenser av et trusselscenario og tilgjengelig bakgrunnskunnskap.

	Konsekvensklasse				
Trusselnivå (sannsynlighet for hendelsen)	**Lav (1)**	**Moderat (2)**	**Høy (3)**	**Svært høy (4)**	**Katastrofal (5)**
(5) Meget høyt: Det er meget stor sannsynlighet for (nesten sikkert) at hendelsen vil skje i løpet av sykehusets levetid, P > 0,95.					
(4) Høyt: Det er mer sannsynlig at hendelsen skjer, enn at den ikke skjer, i løpet av sykehusets levetid, P = [0,95 – 0,7].					
(3) Moderat: Det er omtrent like sannsynlig at hendelsen skjer som at den ikke skjer, i løpet av sykehusets levetid, P = [0,7 – 0,3].	**1A2**	**1A3**		**1A1**	
(2) Lavt: Det er mindre sannsynlig at hendelsen skjer, enn at den skjer, i løpet av sykehusets levetid, P = [0,3 – 0,05].					
(1) Meget lavt: Det er svært lite sannsynlig at hendelsen vil skje i løpet av sykehusets levetid, P < 0,05.					

Fortolkning av farger/risikoaksept	
Akseptabel risiko (1)	Risikonivået er ubetydelig og kostnaden for ytterligere risikoreduksjon vil normalt være svært lite kostnadseffektivt.
Tolererbar risiko (ALARP-område) (2)	Risikonivået i dette område kan tolereres hvis ytterligere risikoreduksjon er upraktisk eller vurderes som lite kostnadseffektivt (ALARP-område).
Høy risiko (3)	Risikonivået i dette området regnes som høy. Risiko må reduseres med forebyggende tiltak.
Svært høy risiko (4)	Risikonivået i dette området regnes som svært høy.Risiko må reduseres uavhengig av kostnad med både forebyggende og konsekvensreduserende tiltak.

Tabell 11 Risikomatrise.

4.1.4 Risikoevaluering

Trusselscenarioene kan visualiseres i en risikomatrise som vist i Tabell 11. Her er eksempelscenario 1A fra Tabell 10 plottet inn i matrisen. Scenarioet er plassert tre steder i matrisen for å illustrere at hendelsen har ulike konsekvenser for hhv liv og helse (1A1), operativ evne (1A2) og omdømme (1A3).
Scenarioet medfører en betydelig risiko knyttet til liv og helse (1A1), og er plassert i «ALARP-området». Risikoreduserende tiltak må derfor vurderes. Se kap. 4.5 for mer informasjon og veiledning i anvendelse av ALARP-prinsippet.

Risikomatrisen er en veiledning til hvordan trusselscenarioer kan evalueres med hensyn til risikonivå og behov for risikoreduserende tiltak. Hensikten er å bidra til å rette søkelyset mot scenarioer og tiltak som krever særskilt oppfølging, men ikke å automatisere beslutninger om risikoaksept. Risikomatrisen må derfor avstemmes med prosjekteier før den legges til grunn.

4.1.5 Risikohåndtering

Prosjekteier er ansvarlig for risikohåndteringen, som ligger utenfor selve risikovurderingsprosessen, jf. Figur 6. Risikohåndtering omfatter i denne sammenheng å beslutte hvilke risikoreduserende tiltak som skal implementeres på bakgrunn av risikovurderingen, samt oppfølgingen av disse tiltakene. I tillegg til føringene fra risikoevalueringen beskrevet i kap. 4.1.4 må helseforetakets system for helhetlig risiko-/sikkerhetsstyring legges til grunn for risikohåndteringen.

Tiltak som ikke er aktivt forkastet basert på en risikoinformert beslutning skal inngå i prosjektets sikringskonsept. Se kap. 4.6 for forslag til innholdsfortegnelse i sikringskonsept.

4.2 Innhold i en systembeskrivelse.

En detaljert systembeskrivelse omfatter typisk en beskrivelse av følgende:

- **Geografisk avgrensning av systemet og beskrivelser av lokasjon og omgivelser.**
  - Beskrivelse av geografisk område defineres som en sykehuslokasjon, og som legges til grunn når det gjennomføres en risikovurdering av ulike lokasjoner.
  - Naturomgivelser og eventuell naturfare.
  - Avstander/responstid for politi og brannvesen.
  - Kommunal infrastuktur, herunder: veger, strøm, vann, kloakk, mv.
  - Risikokilder i nærmiljø, herunder: trusselutsatte bygninger, industrianlegg, offentlig kommunikasjon, rusmiljø, kriminalitetsbelastede områder m.v.
- **Funksjonelle avgrensninger:**
  - Beskrivelse av hvilken type sykehus som skal planlegges og hvorvidt sykehuset har lokale, regionale og/eller nasjonale funksjoner.
  - Beskrivelse av hvilke funksjoner sykehuset har.
- **Tekniske avgrensninger**
  - Forutsetninger knyttet til plassering av funksjoner eller rom.
  - Forutsetninger om hvilke tekniske sikringstiltak er forutsatt når risikovurderingen gjennomføres.
- **Organisatoriske avgrensninger**
  - Hvilke organisatoriske forutsetninger legges til grunn for risikovurderingen, herunder: bemanning, vaktordninger, profesjonell vekter-/vakttjeneste, spesielle rutiner/prosedyrer m.m.?
- **Menneskelig avgrensninger**
  - Hvilke menneskelige forutsetninger legges til grunn for risikovurderingen, for eksempel knyttet til ansattes kompetanse eller trening i håndtering av voldshendelser?
- **Interne og eksterne avhengigheter**
  - Beskrivelse av interne avhengigheter. Hensikten er å avdekke om enkelte funksjoner eller ressurser er spesielt viktige for å kunne gjennomføre andre funksjoner i drifts- og beredskapssituasjoner.
  - Beskrivelse av eksterne avhengigheter. Hensikten er å avdekke om sykehuset er avhengig av spesielle eksterne ressurser for å opprettholde en kvalitetsmessig god drift og/eller beredskap.

4.3 Sjekkliste for sikring i prosjektinnramming

Sjekklisten nedenfor anbefales benyttet som utgangspunkt for å vurdere sikringsbehov i prosjektinnrammingsfasen. I mange tilfeller vil det være lite informasjon om konkret prosjektinnhold på dette tidspunktet. Vurderingene av sikring må tilpasses dette. Hensikten med vurderingene i prosjektinnrammingen er først og fremst å identifisere særtrekk ved prosjektet og legge løpet for det videre arbeidet med sikring og risikostyring i prosjektet.

Det er også viktig å vurdere behovet for informasjonssikkerhet i prosjektet på dette stadiet, slik at ikke beskyttelsesverdig informasjon kommer på avveie.

TEMA	J/N	KOMMENTARER/BESKRIVELSER
Verdier		
Vil sykehuset kunne ivareta funksjoner med lovpålagte sikringskrav? *Eksempler: Forsvarsinstallasjoner; skjermingsverdige objekt; strålevern; informasjon, informasjonssystemer, objekter eller infrastruktur som understøtter grunnleggende nasjonale funksjoner.*		
Vil sykehuset kunne ivareta funksjoner med kjente sikringsbehov? *Eksempler: Akuttmottak, (nærhet til) legevakt, spesielt psykisk helsevern, atom-/protonsenter, HOT-lab, spesielle isolater for smittevern (nivå 4-isolater), CBNe-senter*		
Vil sykehuset kunne ivareta viktige regionale og/eller nasjonale funksjoner? *Eksempler: Som over, men kan også omfatte ordinære sykehusfunksjoner av stor regional og/eller nasjonal viktighet.*		
Trusler *Lokalt politi bør involveres i vurderingene så langt det er mulig.*		
Er det tenkelig at sykehuset verdier, jf. kartlegging ovenfor, utløser spesielle trusler?		
Vil sykehuset kunne omfatte trusselutsatte funksjoner, som akuttmottak og psykisk helsevern?		
Vil sykehuset kunne plasseres i et område med særlige kriminalitetsutfordringer?		
Sårbarheter		
Representerer prosjektet en ny måte å bygge og/eller drifte sykehus? (begrenset erfaring) *Ny teknologi, nye arbeidsmetoder, nye prosjektmodeller, nye kontraktsformer, nye funksjoner m.m. kan medføre ukjente sårbarheter og risiko.*		
Omfatter prosjektet et stort antall ulike funksjoner, ansatt- og pasientgrupper? *Store og komplekse sykehus kan medføre uoversiktlige og ukjente sårbarheter sammenlignet med mindre og mer oversiktlige sykehus.*		
Omfatter prosjektet særskilt sårbare verdier? *Ressurser/innsatsfaktorer under kategoriene liv/helse, operativ evne og omdømme*		
Berøres prosjektet av særlige utfordringer knyttet til teknisk infrastruktur i området? *Kjente områderelaterte utfordringer knyttet til opprettholdelse av strømforsyning, vannforsyning, avløp, overvann, IKT, atkomstveier m.m.*		
Omfatter prosjektet særlige utfordringer knyttet til å etablere effektive barrierer mellom trusler og utsatte verdier?		

TEMA	J/N	KOMMENTARER/BESKRIVELSER
Avklaring av lokalisering		
Vil sikringsrelaterte problemstillinger kunne tenkes å påvirke lokalisering av sykehuset? *Hvis «ja» bør det gjennomføres tilpasset arbeid med sikring i fasen «Avklaring lokalisering». Eksempelvis sikkerhetspsykiatri, akuttmottak, forsvarsinstallasjoner, nukleær aktivitet m.m.*		
Vil lokalisering av sykehuset kunne påvirke sikringskonseptet? *Hvis «ja» bør det gjennomføres tilpasset arbeid med sikring i fasen «Avklaring lokalisering». Eksempelvis nærhet til: kommunal legevakt; områder med høy kriminalitetsrate; «storulykkevirksomhet»; trusselutsatte offentlige virksomheter m.m.*		
I hvilken grad gir potensielle lokasjoner anledning til å etablere trinnvis opptrapping av beredskapen, som beskrevet for beredskapstrinn ALFA-DELTA i Sivilit Beredskapssystem (SBS), på en effektiv måte? *Det må minimum gjøres en avsjekk mot anbefalte tiltak spesifisert i SBS, og vurdere hvordan og i hvilken grad potensiell lokasjon muliggjør effektuering av tiltakene. Viktige forhold er muligheten til å utøve kontroll og begrense atkomst til sykehusområdet og i sykehuset. Et annet viktig forhold som må vurderes er lokasjonens avstand til militære mål.*		
Informasjonssikkerhet i prosjektet		
I hvilken grad omfatter prosjektet verdier (informasjon, objekter m.m.) som ved tap av konfidensialitet, integritet og/eller tilgjengelighet kan medføre betydelige konsekvenser for sykehusets evne til å ivareta liv og helse, operativ evne og/eller omdømme? *Kritikalitetsnivåer for informasjonssikkerhetsplan: normal, hevet (f.eks. referanse til beskyttelsesinstruksen), begrenset/sikkerhetsloven.*		
Er det vurdert hvordan regionale IKT-foretak/enheter (Sykehuspartner HF, Helse Vest IKT, HMIT eller Helse Nord IKT) kan bistå i planleggingen av informasjonssikkerhet i prosjektet?		

Tabell 12 Sjekkliste for sikring i prosjektinnramming

4.4 Arbeidsskjema for sammenlignende/ komparativ risikovurdering (konseptfase, del 1)

Hensikten med sikringsrisikovurderingene i konseptfase del 1 er å finne forskjeller mellom alternativene, identifisere kritiske sårbarheter og viktige risikoreduserende tiltak som det må arbeides videre med i påfølgende faser (for det alternativet som velges). Analyseskjemaet nedenfor representerer et minimumsnivå av hva som bør utføres. Analysen må bygge på en systembeskrivelse for de aktuelle konseptene, jf. kap. 4.2. Det må også gjøres en vurdering av om de generiske trusselscenarioene er relevante og tilstrekkelige for å avdekke forskjeller.

		Konsept A			Konsept B		
ID	**Scenario**	**Årsaker og sårbarheter**	**Anbefalte tiltak**	**Risikovurdering**	**Årsaker og sårbarheter**	**Anbefalte tiltak**	**Risikovurdering**
1	Trusler og fysisk vold mot mennesker på sykehuset	[kvalitativ beskrivelse, fri tekst]	[anbefalte tiltak hvis dette konseptet velges]	[Lav - Medium - Høy]	[kvalitativ beskrivelse, fri tekst]	[anbefalte tiltak hvis dette konseptet velges]	[Lav - Medium - Høy]
2	Hærverk/ skadeverk på utstyr, bygning m.m.						
3	Tyveri av utstyr, eiendeler, medisiner, informasjon m.m.						
4	Fremsettelse av trusler om alvorlig handling mot sykehuset						
5	Selvskading på sykehuset						
6	Rømning fra sykehuset						
7	Frihetsberøvelse på sykehuset						
8	Offentlig uro (f.eks. demonstrasjon) på sykehusets eiendom						
9	Fysisk angrep (uautorisert tilgang) på digitale systemer: informasjons-tyveri, sabotasje						
10	Planlagt og målrettet fysisk angrep mot personer						
11	Planlagt og målrettet fysisk angrep mot kritisk funksjon eller infrastruktur						
12	Annet?						

Tabell 13 Analyseskjema for konseptfase del 1.

4.5 Veiledning til ALARP-prinsippet

Risikoaksept bør generelt baseres på ALARP-prinsippet, som går ut på at man skal redusere risikonivået til et så lavt nivå som er forsvarlig og praktisk gjennomførbart. Hvorvidt en virksomhet velger å gå langt i retning av neglisjerbar risiko, eller eventuelt velge å leve med en risiko opp mot øvre akseptable grense, kan f.eks. avhenge av:

- Forventninger knyttet til risikoreduksjon av et tiltak, forventede følger av å akseptere en risiko eller forventet effekt av å akseptere en spesifikk risiko (mulighetene, for eksempel kostnadsbesparelser, som kan ligge i å ta/akseptere risiko).
- Grense for hhv neglisjerbar og øvre akseptable risiko og hvor nært risikoen i virksomheten ligger disse grensene. Det er ofte lite kostnadseffektivt å redusere en allerede lav risiko, sammenlignet med å fokusere på områder hvor risikoen er høy.
- Nødvendige handlinger eller konsekvenser for virksomheten dersom de ikke følger formelle risikoakseptkriterier. Her ligger det potensial for direkte ulykker og tap, samt tap av omdømme.

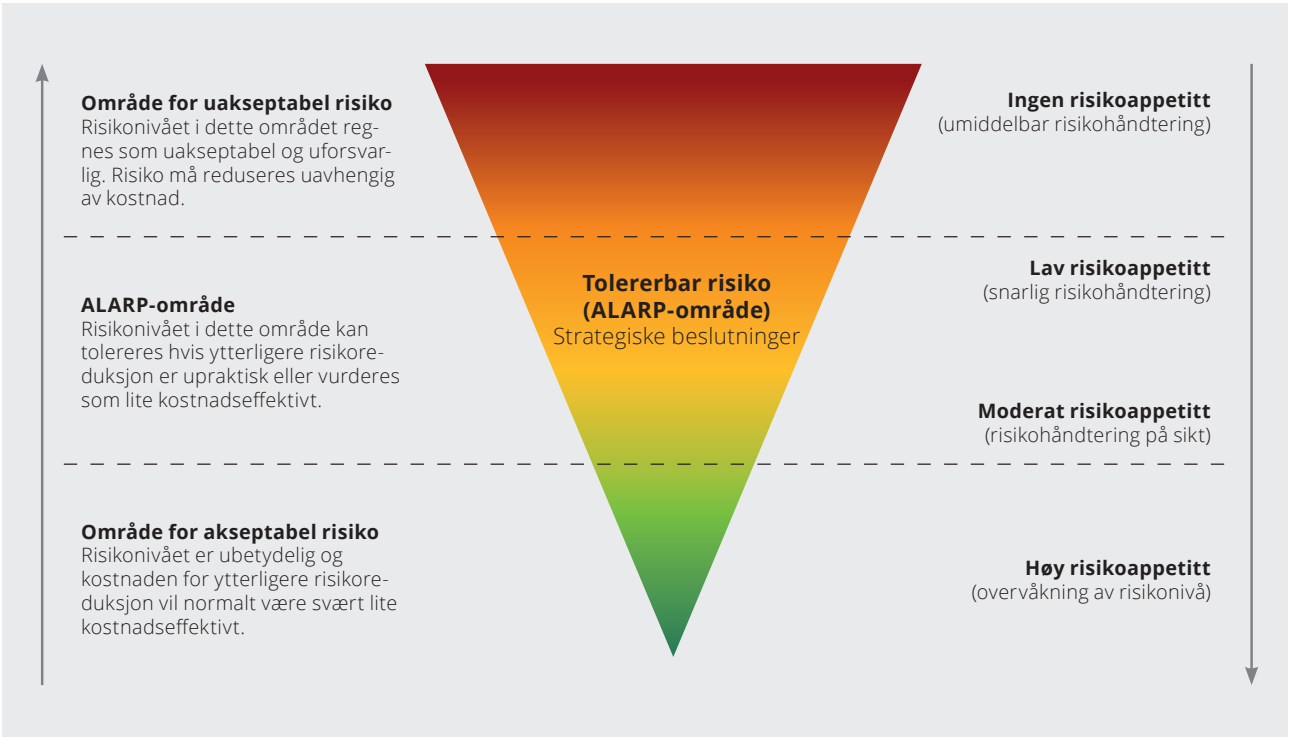
Grunnlaget for å gjennomføre en ALARP-prosess er alle de mulige risikoreduserende tiltakene som er listet opp i forbindelse med risikoidentifiseringen. Tiltak kan også komme fra andre steder, for eksempel forskrifter, veiledninger, god praksis m.m.

De forskjellige tiltakene vurderes nærmere og følges opp som en del av ALARP-prosess (As Low As Reasonably Practicable). Prosessen dokumenteres i et eget ALARP-register. Tabell 1j er et eksempel på et ALARP-register. Konklusjonen fra ALARP-prosessen kan være at tiltak forkastes, at tiltak er under vurdering, at tiltak implementeres, eller at de videreføres til neste fase. For å sikre kontinuitet overleveres ALARP-registeret alltid til neste prosjektfase.

For å vurdere hvorvidt et tiltak bør anbefales implementert i en ALARP-prosess kan følgende kriterier anvendes:

- **God praksis:** Tiltaket er helt vanlig på norske sykehus, dvs regnes som god praksis innen sikring av sykehus.
- **Risikoreduserende effekt:** Tiltaket har en sterk risikoreduserende effekt på enkeltscenarioer eller en bred risikoreduserende effekt (virker på flere trusselscenarioer). Særlig relevant hvis tiltaket har risikoreduserende effekt på scenarioer med storulykkepotensial. Tabell 14 gir et eksempel på hvordan tiltak kan analyseres med hensyn på å vurdere effekt mot ulike scenarioer samt funksjoner (barriere-, deteksjons-, verifikasjons- og/eller reaksjonsfunksjon).
- **Kostnad:** Skjønnsmessig vurdering av kostnaden ved tiltaket. Dette omfatter særlig de økonomiske konsekvensene av tiltaket, men kan også omfatte andre ulemper, for eksempel funksjonelle eller estetiske ulemper.

Tabell 15 er et annet eksempel på verktøy for å vurdere egnetheten av et risikoreduserende tiltak. Et tiltak som har mange funksjoner og virker mot mange scenarioer vil ofte være å foretrekke foran tiltak med få funksjoner og med virkning mot få scenarioer.



Figur 10 ALARP-prinsippet.

ID	Prio	Tiltak	Barriere	Deteksjon	Verifikasjon	Reaksjon	Administrative	Scenario 1	Scenario 2	...	Scenario 11
1		Alarmorganisering (deteksjon, varsling og reaksjon).		X	X						
2		Innbruddsalarm. Iht krav i NS EN 50131 og/eller eventuell FG-godkjenning.		X				X	X	X	X
3		Perimetersikring: Forhindre parkering eller ferdsel med kjøretøy tett inntil bygningen.	X	X	X			X		X	
..		...									

Tabell 14. Eksempel på kartlegging av tiltak som underlag for prioritering. Koble mot tiltakets funksjoner og bredde (treffsikkerhet) mot ulike scenarioer.

Tiltak			**Status**				**Oppfølging**		
ID	**Kort beskrivelse av tiltak**	**Referanse** (Angi hvor tiltaket ble foreslått eller er beskrevet)	**Risikoreduserende effekt** (Angi for hvilke uønskede trusselscenarioer man oppnår positiv effekt)	**Status** (ÅPEN / UNDER VURDERING / FORKASTET / IMPLEMENTERT / VIDEREFØRES)	**Dato for status-endring**	**Kommentar** (Beskriv bakgrunn for status. Ved forkasting skal bakgrunn for dette beskrives)	**Ansvarlig for å følge opp** (Angi navn eller selskap)	**Frist** (Angi dato eller fase)	**Kommentar**
	Mekaniske kjøretøybarrierer foran hovedinngang.	Analysemøte, 11. mars 2019	Scenario 9, 10, 11 og 12	UNDER VURDERING	15. mars 2019	Analysegruppen anbefaler at tiltaket implementeres.	Prosjektleder	30. mars 2019	Må koordineres med LARK, ARK, RITrafikk og RIE.

Tabell 15 Tiltaks-/ALARP-register (eksempel).

4.6 Innholdsfortegnelse for sikringskonsept

Nedenfor følger anbefaling til innholdsfortegnelse for et sikringskonsept for sykehus. Det må vurderes om det skal lages ett sikringskonsept for hele bygningsmassen, eller om det er hensiktsmessig å lage flere konseptrapporter. Det kan for eksempel være store forskjeller i krav til sikring for en somatisk poliklinikk-avdeling og en avdeling for sikkerhetspsykiatri. Et egnet alternativ til oppbygging av sikringskonseptet kan være å anvende NS 3451 Bygningsdelstabellen som rammeverk. Sikringskonseptet består da av bygningsdelene som overskrifter og tilhørende krav til sikring beskrives under hver bygningsdel

TEMA	BESKRIVELSE/KOMMENTARER
Innledning	
Om oppdraget	
Forutsetninger og avgrensninger	
Sikringsmål/evalueringskriterier for risiko	
Sentrale begreper og sikringsprinsipper	
Bakgrunnsdokumenter	Henvisning til relevante lover, forskrifter, standarder, veiledninger, kravspesifikasjoner m.m.
Systembeskrivelse	Beskrivelse av bygg og prosjekt. Dette kan være hele bygningsmassen eller deler av bygningsmassen, hvis oppsplitting er hensiktsmessig. Se veiledning for systembeskrivelse i kap. 4.2.
Styringssystem for informasjonssikkerhet i prosjektet	
Konsept for organisatorisk sikkerhet	Utgjør en viktig forutsetning for konsept for fysisk sikring. Organisatoriske sikkerhetstiltak må sees i sammenheng med eksisterende organisering og behov for organisatoriske tiltak i nytt bygg. Dette arbeidet må gjennomføres i tett samarbeid med HF.
Konsept for fysisk sikring	
Soneinndeling	Beskrivelse av konsept for sikkerhetsmessig område- og soneinndeling (utvendig og innvendig).
Områdesikring/perimetersikring	
Krav til utvendig vegger, dører og vinduer	
Krav til sikring av innvendige vegger, dører og vinduer	
Elektroniske sikringsanlegg	Videoovervåkning (TVO/ITV), adgangskontroll og innbruddsalarm, låsesystemer, person- og overfallsalarmer, sikringsbelysning, talevarslingsanlegg m.m.
Merking og skilting	
Sikring av teknisk infrastruktur	Brannsikring av kritiske infrastruktur, nødstrøm, automatiske slokkeanlegg m.m.
Særlige sikringstiltak for utvalgte rom/områder	Akuttmottak somatikk/psykiatri, psykiatri generelt, resepsjoner og skranker, post- og varemottak, rømningsveier, virksomhetskritisk utstyr/rom, møterom, lagerrom, medisinrom, sikring av rom for farlig stoff.
Referanser	
Tegninger	Soneplaner, robusthetssoner, detaljer (etter behov).

Tabell 16 Anbefaling til innholdsfortegnelse for sikringskonsept

Identifikasjon av sikringsrisiko omfatter å utarbeide en tydelig og omfattende liste over tenkelige uønskede trusselscenarioer.

Del 5. Standard for grunnsikring i sykehus

Hensikten med dette dokumentet er å beskrive hva som er anbefalte grunnsikringsprinsipper ved sikring av sykehusbygninger. Det er denne grunnsikringen som skal benyttes som utgangspunkt når man gjennomfører forenklet sikringsrisikovurdering i tidligfase av et prosjekt.

5.1 Innledning

Hensikten med dette dokumentet er å beskrive hva som er anbefalte grunnsikringsprinsipper ved sikring av sykehusbygninger. Det er denne grunnsikringen som skal benyttes som utgangspunkt når man gjennomfører forenklet sikringsrisikovurdering i tidligfase av et prosjekt. Det er også dette man skal benytte som utgangspunkt for kostnadsberegninger av sikring i nye sykehusprosjekter i tidligfase. Som basis for grunnsikringsprinsippene har man benyttet erfaringer fra sykehusprosjekter gjennomført, og påbegynt, i perioden 2012-2020, og det er hentet inn innspill fra flere helseforetak via Sykehusenes sikkerhetsnettverk (NSS).

Det er viktig at utformingen av bygget og grunnsikringsprinsippene som legges til grunn i tidligfase avstemmes med helseforetaket og at disse er i samsvar med foretakets eksisterende beredskapsplaner. Her må de prosjekterende, sammen med helseforetaket, påse at relevante forhold for økt egenbeskyttelse, jf. Sivilt beredskapssystem (SBS) (JBD, 2015), kan ivaretas på en forsvarlig måte.

I et nybygg- og/eller rehabiliteringsprosjekt kan grunnsikringskonseptet komme i konflikt med andre viktige premisser. Et typisk eksempel er brannkonseptets krav til rømning ved brann og mulige konflikter med adgangskontroll. Prosjektet må identifisere motstridende funksjonskrav og søke å finne løsninger som ivaretar alle behov. I tilfeller der det ikke finnes løsninger som ivaretar alle behov må kravene prioriteres, fortrinnsvis basert på en risikovurdering.

5.2 Bruk av dokumentet

Dette dokumentet skal benyttes som utgangspunkt for kostnadsberegninger og gjennomføring av sikrings-risikovurderinger, og erstatter ikke behovet for å gjennomføre analyser. Grunnsikringen tar ikke høyde for lokale forskjeller på sykehusene eller på det lokale trusselnivået. Grunnsikringsnivået er beskrevet som en blanding av konkrete spesifikasjoner og overordnede krav til fysiske og elektroniske tiltak, men har ingen krav til selve utformingen av bygget. For å utforme bygget må man bruke sikringsrisikovurderingen som en del av en helhetlig vurdering gitt de grunnsikringstiltak som ligger til grunn.

Allerede etablerte organisatoriske tiltak, som forutsettes videreført i ny løsning, må meldes inn fra helseforetaket. Eventuelle nye organisatoriske tiltak kan komme som et resultat av sikringsrisikovurderingen i samarbeid med helseforetaket. Grunnsikringen er for enkelte områder utformet for å understøtte en forhøyning av sikkerhetsnivå ved en beredskapssituasjon, men her må helseforetaket selv komme med innspill for å sikre at man prosjekterer de riktige sikkerhetstiltakene for å understøtte beredskapsplanene.

5.3 Soneplan

Soneplanen er et verktøy for visuelt å få oversikt over hvordan de forskjellige områder og rom er avlåst. Arbeidet med soneplan skal startes allerede ved de første skissene av bygget. Soneplanen vil gi både de prosjekterende, de utførende og brukerne en mulighet til å se for seg hvordan man kan sikre en verdi, og kanskje viktigst: hvordan det blir for de som bruker bygget å bevege seg rundt med de avlåsninger som er valgt. For å visualisere er det følgende farger som skal benyttes;

Figur 12 Eksempel på soneplan

Sone 0 (utvendig): Åpent område for alminnelig ferdsel, normalt ikke avstengt. Området rundt sykehuset skal være overvåket og ha sikkerhetsbelysning.

Sone 1 (utvendig): Utvendig område som er stengt for alminnelig ferdsel. Av hensyn til inntrengning eller rømning er området sperret for andre enn de med særskilt tillatelse. Området er videoovervåket og har sikkerhetsbelysning.

Grønn sone: Åpne fellesområder og rom som er tilgjengelig for ansatte, studenter, pasienter og besøkende til enhver tid, gitt at man har kommet inn på sykehuset.

Gul sone: Delvis åpent område. Fri adgang deler av dag/døgn som defineres som åpningstid (som grønn sone i åpningstiden) og adgangskontrollert område utenfor åpningstid.

Blå sone: Lukket og adgangskontrollert område. Begrenset adgang hele døgnet. Nivå på adgangskontroll varierer etter behov og tid på døgnet fra kun kort til kort og kode.

Grått rom: Rom med fysisk nøkkel slik at rommet kan avlåses hvis ønskelig

Lilla rom: Lukket og adgangskontrollert rom. Rommet skal kunne låses men være tilgjengelig for definerte ressurser. Det er for disse rommene ikke behov for å kunne logge hvem som har åpnet døren eller for å gi alarm ved ugyldig åpning. Typisk løsning er kortlås (hotellås). Løsningen passer ikke på rom med høy bruksfrekvens (over 50 passeringer pr. dag).

Rød sone/rom: Strengt begrenset adgang, kun for personell med tjenstlig behov. Det skal være kontroll av innpasserende til rommet både innenfor og utenfor arbeidstid ved hjelp av automatisk adgangskontroll.

Figur 11 Fargekart for soneplan

5.4 Robusthetsmatrise

Robusthetsmatrisen benyttes for å illustrere områder hvor det er fare for at pasientene skader seg selv eller andre. Robusthetsmatrisen visualiseres på samme måte som soneplanen ved å fargelegge plantegningene. Men i tillegg vil det være en matrise som gir beskrivelse av ønsket robusthet for de ulike installasjonene innenfor en robusthetssone. Robusthetsmatrisen skal som et minimum utarbeides for alle psykiatriske sykehus, men det anbefales å utarbeide dette for somatiske sykehus også, særlig for akuttmottak og andre tilvarende funksjoner.

Robusthetsnivå 0 (R0): Ingen spesielle krav. Dette er rom der pasienter ikke oppholder seg, eller rom der pasienten ikke oppholder seg uten at det er en planlagt hendelse og hvor personalet har rutiner som tar hensyn til at de tar pasienter med i usikret sone.

Robusthetsnivå 1 (R1): Medium robusthetskrav. Dette er rom der pasienten ikke regelmessig og planlagt er alene, og der utagering eller selvskading som en regel oppdages og forhindres av ansatte.

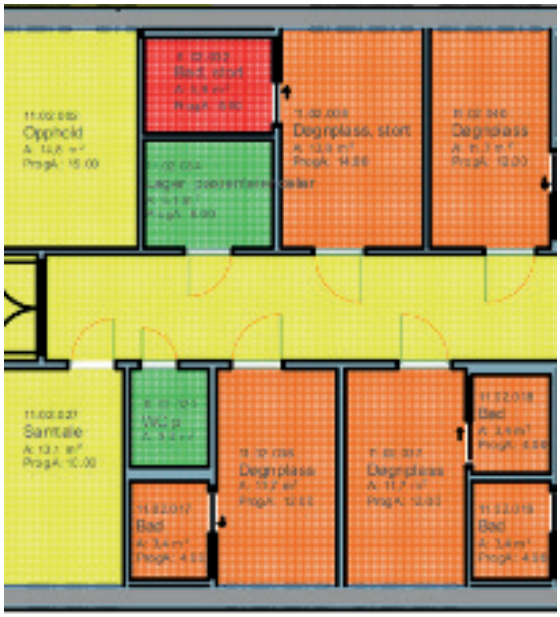
Robusthetsnivå 2 (R2): Omfattende robusthetskrav. Dette er først og fremst pasientrom, dvs. rom der pasient regelmessig og planmessig er alene. Dette medfører at ansatte ikke har oversikt til enhver tid og at situasjoner med selvskading, vold og hærverk ikke oppdages umiddelbart.

Robusthetsnivå 3 (R3): Svært omfattende robusthetskrav. Dette er i hovedsak for døgnområde sikkerhet, samt forsterkete enheter. Omfatter først og fremst arealer der pasienter er dømt til soning og der igjennom økte krav til rømningssikkerhet.

Figur 13 Fargekart robusthetsmatrise

NS	Robusthetsmatrise	Robusthetsnivå 0 (R0)	Robusthetsnivå 1 (R1)	Robusthetsnivå 2 (R2)	Robusthetsnivå 3 (R3)
236, 242	Vegger	Ingen spesielle krav	Innvendige vegg overflater skal tåle kraftige slag eller spark. Minimum løsning: Robustgips med strie og bakenforliggende kryssfinerplate	Innvendige vegg overflater skal tåle kraftige slag eller spark. Minimum løsning: Robustgips med strie og bakenforliggende kryssfinerplate	Som R2-oransje
244	Dører	1. Dører bør være innadslående, ikke slå ut i korridor og fellesareal	1. Dører bør være innadslående, ikke slå ut i korridor og fellesareal	1. Dører skal enten være utadslående eller tovegs antibarrikadedør for å hindre barrikadering.	Som R2-oransje

Figur 14 Eksempel Robusthetsmatrise



Figur 15 Fargekart robusthetsmatrise

5.5 Grunnsikringskonsept for fysisk sikring

5.5.1 Soneinndeling

Soneinndeling og utformingen av bygget må ta hensyn til mange aspekter, deriblant sikkerheten til pasienter, pårørende, besøkende og ansatte, men først og fremst må utformingen understøtte planlagt bruk av bygget. For et grunnsikringskonsept vil det være vanskelig å beskrive hvordan sikkerheten skal ivaretas uten å kjenne utformingen og bruken og det er derfor ikke hensiktsmessig at dette er en del av grunnsikringskonseptet. Krav til soneinndeling og utforming må komme som et resultat av sikringsrisikovurderingen hvor helseforetaket, sammen med de prosjekterende, må finne risikoreduserende tiltak uten at dette går på bekostning av byggets tiltenkte bruk.

5.5.2 Områdesikring/perimetersikring

Uteområdet må utformes på en slik måte at man ikke kan kjøre biler helt inntil bygget som en generell regel. Der det ikke er mulig å unngå dette, skal man forsøke å ha så stor avstand som mulig til bygget uten at dette går utover brukerne av bygget.

Det skal også prosjekteres inn sperringer for å hindre at kjøretøy kan kjøre inn i bygningsmassen, eller redusere farten de kan kjøre inn i bygningsmassen med. Fartsreduserende tiltak, som svinger, innsnevringer, fartsdempere i veien e.l., skal tilstrebes der hvor man skal kunne kjøre inntil bygget.

5.5.3 Krav til utvendige vegger, dører og vinduer

Somatikk og administrasjon

- Vegger over 4 meter over bakkeplan har ingen spesielle krav. Vegger inntil 4 meter over bakkeplan skal som hovedregel prosjekteres med samme innbruddsmotstand som vinduer og dører. Som referanse kan Forsvarsbygg sin sikringshåndbok benyttes.
- Dører, vindu og glass: RC2 i henhold til NS-EN1627:2011.
- Lås og beslag: Skal minimum være FG-godkjent ihht. FG-310:2 klasse 2b eller tilsvarende.
- Bygg for psykisk helsevern og bygg for kritisk infrastruktur
- Robusthetsmatrisen må legges til grunn for all prosjektering i bygg for psykisk helsevern
- Vegger skal som hovedregel prosjekteres slik at de har samme innbruddsmotstand som vinduene og dørene. Som referanse kan Forsvarsbygg sin sikringshåndbok benyttes.
- Dører, vindu og glass: RC4 i henhold til NS-EN1627:2011.
- Lås og beslag: Skal minimum være FG-godkjent ihht. FG-310:2 klasse 3 eller tilsvarende.

5.5.4 Krav til sikring av innvendige vegger, dører og vinduer

Somatikk og administrasjon

- Det er ingen spesielle krav til vegger innvendig foruten i soneskille inn til rom som er kritiske og som i soneplan er merket røde. Der skal vegger skal som hovedregel prosjekteres slik at de har samme innbruddsmotstand som vinduene og dørene. Som referanse kan Forsvarsbygg sin sikringshåndbok benyttes.
- Dører, vindu og glass: RC2 i henhold til NS-EN1627:2011.
- Lås og beslag: Skal minimum være FG-godkjent ihht. FG-310:2 klasse 2b eller tilsvarende.
- Bygg for psykisk helsevern og bygg for kritisk infrastruktur
- Robusthetsmatrisen må legges til grunn for all prosjektering i bygg for psykisk helsevern
- Vegger skal som hovedregel prosjekteres slik at de har samme innbruddsmotstand som vinduene og dørene. Som referanse kan Forsvarsbygg sin sikringshåndbok benyttes.
- Vindu og glass: RC4 i henhold til NS-EN1627:2011.
- Lås og beslag: Skal minimum være FG-godkjent ihht. FG-310:2 klasse 3 eller tilsvarende.

5.5.5 Elektroniske sikringsanlegg

For alle elektroniske sikringsanlegg skal det legges til grunn at det skal etableres som en georedundant løsning, være lokalisert med fysisk avstand der server, eller annet sentralutstyr, installeres i to separate datasenter eller i lignende rom. Sikkerhetsnivået for løsningen med tanke på redundans må det gjennomføres en egen vurdering av sammen med helseforetaket.

Videoovervåkning (ITV)

Det skal etableres videoovervåkning på sykehuset som overvåker, og tar opptak av, steder hvor man kan forvente at det skjer uønskede handlinger eller hvor det strategisk er hensiktsmessig å overvåke for å se hvem som kommer inn i bygningen og hvem som oppholder seg rundt bygningen.
ITV systemet skal benyttes som alarmgiver ved å benytte intelligent videodeteksjon. Denne deteksjonen skal benyttes til å varsle hvis det er bevegelse i arealer det ikke skal være bevegelse, samt til å spare lagringsplass ved kun å ta opptak ved bevegelse.
Det anbefales at det er vaktpersonell som overvåker videobildene og at bildene benyttes for raskt å kunne verifisere om en alarm er reell eller ikke. Der det ikke

er vaktpersonell tilgjengelig, må videoovervåkningen som et minimum ta opptak for dokumentasjon etter en hendelse. Videoovervåkningen skal være av en slik kvalitet at man skal kunne identifisere personer som kommer inn på sykehuset uansett lysforhold, og kunne observere det som skjer rundt fasade uansett lysforhold. Opptakene skal lagres i sentralt hoved-kommunikasjonsrom eller på regionalt datasenter. Det anbefales at systemet settes opp med redundans på maskinvare og at det installeres geografisk adskilt.

Adgangskontroll (AAK)

Det skal etableres et adgangskontrollsystem for å kunne regulere tilgangen til sykehuset generelt, samt regulere tilgangen til rom og områder i henhold til soneplan. Adgangskontrollanlegget skal være mulig å programmere slik at tilgang til områder og rom for den enkelte skal kunne endres etter behov av helse-foretaket selv.

Adgangskontrollen skal kunne settes opp til å alarmere hvis en dør åpnes uten at gyldig tilgang er gitt (innbrudd), eller døren holdes åpen for lenge. Dette skal være iverksatt som et minimum på alle dører i fasaden og i dører som gir tilgang til blå og gul sone og røde rom. For tilgang til grå rom kan det benyttes kortlås (hotellås) som er trådløse. Det anbefales ikke trådløse systemer for adgangskontroll utover for kortlås. Adgangskontrollsystemet skal installeres på en slik måte at det er begrenset tilgang til kontrollenheter og til servere.

Innbruddsalarm (AIA)

Det skal etableres innbruddsalarm, enten selvstendig eller som en del av adgangskontrollen ved utsatte områder som medisinrom, sykehusapotekene, varelager, kiosk m.m. Innbruddsalarmen skal ha alarmoverføring til egen eller ekstern vektertjeneste og utstyret skal være godkjent i henhold til Forsikringsselskapenes Godkjenningsnemds (FG) grad 3 for innbruddsalarm. Viser her til FG publikasjon 200:3 FG-regler for automatiske innbrudds og overfallsalarmsystemer.
Installasjonen av utstyret skal følge rommet/skallets beskyttelsesklasse, normalt vil dette gi FG grad 2 for innbruddsalarmen.

Ransalarm

Det skal legges opp til en kablet ransalarm i alle ekspedisjoner, resepsjoner, mottak og andre kritiske lokasjoner som f.eks medisinrom som ligger i områder med pasienter. Ransalarmen skal varsle interne ressurser, som kollegaer eller vektertjeneste. Ransalarm skal også kunne varsle ut til ekstern vektertjeneste.

Overfallsalarm

Det skal etableres en trådløs overfallsalarm for de som arbeider på somatisk akuttmottak, innen psykisk helsevern og for de som arbeider alene på natt. Overfallsalarmen skal for akuttmottak og psykisk helsevern kunne gi posisjon ved alarm på romnivå, mens for øvrige deler av sykehuset skal den minimum gi alarm på avdelingsnivå. Overfallsalarmen skal varsle interne ressurser, som kollegaer og/eller vektertjeneste. Overfallsalarmen skal også kunne varsle ut til ekstern vektertjeneste.

Brannalarm (ABA)

Det skal installeres et brannalarmanlegg i henhold til gjeldende regelverk og prosjektets brannkonsept. Ihht NS3960 skal det også legges opp til deteksjon på bad som benyttes for pasienter innen psykisk helsevern, da man her har betydelig risiko for ildspåsettelse.

Talevarsling

Det skal installeres anlegg for talevarsling ihht NS3961. Terskelen for å unnlate å installere talevarsling skal være høy. Talevarslingen skal kunne benyttes til annet formål enn brann slik som for eksempel PLIVO-hendelser (Pågående Livstruende Vold) eller andre beredskapshendelser.

5.5.6 Merking og skilting

Ingen rom som inkluderer kritisk infrastruktur skal merkes på en slik måte at de er enkelt identifiserbare.

5.5.7 Sikring av teknisk infrastruktur

Kritisk teknisk infrastruktur som vann, avløp, strøm og IKT er viktig for å kunne opprettholde forsvarlig drift av sykehuset. Kritikaliteten av denne infrastrukturen varierer fra bygg til bygg, region til region og helseforetak til helseforetak. Dette gjør at det ikke er hensiktsmessig å legge føringer for hvordan denne infrastrukturen skal bygges eller sikres i dette dokumentet.

Det er opp til helseforetaket/prosjektet å definere omfang og løsning for dette basert på tidligere erfaringer og gjennomførte risiko- og sårbarhetsanalyser for utilsiktede hendelser. Det må også defineres hvilken grad av redundans det legges opp til på disse systemene. Når omfang og løsning er definert må det gjennomføres en sikrings-risikovurdering spesifikt for kritisk infrastruktur på samme måte som man gjør for resten av bygget.

5.5.8 Særlige sikringstiltak for utvalgte rom/områder

Må beskrives som en del av arbeidet med sikkerhet.

5.6 Grunnsikring – ansvarsmatrise prosjektering

Sikringsfaget er i utgangspunktet et premissgivende fag, sammenlignbart med Brannsikkerhet (RIBR). Samhandling og koordinering mot andre fag må ivaretas gjennom prosjektets steg. Matrisen nedenfor er et utgangspunkt for å identifisere viktige grensesnitt mellom fagene, men dette må tilpasses hvert enkelt prosjekt

Se tabell på neste side

Nummer	Beskrivelse	Tiltak	ARK	RIE	RIV	RIB	IARK	RIBR	Byggherre	Helseforetaket
1	Kjøretøysperrer	Kjøretøysperre	x				x			
2	Veggkonstruk-sjoner	Dører	x							
		Porter	x							
		Glass/vinduer	x							
		Vegger	x							
3	Soneplaner/ robusthetsmatrise	Utarbeide soneplaner og ro-busthetsmatrise	x	x					x	x
4	Merking og skilting	Merking	x							x
		Skilting	x							x
5	Adgangskontroll	Adgangskontroll på dører		x				(x)		
6	Innbruddsalarm	Innbruddsalarm		x						
		Utarbeide alarmorganisering						x		x
7	Lås og beslag	Lås og beslag	x	x				(x)		
		Låsplan							x	
8	Videoovervåking	Etablering av system for vi-deoovervåkning (TVO).		x						
		Utarbeide hensiktsskjema for alle kameraer		x					x	x
9	Person og overfalsalarm	Etablere trådbundne person- og overfallsalarmer.		x						
		Trådløst person- og overfallsa-larmsystem		x						
10	Sikkerhets-belysning	Utarbeide plan og beskrivelse for sikringsbelysning, som må sees i sammenheng med TVO-omfang.	x	x			x			
11	Talevarslings-anlegg	Etablere talevarsling også for bruk ved andre hendelser		x				(x)		

Tabell 17. Ansvarsmatrise prosjektering.

Vold og trusler er hendelser hvor arbeidstakere blir fysisk eller verbalt angrepet i situasjoner som har forbindelse med deres arbeid, og som innebærer en åpenlys eller antydet trussel mot deres sikkerhet, helse eller velvære

Del 6. Vedlegg

Vedlegg A: Bakgrunn om risikobegrepet

a) Innledning om risikobegrepet

Ofte omtales risiko for en hendelse som «produktet av sannsynligheten og konsekvensen av hendelsen». En slik definisjon finner vi i NS 5814 Krav til risikovurderinger. Innenfor sikringsfaget har risikobegrepet vært mye diskutert. Diskusjonen har i stor grad vært knyttet til risikobegrepets sterke tilknytning til nettopp sannsynlighetsbegrepet. Et vanlig kritisk spørsmål er: Hvordan kan man sette sannsynligheter for hendelser som aldri tidligere har skjedd, for eksempel en terroraksjon mot et norsk sykehus?

Som en følge av behovet for å se annerledes på risiko i sikringsfaget, ble det etablert en komité i Standard Norge som skulle arbeide med denne problemstillingen. I 2012 resulterte dette arbeidet i at Standard Norge publiserte standarden NS 5830 Samfunnssikkerhet – Beskyttelse mot tilsiktede handlinger – Terminologi. I NS 5830 er ikke risiko knyttet til sannsynlighetsbegrepet. Risiko er her definert som forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet ovenfor den spesifiserte trusselen (NS 5830). Denne definisjonen av risiko blir ofte omtalt som «trefaktormodellen». I denne veilederen har vi valgt å kombinere elementene fra trefaktormodellen og den tradisjonelle forståelsen av risiko. Vi ser at risikobegrepet fra NS 5830 trekker inn viktige elementer, som er sentrale å vurdere når vi ser på tilsiktede uønskede handlinger. Vi er nødt til å ha et forhold til hvilke verdier vi skal beskytte, hvilke trusler verdiene våre er utsatt for, og hvor enkelt eller vanskelig det vil være for ulike trusselaktører å skade verdiene våre (sårbarhet). Til tross for dette, ser vi også noen utfordringer med å introdusere et separat risikobegrep knyttet til tilsiktede uønskede handlinger:

1. Et separat risikobegrep innenfor sikringsfaget vil gjøre det utfordrende å sammenligne risikobildet og tiltak fra risikovurderingene med sykehusets øvrige risikobilde.
2. Kritikken av «det tradisjonelle» risikobegrepet er unyansert, og bygger på en for snever definisjon av risiko.
3. Kritikken av sannsynlighetsbegrepet er knyttet til en spesifikk, og for snever, oppfatning av hva en sannsynlighet representerer.
4. Disse problemstillingene diskuteres nærmere i de følgende kapitlene.

b) Risikobegrepet og ulike typer risikovurderinger

Den første problemstillingen er knyttet til felles forståelse av et begrep (risiko) som brukes i mange sammenhenger. Risikovurderinger gjøres på mange temaer i forbindelse med planlegging, bygging og drift av sykehus. Eksempler er risikovurderinger (eller ROS-analyser) av; naturfare (flom, skred, geoteknisk

risiko, ekstremvær) i forbindelse med regulering av tomt; tap av kritisk infrastruktur (strøm, vann, avløp, IKT m.m.); sikkerhet, helse og arbeidsmiljø (SHA) i henhold til Byggherreforskriften; miljørisikovurderinger, og; risikovurderinger knyttet til brannsikkerhet. Et felles risikobegrep vil gjøre det enklere å sammenligne risikoer og prioritere mellom ulike tiltak i situasjoner hvor det er begrensede tilgjengelige ressurser.

c) En bred definisjon av risiko

Den andre problemstillingen er knyttet til den tradisjonelle forståelsen av risikobegrepet. Selv om risiko for en hendelse ofte omtales som produktet av sannsynligheten og konsekvensen av hendelsen, så er ikke dette en dekkende definisjon av begrepet risiko. Produktet av sannsynlighet og konsekvens er en indeks (et verktøy) som beskriver visse sider av risikoen. En slik indeks gir et smalt og ufullstendig bilde av risikoen. Så lenge dette er den rådende oppfatningen av hva risiko er, vil begrepet være lite hensiktsmessig i forbindelse med vurderinger av både utilsiktede og tilsiktede uønskede handlinger.

Så hva er egentlig risiko? Risiko handler om fremtidige konsekvenser av en aktivitet og usikkerhet. Konsekvensene kan anses som avvik i forhold til en referanse, for eksempel en normaltilstand for sykehuset. For aktiviteten å drive et sykehus, kan konsekvenser som avviker fra normaltilstanden for eksempel være skadde og omkomne personer som følge av tilsiktede uønskede handlinger. Vi vet imidlertidig ikke om tilsiktede uønskede handlinger vil inntreffe i fremtiden, eller hvor store konsekvensene faktisk vil bli. Det er altså usikkerhet knyttet til konsekvensene. En god beskrivelse av risiko, vil derfor inkludere usikkerhet. Dette er en svakhet ved både den tradisjonelle oppfatningen (sannsynlighet x konsekvens) og trefaktormodellen. Der usikkerhet reduseres til sannsynlighet (jf. NS 5814-definisjonen) blir usikkerhetsvurderingen for snever. I trefaktormodellen (jf. NS 5830-definisjonen) er usikkerhetsdimensjonen fullstendig fraværende.

d) Sannsynlighetsbegrepet

Den tredje problemstillingen er knyttet til hvordan sannsynlighetsbegrepet skal forstås i en risikovurderingskontekst. Som mange andre begrep, har også begrepet sannsynlighet ulike fortolkninger avhengig av hvilket faglig ståsted man har. Når det rettes kritikk mot bruken av sannsynlighetsbegrepet i risikovurderinger, er dette ofte med utgangspunkt i at sannsynlighet defineres som en relativ frekvens (frekvenssannsynlighet). Frekvenssannsynligheter kan illustreres med terningkast: Hvis man er interessert i å finne sannsynligheten for å få seks øyne på terningen i neste kast, kan man estimere sannsynligheten ved å gjennomføre gjentatte forsøk under like betingelser med terningen. Etter mange forsøk med terningen kan vi se på forholdet mellom summen av suksesser (antall ganger man fikk seks øyne) over summen av antall forsøk. Dette vil gi et estimat for frekvenssannsynligheten, som (med en rettferdig terning) ganske raskt vil nærme seg 1/6 etter en del forsøk.

Når vi snakker om sannsynlighet i en risikovurderingskontekst, der vi ser på utfordringer i den virkelige verden, blir referansen til terningkast og gjentatte forsøk meningsløs. Vi kan ikke utføre forsøk med et sykehus og telle opp forholdet mellom antall ganger et terrorangrep skjedde og det totale antall forsøk. Sannsynlighetsbegrepet må få et annet innhold enn det vi legger i frekvenssannsynligheter. Risiko er, som nevnt ovenfor, knyttet til fremtidige og usikre konsekvenser. Når vi bruker sannsynlighetsbegrepet i forbindelse med en terrorhendelse i fremtiden, representerer sannsynligheten analytikerens grad av tro knyttet til om hendelsen vil inntreffe innenfor et spesifisert tidsrom. Det etableres ingen referanse til forsøk og relative frekvenser. Slike sannsynligheter kalles subjektive sannsynligheter (De Finetti, 1937; Lindley, 2006), eller kunnskapsbaserte sannsynligheter (Aven, 2003). Denne fortolkningen av sannsynligheter er nok ikke like kjent som frekvenssannsynligheter, men har et like sterkt vitenskapelig fundament.

La oss nå forsøke å besvare spørsmålet vi stilte ovenfor: «Hvordan kan man sette sannsynligheter for hendelser som aldri tidligere har skjedd, for eksempel en terroraksjon mot et norsk sykehus?» i lys av de ulike fortolkningene av sannsynlighetsbegrepet. Hvis vi legger til grunn forståelsen om frekvenssannsynlighet, vil det ikke være mulig å sette en sannsynlighet for en terroraksjon mot et norsk sykehus.

Det finnes ingen eksempler på slike hendelser tidligere, og vi kan heller ikke etablere et hypotetisk eksperiment der vi ser på driften av et likt sykehus gjentatte ganger, og teller opp antall ganger et terrorangrep inntraff. Hvis vi, derimot, bruker forståelsen om kunnskapsbaserte sannsynligheter, er det fullt mulig å sette en sannsyn-

lighet. Når en risikoanalytiker sier at sannsynligheten for et terrorangrep i sykehusets levetid er mindre enn 1 %, er dette det samme som at analytikerens grad av tro om terrorhendelsen sammenlignes med å trekke en spesifikk kule i en urne med 100 kuler. Slik er det altså fullt mulig å sette en sannsynlighet for en fremtidig terrorhendelse på et norsk sykehus.

e) Sannsynlighet og kunnskapsgrunnlag

Diskusjonen i 6.4 viser hvordan det er mulig å sette en sannsynlighet for en hendelse som aldri har skjedd før. Men så kommer neste spørsmål: er det nyttig å sette en sannsynlighet, og kan vi basere beslutninger på den vurderingen som analytikeren har gjort?

Det vi skal merke oss her, er at det ikke finnes objektive sannsynligheter knyttet til om et terrorangrep vil inntreffe på et sykehus i fremtiden. Prediksjonsevnen er avhengig av analytikerens kunnskapsgrunnlag, som kan være sterkt eller svakt. Dersom vi ser på hendelsen «vold mot ansatt på sengepost for psykisk helsevern», finnes det statistikk fra norske sykehus som kan underbygge analytikerens grad av tro om at hendelsen også vil inntreffe i fremtiden. Det er imidlertid ikke et én-til-én-forhold mellom statistikk og analytikerens sannsynlighetsvurdering. Statistikken bygger på en mengde forutsetninger om hvordan ting har vært i norske sykehus tidligere. Analytikerens sannsynlighetsvurdering bygger på hvordan ting skal bli i det konkrete sykehuset som analyseres. Så når analytikeren angir at sannsynligheten for hendelsen «vold mot ansatt på sengepost for psykisk helsevern» er større enn 90 % i løpet av ett år, bygger dette på et sterkt empirisk grunnlag som analytikeren har tatt hensyn til i sin vurdering. Analytikerens vurdering av sannsynligheten for et terrorangrep (< 1 % i løpet av levetiden til sykehuset) bygger ikke på det samme sterke empiriske grunnlaget.

Styrken på bakgrunnskunnskapen for fastsettelse av en sannsynlighet er viktig for troverdigheten til analysen, eller hvor mye vekt en beslutningstaker skal legge på sannsynlighetsvurderingen. Der bakgrunnskunnskapen er sterk bør sannsynlighetsangivelsen tillegges mer vekt enn der bakgrunnskunnskapen er svak. Når sannsynligheter brukes i en risikovurdering er det derfor viktig at det også spesifiseres hvilken bakgrunnskunnskap som er benyttet. På denne måten kan beslutningstaker gjøre sin egen vurdering av analysens troverdighet og bestemme hvilken vekt sannsynlighetsvurderingen skal få når beslutninger skal tas.

f) Risikoperspektiv for tilsiktede handlinger

I denne veilederen legges det til grunn at risiko er kombinasjonen av hendelser (A) med konsekvenser (C) og tilhørende usikkerheter (U) (Aven, 2007; 2010). Her forstår vi A som alle mulige uønskede hendelser (f.eks. uønskede tilsiktende handlinger), C er alle mulige konsekvenser av disse uønskede hendelsene og U er uttrykk for at konsekvensene er usikre.

Verdier, sårbarhet og trusler vil være sentrale elementer i risikovurderingen. Konsekvensenes, det vil si tapets, størrelse vil være avhengig av systemets verdi. Hvorvidt konsekvenser/tap realiseres ved en hendelse, er avhengig av systemets sårbarhet for den aktuelle hendelsen. Trusler vil være de underliggende årsakene til at konsekvenser/tap kan oppstå. Usikkerhetsaspektet er knyttet til manglende kunnskap, blant annet om hvilke konsekvenser/tap som kan inntreffe, hvilke aktører som kan utføre tilsiktede uønskede hendelser og hvilke virkemidler disse aktørene kan benytte seg av. Usikkerhet er også knyttet til den bakgrunnskunnskapen vi legger til grunn for våre vurderinger av disse aspektene. Usikkerhet er derfor en helt sentral, og uatskillelig, del av risikobegrepet, som ikke gjenspeiles i NS 5830-seriens definisjon av risiko, og som kun uttrykkes i form av sannsynlighet i den tradisjonelle definisjonen av risiko jf. NS 5814.

En samlet risikobeskrivelse for denne risikomodellen, dvs de konkrete størrelsene vi ser på og vurderer i en risikovurdering, vil være (A', C', S, K):

- A' og C' er de spesifikke hendelsene og konsekvensene som er vurdert
- S er sannsynligheter for A' og C'
- K er bakgrunnskunnskapen som A', C' og S er basert på.

En viktig grunn til at vi velger å bruke denne måten å beskrive risiko på er at den eksplisitt adresserer bakgrunnskunnskapen K. Det er dessverre alt for ofte at man i forbindelse med analyser av risiko får presentert et risikobilde uten informasjon om hvilken kunnskap dette risikobildet er basert på.

Vold og trusler er hendelser hvor arbeidstakere blir fysisk eller verbalt angrepet i situasjoner som har forbindelse med deres arbeid, og som innebærer en åpenlys eller antydet trussel mot deres sikkerhet, helse eller velvære.

Trusler er verbale angrep eller handlinger som tar sikte på å skade eller skremme en person.

Vold er enhver handling som har til hensikt å føre til fysisk eller psykisk skade på person. Det kan også defineres som vold når arbeidstakere opplever utagerende handlinger hvor det utøves stort skadeverk på inventar og utstyr.

Arbeidstilsynet (2017)

Vedlegg B: Vold og trusler i helseinstitusjoner

Sikring mot vold og trusler i helsesektoren medfører tilsynelatende et dilemma. Samtidig som ansatte på helseinstitusjoner har krav på et trygt arbeidsmiljø, representerer behandlingen av pasienter en fare for vold og trusler som følge av pasientenes diagnoser. Her er man i en situasjon hvor aktivitetene som bidrar til pasientenes behandling er det som skaper sårbarhet i forbindelse med voldshandlinger. Det er heller ikke alltid like lett å definere om en uønsket hendelse har sin opprinnelse i sykdom eller er en «tilsiktet handling» fra pasientens side. På den annen side er det kanskje ikke så interessant å lage et klart skille mellom hvilke hendelser som har sitt utspring i sykdom eller tilsiktede handlinger. Hovedpoenget er kanskje å innse at en helseinstitusjon representerer en stor verdi for samfunnet, både i form av sin operative funksjon og de mange menneskene som oppholder seg der, og står samtidig ovenfor hyppig forekommende trusler mot disse verdiene?

I mange tilfeller er truslene interne og en uatskillelig del av virksomhetens aktiviteter. En systematisk tilnærming til sikring av personer, bygning og teknisk infrastruktur er derfor viktig for å oppnå balanse mellom sentrale verdier, som åpenhet; tilgjengelighet; trygghet for ansatte, pasienter og pårørende, og; sikkerhet mot tap av operativ funksjon og materielle verdier.
Arbeidsmiljøloven skal blant annet sikre et arbeidsmiljø som gir grunnlag for en helsefremmende og meningsfylt arbeidssituasjon, og gi full trygghet mot fysiske og psykiske skadevirkninger, jf. arbeidsmiljøloven § 1–1. Regelverket krever at arbeidstaker skal, så langt det er mulig, beskyttes mot vold, trusler og uheldige belastninger som følge av kontakt med andre, jf. arbeidsmiljøloven § 4–3.

Ifølge Arbeidstilsynet (2017) er det en økende risiko for vold og trusler i arbeidslivet, både i Norge og internasjonalt. Omtrent 200 000 arbeidstakere varsler om vold eller trusler i forbindelse med arbeidet hvert år, og det er mer enn dobbelt så mange kvinner som menn som rapporterer at de blir utsatt for vold og trusler. Kvinner under 25 år er gruppen som oftest rapporterer om vold og trusler. Arbeidstilsynet påpeker at en mulig årsak til at kvinner er mer utsatt, er at det er flere kvinner enn menn som arbeider i utsatte bransjer. Helserelaterte yrker som vernepleiere, sosialarbeidere, pleie- og omsorgsarbeidere og sykepleiere er blant de mest utsatte yrkene. Fellestrekk er at arbeidstakere i stor grad er i kontakt med andre mennesker gjennom sitt arbeid og utfører tjenester overfor en tredjeperson. Det å jobbe ansikt-til-ansikt med for eksempel kunder eller pasienter øker sannsynligheten for å bli utsatt for vold og trusler. Det gjelder særlig arbeid med mennesker som befinner seg i en sårbar livssituasjon på grunn av for eksempel sykdom, rus eller liknende. Alenearbeid, natt- og kveldsarbeid og det å jobbe med penger og andre verdier øker også risikoen.

Arbeidsmiljøloven skal blant annet sikre et arbeidsmiljø som gir grunnlag for en helsefremmende og meningsfylt arbeidssituasjon, og gi full trygghet mot fysiske og psykiske skadevirkninger, jf. arbeidsmiljøloven § 1–1. Regelverket krever at arbeidstaker skal, så langt det er mulig, beskyttes mot vold, trusler og uheldige belastninger som følge av kontakt med andre, jf. arbeidsmiljøloven § 4–3.

Ifølge Arbeidstilsynet (2017) er det en økende risiko for vold og trusler i arbeidslivet, både i Norge og internasjonalt. Omtrent 200 000 arbeidstakere varsler om vold eller trusler i forbindelse med arbeidet hvert år, og det er mer enn dobbelt så mange kvinner som menn som rapporterer at de blir utsatt for vold og trusler. Kvinner under 25 år er gruppen som oftest rapporterer om vold og trusler.

Arbeidstilsynet påpeker at en mulig årsak til at kvinner er mer utsatt, er at det er flere kvinner enn menn som arbeider i utsatte bransjer. Helserelaterte yrker som vernepleiere, sosialarbeidere, pleie- og omsorgsarbeidere og sykepleiere er blant de mest utsatte yrkene. Fellestrekk er at arbeidstakere i stor grad er i kontakt med andre mennesker gjennom sitt arbeid og utfører tjenester overfor en tredjeperson. Det å jobbe ansikt-til-ansikt med for eksempel kunder eller pasienter øker sannsynligheten for å bli utsatt for vold

	Fysisk vold	Trusler om fysisk vold	Psykisk mishandling (trakas-sering, mobbing)
Pasient	88,4 %	77,6 %	39,6 %
Kombinasjonen pasi-ent/pårørende	6,8 %	10,2 %	16,1 %
Pårørende	2,5 %	8,3 %	14,7 %
Kollega	1,1 %	8,3 %	14,7 %
Pasient + kollega	0,6 %	0,2 %	4,1 %
Lege	0,0 %	0,2 %	1,0 %

Tabell 18. Trusselaktører med hensyn til fysisk vold, trusler om fysisk vold og psykisk mishandling av helsepersonell (Roche, Diers et al., 2010)

og trusler. Det gjelder særlig arbeid med mennesker som befinner seg i en sårbar livssituasjon på grunn av for eksempel sykdom, rus eller liknende. Alenearbeid, natt- og kveldsarbeid og det å jobbe med penger og andre verdier øker også risikoen.

Intensjonen bak vold og trusler varierer, men Arbeidstilsynet (2017) skiller mellom relasjonell vold/trusler og instrumentell vold/trusler. I hovedtrekk betyr førstnevnte at vold og trusler utøves som et mål i seg selv, mens i sistnevnte tilfelle er vold og trusler et middel for å oppnå noe annet.

Organisatoriske faktorer som synes å bidra til volds- og trusselhendelser er tidspress, arbeidstempo, overtidsarbeid, krav om hurtige beslutninger og når det gjennomføres arbeidsoppgaver som ligger utenfor kompetanseområdet til arbeidstakeren. Kompetanse og kapasitet i forhold til å håndtere vold og trusler er av stor betydning for både forebygging og utfall av hendelser. Det bør legges vekt på god opplæring, tilstrekkelig bemanning og kontinuitet i arbeidsforhold for å forebygge volds- og trusselhendelser.

a) Omfang av problemet i helseinstitusjoner

Vold og trusler mot ansatte på helseinstitusjoner generelt, og institusjoner for psykisk helsevern spesielt, er et globalt problem som er gjenstand for omfattende forskningsaktivitet (se f.eks.: d'Ettorre & Pellicani, 2017; Wolf, Perhats et al., 2018; Lee Gillespie, Papa & Gómez, 2017; Geoffrion, Goncalves et al., 2017; Dawson, Lachner et al., 2018; Ramacciati, Ceccagnoli et al., 2018; Roche, Diers et al., 2010; Lau, Magarey & Wiechula, 2012 (part I and II); Morken, Baste et al., 2018; McDermott, Dualan & Scott, 2011; Cutcliffe & Riahi, 2013 (part I); Hahn, Müller et al., 2013). Det er ikke gjort noen vurdering av hvorvidt utenlandsk forskning er overførbar til norske forhold. Hensikten med dette kapittelet er først og fremst å beskrive hvilken type forskning som finnes og presentere et datagrunnlag som kan være utgangspunkt for gode faglige diskusjoner.

Selv om problemet beskrives som størst innen psykisk helsevern og akutt somatisk behandling, er ikke øvrige deler av sykehuset unntatt risiko. Foruten psykisk helsevern og aktutt somatikk, beskrives problemet som fremtredende innenfor enhetene postoperativ (recovery), anestesi, rehabilitering (intermediate care og step-down) og intensivbehandling (Hahn, Müller et al., 2013).

Roche, Diers et al., (2010) har studert hvem som er trusselaktører for hhv fysisk vold, trusler om fysisk vold og psykisk mishandling. Resultatene er gjengitt i tabell 18. Av tabellen ser vi at pasienter utgjør den største trusselen innen alle hendelseskategorier, og særlig innenfor hendelseskategorien fysisk vold og trusler om fysisk vold. Samtidig ser vi at pårørende er en trusselaktør, særlig knyttet til trusler mot og psykisk mishandling av helsearbeidere. Det er også verdt å peke på at kolleger utgjør en trussel med hensyn til psykisk mishandling (trakassering og mobbing).

Studier av hyppigheten av hendelser har forskjellig utgangspunkt med hensyn til studieobjekter og bruker ulike måleenheter. Her følger likevel noen eksempler som kan beskrive omfanget av ulike hendelser på institusjoner for psykisk helsevern:

- Mellom 24 % og 80 % av helsearbeidere i akutt psykisk helsevern er angrepet av en pasient i løpet av karrieren. Verbale angrep og trusler rammet ca. 45-80 % av helsearbeiderne, mens seksuell trakassering rammet mellom 9,5-37,2 % av helsearbeiderne (D'Ettorre & Pellicani, 2017).
- En studie av trussel- og voldshendelser på institusjoner for akutt psykiatri estimerte 0,55 voldshendelser pr seng pr måned (Carr, Lewin et al., 2008).
- En studie av 70 000 psykiatripasienter viste at 48 % av pasientene på sikkerhetsavdeling (forensic psychiatric wards) var voldelige i løpet av studieperioden på 31 måneder. For akutt-psykiatrisk avdeling var tallet 26 % over en periode på 19 måneder. For mindre akutte avdelinger var tallet 22 % over en studieperiode på 16 måneder (Ramesh, Igoumenou et al., 2018).

- Chen, Huang et al. (2011) har sett på ulike uønskede hendelser mot kvinnelige sykepleiere i akutt psykiatrisk sykehus, og rapporterer hendelsesrater. Fysisk vold: 2,3 hendelser pr ansattår, verbal trakassering/trusler: 7,8 hendelser pr ansattår, mobbing 0,3 hendelser pr ansattår, og seksuell trakassering: 1,0 hendelser per ansattår.

b) Syn på problemet

Til tross for mye forskning på problemstillingen antas det at trusler og vold mot helsearbeidere er underrapportert, og et fenomen vi har manglende kunnskap om. Studier viser for eksempel at helsearbeidere har ulike terskler for hva som skal defineres som aggresjon og vold, der trusler og vold bortforklares. Et eksempel er at helsearbeideren ikke anser seg selv som målet for handlingen, men mer som et tilfeldig offer for en uunngåelig og uforutsigbar handling (Ramacciati, Ceccagnoli et al., 2018; Lau, Magarey & Wiechula, 2012b).

Studier viser også at det er en tydelig sammenheng mellom voldsutøvelse og psykisk sykdom eller annen sykdom. Helsearbeidere har da gjerne en høy terkskel for å rapportere om hendelser og/eller at hendelsene ikke tas på tilstrekkelig alvor i institusjonens ledelse (D'Ettorre & Pellicani, 2017; Chen, Huang et al. 2011). For å få til forbedringer med hensyn til trusler og vold på arbeidsplassen, er det ikke gunstig at problemet oppfattes som uungåelig og uforutsigbart. Det er viktig at det finnes tro på at problemet er mulig å løse.

Mange studier beskriver ulike risikovurderingsmetoder for predikere fare for trusler og vold, der disse i stor grad har fokus på kjennetegn ved pasienten (intern modell). Disse interne modellene gir begrenset nytteverdi i konteksten planlegging og bygging av nye sykehus og helseinstitusjoner. Mer nytte finner man i mer system-orienterte modeller. I en systemmodell forklares ikke pasientens handlinger bare ved interne kjennetegn. Pasientens handlinger er i større grad et resultat av samspillet mellom pasienten, helsearbeiderne og de fysiske omgivelsene på institusjonen (se f.eks. Cutcliffe & Riahi, 2013; Nijman, Campo et al., 1999). I vegtrafikken har det for eksempel tradisjonelt vært vanlig å plassere skyld for en ulykke på trafikanten. I nyere sikkerhetstenkning, og som et resultat av nullvisjonen, er det i dag en større anerkjennelse for at ulykker produseres i samspillet mellom trafikant, kjøretøy og veginfrastrukturen. Sikrere kjøretøy og veginfrastruktur bidrar til større sikkerhetsmarginer, der trafikantens kompetanse og tilstand får mindre avgjørende betysning for ulykkesrisiko. En tilsvarende tenkning synes hensiktsmessig også for trusler og vold mot helsearbeidere. Ifølge Cutcliffe & Riahi (2013) må de som kjenner problemet på kroppen, dvs de som bor og jobber på institusjonene, involveres i designprosessene. Det finnes et uforløst potensial i å gjøre avdelingene bedre utformet for å forebygge aggresjon og vold, eller i det minste unngå at dårlig design blir et triggerelement for aggresjon og vold.

c) Mulige årsaker til trusler og vold

Når vi ser på beskrivelser av årsaker til trusler og vold mot helsearbeidere er det tydelig at pasientinterne faktorer som psykisk sykdom (schizofreni, bipolar lidelse m.m.), alder (lav alder), kjønn (menn), tidligere voldshistorikk og rusmiddelbruk er viktige predikatorer for fremtidige voldshendelser (D'Ettorre & Pellicani, 2017; Chen, Huang et al. 2011; Gillespie, Papa & Gómez, 2017; Dawson, Lachner et al., 2018; HOD, 2010). Lau, Magarey & Wiechula (2012b) har sett på hva som kan indikere at en voldelig handling er nært forestående, og beskriver følgende pasient-interne faktorer: personen kommer med verbale trusler og trakassering, stirring, gretten atferd/holdning, anspent/stiv kroppsholdning, rastløs, skjeling med øyene, unngår øyekontakt, roper, hvisker og mumler, ikke imøtekommende ved ankomst, samarbeider ikke eller gir et uvennlig svar på en vennlig hilsen.

Går vi til årsaksfaktorer relatert til helsearbeiderne, ser vi at kommunikasjonsferdigheter er et sentralt tema (Ramacciati, Ceccagnoli et al., 2018). Riktig kommunikasjon kan bidra til å nedeskalere en potensiell voldssituasjon. Dette avhenger av helsearbeidernes formelle ferdigheter i form av opplæring, kurs og trening, personlige egenskaper og dagsform. En sliten helsearbeider har ikke samme evne til å verken detektere eller håndtere en aggressiv pasient som en opplagt helsearbeider. Dette påvirker pasientbehandlingen, helsearbeiderens privatliv og arbeidsmiljøet ved institusjonen (Wolf, Perhats et al., 2017). Helsearbeiderens tilnærming til pasienten er også av betydning. Forhold som kan fremme aggresjon og voldssituasjoner er for eksempel uforberedt invasjon av pasientens privatssfære eller en autoritær, dømmende eller konfronterende fremtoning (Lau, Magarey & Wiechula, 2012b; Shafran-Tikva, Chinitz et al., 2017). Avslag på forespørsler er også beskrevet som en vanlig trigger til aggresjon og voldshendelser. Eksempler kan være å avslag på forespørsel om: medisiner, sykemelding, retningsbeskrivelser, parkeringstillatelse, hjelp til å frakte pasienter til/fra parkeringsplass, rullestol, mat og drikke, henvisning til spesialist, røyking og innlegging (Lau, Magarey & Wiechula, 2012b; Koukia et al., 2013). Dette er interpersonale forhold som henger sammen med bl.a. pasientene og pårørende sine forventninger til personalet (interne faktorer), tilgjengelig informasjon om relevante tjenester (fysiske omgivelser) og personalets måte å respondere på forespørselen og hvordan avslaget gis. Gode kommunikasjonsferdigheter er igjen avgjørende for å unngå unødig frustrasjon og potensielle voldssituasjoner.

Av faktorer knyttet til de fysiske omgivelsene nevnes for eksempel følgende som mulige triggere for aggresjon og vold (Cutcliffe & Rihani, 2013):

- (For) høy sengetetthet og persontetthet (trengsel).
- Støy.

- Låste dører, eller følelsen av å være innestengt. Dette beskrives som en økende trend i UK etter mønster fra US. Studier viser at låste dører/rom bidrar til økt sannsynlighet for vold mot andre, mot objekter og selvskading, men sammenhengene er usikre.
- Mangel på privatliv på avdelingen.
- I tillegg til overnevnte, er også tid og venting en faktor som ofte nevnes som utløsende for aggresjon og voldshandlinger (se f.eks.: Gillespie, Papa & Gómez, 2017; Ramacciati, Ceccagnoli et al., 2018; Roche, Diers et al., 2010; Lau, Magarey & Wiechula, 2012b; Shafran-Tikva, Chinitz et al., 2017; Koukia et al., 2013). Dette kan være lang ventetid for å få behandling, for eksempel som følge av underbemanning på avdelingen eller tidsnød pga uhensiktsmessig prioritering av oppgaver på institusjonen, forsinkelser og uferdige oppgaver på avdelingen. Et annet forhold er informasjon og kommunikasjon omkring ventetid. Inkonsistent, feil og/eller utydelig informasjon om ventetid bidrar til frustrasjon og usikkerhet, som igjen kan trigge aggresjon og voldelig atferd hos pasienter eller pårørende.

d) Konsekvenser av trusler og vold

Studier av konsekvenser av trusler- og voldshandlinger peker på utvikling av symptomer på psykiske lidelser etter hendelsen. Dette kan være angst, depresjon og unnvikende atferd, post-traumatisk stress (D'Ettorre & Pellicani 2017; Hassankhani, Parizad et al. 2018). Fysiske helseplager omfatter fysiske skader, stressrelaterte kroniske tilstander og søvnproblemer. En undersøkelse fant at 26 % av de som ble utsatt for vold ble alvorlig skadet, herunder bruddskader, øyeskader og permanent funksjonshemming (d'Ettorre & Pellicani, 2017).

En annen konsekvens er trusler mot profesjonell og sosial integritet (Hassankhani, Parizad et al. 2018; Lau, Magarey & Wiechula, 2012b). Dette kan være at den som utsettes for trussel- eller voldshandlinger mister interessen for jobben, isolerer seg, blir selvbeskyttende og mindre imøtekommende, utvikler dårlige relasjoner til kolleger og gir redusert kvalitet på behandling av pasienter. Trusler mot sosial integritet omfatter for eksempel ødelagte familierelasjoner og tidkrevende oppfølgingsaktiviteter. Cutcliffe & Riahi (2013) rapporterer om lignende konsekvenser, og påpeker også at å usettes for voldshendelser kan føre til fryktbaserte responser til pasienter med voldsatferd, som igjen kan trigge mer aggresjon og vold. I tillegg påpeker de at trusler og vold mot helsearbeidere er veldig kostbart for samfunnet.

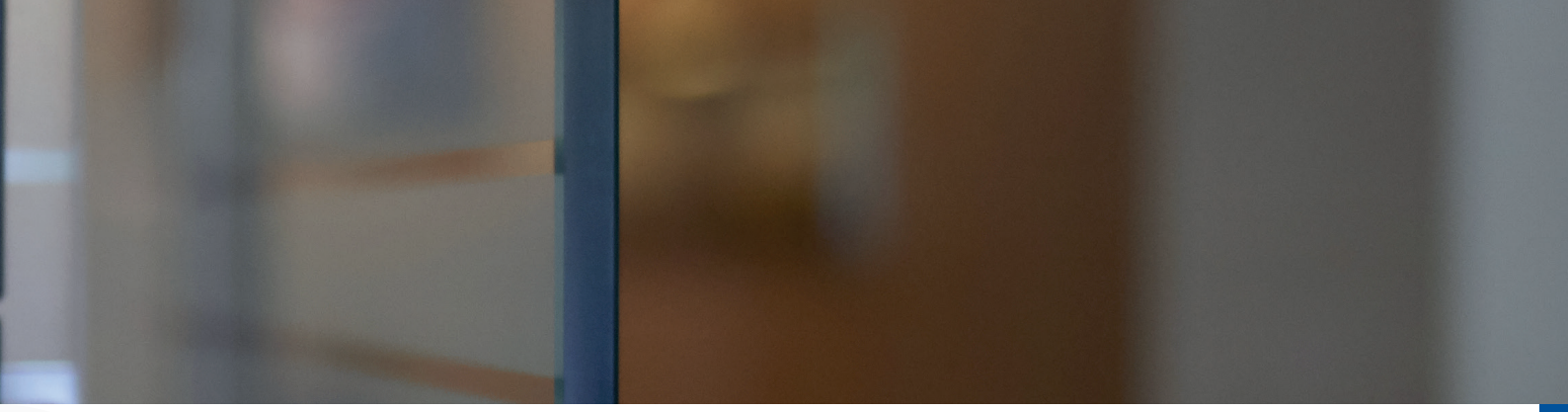
Drap på psykiatriske avdelinger betraktes som en sjelden hendelse. Samtidig er det begrenset kunnskap om fenomenet og omstendigheter rundt hendelsene (Nielssen & Large, 2012; Gordon, Oyebode & Minne, 1997).

- I perioden 1985-2010 ble 11 drap, utført av 10 pasienter, registrert på avdelinger for psykiatrisk helsevern i Australia og New Zealand. Åtte drap på psykiatriske sykehus i tiårsperioden 1955-1954 i Sverige. Seks drap over en 30 årsperiode i England og Scotland. To drap over en 13 årsperiode på en 335 sengers høysikkerhetsavdeling i Spania og 34 selvmord i samme perioden (Nielssen & Large, 2012).
- Fire drap pr 100 000 sengeår i Asutralia og 5,3 drap pr 100 000 sengeår i New Zealand (Nielssen & Large, 2012).
- Medpasienter synes å være mer utsatt med hensyn til drap enn helsearbeidere/ansatte (Nielssen & Large, 2012).
- Deler inn i tre kategorier: 1) Drap utført av akutt psykotisk pasient nært etter innleggelse, 2) drap utført av pasienter med en voldelig historie på høysikkerhets sykehus eller tvunget psykisk helsevern, og 3) drap utført av langtidspasienter (demens, kognitiv funksjonsevne og komorbid psykotisk sykdom) på sårbare medpasienter (Nielssen & Large, 2012).
- Flere av hendelsene inntraff nylig etter åpning av avdelingen/sykehuset, før rutiner og sikkerhetssystemer var skikkelig på plass (Nielssen & Large, 2012).
- 10 drap ble utført på Nederlanske psykiatriske sykehus i perioden 1988-1998 (Van Koningsveld, Colon & Raes, 2001).
- Det er registrert 16 drap og 300 selvmord i engelske fengsler i perioden 1972-1987. I spesialsykehuset (høysikkerhetssykehus) Broadmoor Hospital ble det registrert 2 drap av 194 dødsfall i 30-årsperioden 1966-1995. En svensk studie (Ekblom, 1970) beregnes individuell risiko for at en sykepleier skal bli drept til 1 i løpet av 110 000 arbeidsår eller 1 i løpet av 250 millioner arbeidstimer (Gordon et al., 1997).
- I perioden 1978-1988 ble det registrert 9 drap på sykehus i Miami, Florida, USA (Copeland, 1990).
- Drapsraten i Norge har historisk vært mellom 0,5-1,1 drap pr 100 000 innbyggere pr år. NOU 2010-3 ser spesielt på perioden 2004-2009, hvor drapsraten var 0,64 drap pr 100 000 innbyggere pr år. Av 103 gjerningspersoner bodde 11 (11 %) på «hospits/hybelhus/fengsel/institusjon.» 71 % av gjerningspersonene hadde en diagnostiserbar psykisk lidelse på gjerningstidspunktet og 75 % hadde en psykisk lidelse i løpet av livet. De vanligste psykiske lidelsene på gjerningstidspunktet var rusrelaterte diagnoser (38 %), personlighetsforstyrrelser (30 %) og schizofreni/paranoid psykose (18 %). Tidligere historie med vold, sammen med alder og kjønn (menn i aldersgruppen 17-45 år), nevnes som den viktigste indikator for fremtidig vold. Repeterende voldshendelser gjelder særlig for personer med psykisk lidelse (HOD, 2010).

- Kripos (2017) rapporterer om 25 drapssaker med 25 ofre og 29 gjerningspersoner i 2017. 83 % av gjerningspersonene var menn og 17 % var kvinner i 2017 (87 % menn i perioden 2008-2017). I perioden 2008-2017 var om lag halvparten av gjerningspersonene ruspåvirket og om lag halvparten av gjerningspersonene var tidligere domfelt.
- Drap på barnevernsinstitusjon i Asker 28. oktober 2014 (Eie, 2017). Hadde tilgang til vannkoker, spisse blyanter, tyngre kjøkkenutstyr. Trygghetsalarmen var lagt bort med vilje for å unngå å trigge gjerningspersonen.

Vold og trusler er den vanligste årsaken til registrerte skader på norske sykehus. Ved SUS er for eksempel mer enn 70 % av sakene som meldes som ansattskade relatert til vold og trusler. I perioden 2014-2018 er det i snitt registrert ca. 1200 saker på år knyttet til ansattskader forårsaket av vold og trusler ved SUS. Dette tilsvarer mer enn tre saker pr dag. Ikke alle disse sakene har ført til faktiske skader, men omfatter volds- og trusselhendelser med skader og potensielle skader (Heie, 2017).

ID	Uønsket hendelse	Potensielle trusselaktører
1	Trusler og fysisk vold mot personer på sykehuset	Ansatte (inkl. utro tjenere) Pasienter Pårørende til pasienter Leverandører Besøkende/gjester Psykisk syke Rusmisbrukere Småkriminelle gjenger Meningsmotstandere
2	Hærverk/skadeverk på utstyr, bygning m.m.	Ansatte (inkl. utro tjenere) Pasienter Pårørende til pasienter Leverandører Besøkende/gjester Psykisk syke Rusmisbrukere Småkriminelle gjenger Meningsmotstandere
3	Tyveri av utstyr, eiendeler, medisiner, informasjon m.m.	Ansatte (inkl. utro tjenere) Pasienter Pårørende til pasienter Leverandører Besøkende/gjester Psykisk syke Rusmisbrukere Småkriminelle gjenger Meningsmotstandere Organiserte kriminelle Konkurrerende institusjoner Meningsmotstandere Fremmede staters etterretning



4	Fremsettelse av trusler om alvorlig handling	Psykisk syke Småkriminelle gjenger Meningsmotstandere Fremmede staters etterretning Hackere, cyberkriminelle
5	Selvskading på sykehuset	Pasienter
6	Rømning fra sykehuset (psykisk helsevern, demens, barn m.m.)	Pasienter
7	Frihetsberøvelse av mennesker på sykehuset (gissel-situasjon, kidnapping m.m.)	Pasienter
		Pårørende til pasienter
		Psykisk syke
		Organiserte kriminelle
		Terrorister
8	Offentlig uro (f.eks. demonstrasjon) på sykehusets eiendom	Meningsmotstandere
		Småkriminelle gjenger
9	Fysisk angrep (uautorisert tilgang) på digitale systemer: informasjonstyveri, sabotasje	Organiserte kriminelle Konkurrerende institusjoner Fremmede staters etterretning Hackere/cyberkriminelle
10	Planlagt og målrettet fysisk angrep mot personer	Psykisk syke Organiserte kriminelle Fremmede staters etterretning Terrorister
11	Planlagt fysisk angrep mot kritisk funksjon eller infrastruktur	Psykisk syke Småkriminelle gjenger Meningsmotstandere Terrorister

Tabell 19 Forslag til 11 overordnede generiske trusselscenarioer og tilhørende trusselaktører

Vedlegg C: Mer om generiske trusselscenarioer

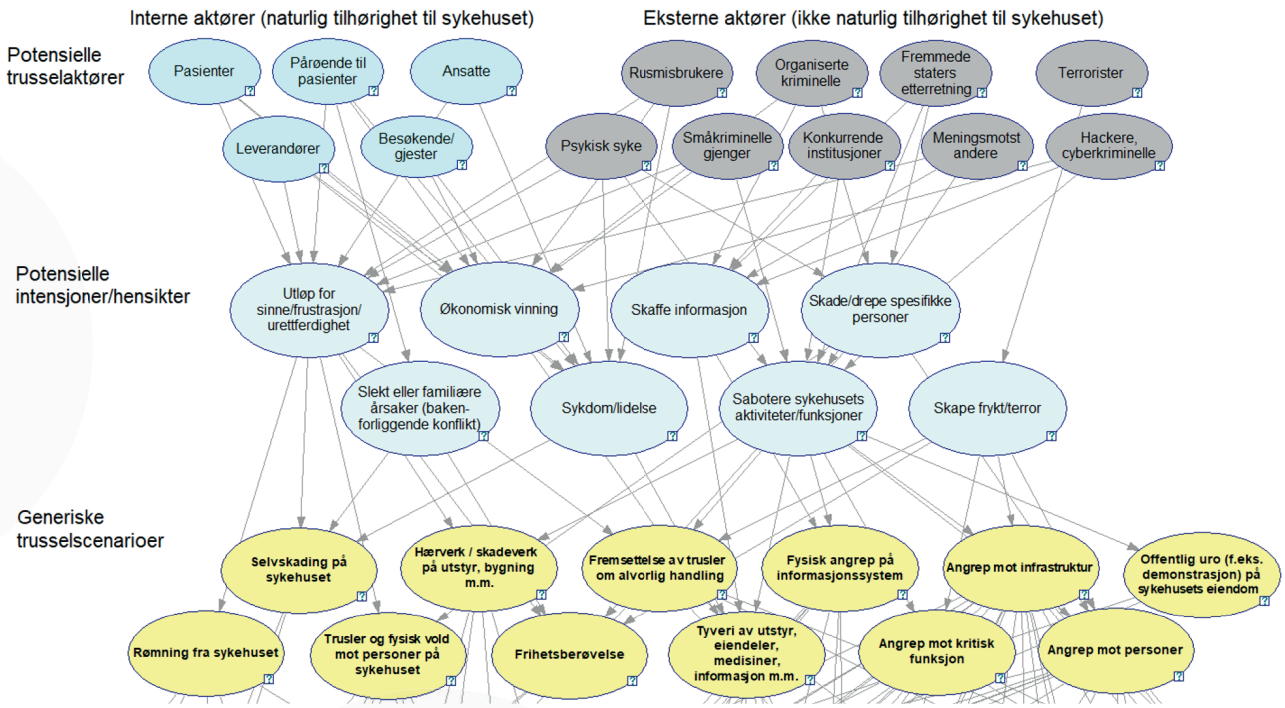
Scenarioene i veilederen er definert som tenkelige uønskede hendelser, og er systematisk bygget opp ved å kombinere de to elementene potensielle trusselaktører og trusselaktørers potensielle intensjoner/hensikter.

Bakgrunnen for de 11 generiske trusselscenarioene er illustrert i Tabell 20. De generiske scenarioene (uønskede hendelser) bygger på en kobling mellom potensielle trusselaktører (interne og eksterne) og potensielle intensjoner/hensikter. Først ble det identifisert et sett med potensielle trusselaktører i form av personer eller grupper som man enten vil finne på sykehuset (interne), og/eller i sykehusets omgivelser (eksterne). Deretter ble det identifisert et sett med potensielle intensjoner/hensikter ulike aktører vil kunne ha for å utføre en uønsket tilsiktet handling. De generiske trusselscenarioene er resultatet av å koble potensielle aktører med potensielle intensjoner.

Ett eksempel: Dersom vi kobler aktøren «pasient» med intensjonen «økonomisk vinning» kan vi få den uønskede hendelsen nr. 3: «Tyveri av utstyr, eiendeler, medisiner, informasjon m.m.». Det er verdt å merke seg at det vil kunne finnes forskjellige trusselaktører og intensjoner bak de generiske trusselscenarioene. Generisk trusselscenario nr 3 kan for eksempel også være et resultat av at aktøren «konkurrerende institusjon» har en intensjon om å «sabotere» sykehusets drift. På denne måten mener vi det er laget en relativt kortfattet liste over scenarioer med lik detaljeringsgrad. De generiske trusselscenarioene er utgangspunktet for en analyse av spesifikke trusselscenarioer, tilpasset det aktuelle sykehuset, hvor både trusselaktør og verdi er definert. Listen er ikke uttømmende, og det vil alltid være hensiktsmessig å vurdere om scenarioene er relevante for det aktuelle sykehuset, eller om det skal tilføyes flere scenarioer.

Potensielle trusselaktører, interne	Pasienter; pårørende; ansatte; leverandører; besøkende/gjester
Potensielle trusselaktører, eksterne	Rusmisbrukere; psykisk syke; organiserte kriminelle; småkriminelle gjenger; fremmede staters etterretning; konkurrerende institusjoner; meningsmotstandere; terrorister; cyberkriminelle/hackere
Potensielle intensjoner/ hensikter	Utløp for sinne/aggresjon; økonomisk vinning; skaffe informasjon; skade/drepe spesifikke personer; slekt eller familiære årsaker (bakenforliggende konflikt); sykdom/lidelse; sabotere sykehusets aktiviteter/funksjoner; skape frykt/terror
Generiske trusselscenarioer	1. Trusler og fysisk vold mot personer på sykehuset 2. Hærverk/skadeverk på utstyr, bygning m.m. 3. Tyveri av utstyr, eiendeler, medisiner, informasjon m.m. 4. Fremsettelse av trusler om alvorlig handling 5. Selvskading på sykehuset 6. Rømning fra sykehuset (psykisk helsevern, demens, barn m.m.) 7. Frihetsberøvelse av mennesker på sykehuset (gisselsituasjon, kidnapping m.m.) 8. Offentlig uro (f.eks. demonstrasjon) på sykehusets eiendom 9. Fysisk angrep (uautorisert tilgang) på digitale systemer: informasjonstyveri, sabotasje 10. Planlagt og målrettet fysisk angrep mot personer 11. Planlagt fysisk angrep mot kritisk funksjon eller infrastruktur

Tabell 20. Beskrivelse av bakgrunnsvariabler for etablering av 11 generiske trusselscenarioer.



Figur 16. Nettverk som viser koblingen mellom potensielle trusselaktører og potensielle intensjoner/hensikter og generiske trusselscenarioer. Angrep mot infrastruktur og kritisk funksjon er slått sammen til ett generisk trusselscenario i veilederen.

Del 7. Litteraturliste

ASD (2005). Arbeidsmiljøloven. Arbeids- og sosialdepartementet, LOV-2005-06-17-62.

Sykehuspartner (2018). Lærdommer etter angrepet mot Helse Sør-Øst. Presentasjon v/Christan Jacobsen, 28.11.2018. Web-adresse: https://ehelse.no/normen/presentasjoner/_/attachment/download/873e1a33-b003-43df-950e-14c6b-014b7cd:a878183a24f43fefc54138e61d-beb4d0946d977b/1300_jacobsen_angrep_mot_HSO.pdf

Aven, T. (2003). Foundations of risk analysis: a decision-oriented perspective. Chichester: Wiley.

Aven, Terje (2007). A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering and System Safety 2007;92:745-754.

Aven, Terje (2010). On how to define, understand and describe risk. Reliability Engineering and System Safety 2010;95:623-631.

AG (2018). Protective Security Policy Framework. Section 3: Security planning and risk management. Australian Government (AG), Attorney-General's Department, v2018.1.

FD (2019). Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften). Forsvarsdepartementet (FD). FOR-2018-12-20-2053.

FEMA (2011). Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings. FEMA-426/BIPS-06/October 2011, ed. 2. Department of Homeland Security.

FFI (2015). Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. Forsvarets Forskningsinstitutt.

FFI (2017). Hvordan kommunisere det vi ikke vet? En kvalitativ studie om risikoforståelse og risikokommunikasjon i en terrorismekontekst. Forsvarets Forskningsinstitutt.

FFI (2018). Hva er egentlig verdivurdering? Forsvarets Forskningsinstitutt.

FFI (2018). Sannsynligheter og usikkerheter – begrepsavklaring i forbindelse med risikovurderinger. Forsvarets Forskningsinstitutt.

Hagen, I. M. (2019). Vold og trusler – et stort arbeidsmiljøproblem i helse- og sosialsektoren. Forskningsstiftelsen FAFO.

Heie, Kjersti (2016). Styresak 67/16 Tiltaksplan vold og trusler. Helse Stavanger, Stavanger Universitetssykehus. Underlag til styremøte 20.09.16.

7

HelseCERT (ikke datert). Risikobildet for helsesektoren. Digitale helsetrender, trusselbildet, cyberangrep og anbefalinger. Presentasjon v/Gunnar A. Johansen. Web-adresse: https://ehelse.no/styrer-og-utvalg/nufa-fagutvalget/_/attachment/download/bc138ddf-8138-4018-9473-35299fb0cd1c:48ba1fa6ad0e-4812ec7833cbf1573e62ccea95ce/Sak%2033-19%20HelseCERT.pdf

HSØ (udatert). Sikringsrisikoanalyse i sykehus. En veileder for helseforetakene i Helse Sør-Øst. Helse Sør-Øst (HSØ).

ISO (2018). NS-ISO 31000:2018 Risikostyring - Retningslinjer. Standard Norge, Lysaker.

JBD (2019). Lov om nasjonal sikkerhet (sikkerhetsloven). Justis- og beredskapsdepartementet (JBD). LOV-2018-06-01-24.

JBD (2015). Fastsetting av Sivilt Beredskapssystem (SBS). Delegering av myndighet. FOR-2015-04-10-347.

Lindley, D. (2006). Understanding uncertainty. Hoboken, N.J.: Wiley.

NKSB (2016). Sikringshåndboka – Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje, spionasje og annen kriminalitet. Nasjonalt kompetansesenter for sikring av bygg (NKSB), Forsvarsbygg, desember 2016 (2. utgave).

SN (2008). NS 5814:2008 Krav til risikovurderinger. Standard Norge (SN), Lysaker.

SN (2012). NS 5830:2012 Samfunnssikkerhet, terminologi. Standard Norge (SN), Lysaker.

SN (2014). NS 5832:2014 Krav til sikringsrisikoanalyse. Standard Norge (SN), Lysaker.

SN (2019). NS 3960:2019 Brannalarmanlegg – Prosjektering, installasjon, drift og vedlikehold. Standard Norge (SN), Lysaker.

Sykehusbygg (2017). Veileder for tidligfasen i sykehusbyggprosjekter. Sep./okt. 2017.

Talbot, J. & Jakeman, M. (2009). Security Risk Management – Body of Knowledge (SRMBOK). Wiley.

Wedervang-Resell, A., Østraat, I.E., Haga, M., Klingenberg, E. & Berglund, K. (2017). Kartlegging av vold mot helsepersonell og medpasienter. Helsedirektoratet Rapport IS-2618, 07/2017.

York, T.W. & MacAlister, D. (2015). Hospital and Healthcare Security, 6th Edition. Butterworth-Heinemann.

Referanser til vedlegg om vold og trusler i helseinstitusjoner

Arbeidstilsynet (2017). Vold og trusler i forbindelse med arbeidet: Forebygging, håndtering og oppfølging. Arbeidstilsynets publikasjoner best.nr. 597, februar 2017.

Carr, V.J., Lewin, T.J., Sly, K.A., Conrad, A.M., Tirupati, S., Cohen, M., Ward, P.B. & Coombs, T. (2008). Adverse incidents in acute psychiatric inpatient units: rates, correlates and pressures. Aust N Z J Psychiatry 2008;42:267-82.

Chen, W-C., Huang, C-J., Chen, C-C., & Wang, J-D. (2011). The Incidence and Risk Factors of Workplace Violence towards Female Nurses Reported via Internet in an Acute Psychiatric Hospital, Archives of Environmental & Occupational Health, 66:2, 100-106.

Copeland, A.R. (1990). Homicide in the hospital. Journal de Medecine Legale Droit Medical 33(3), pp. 159-164.

Cutcliffe, J.R. & Riahi, S. (2013). Systemic perspective of violence and aggression in mental health care: Towards a more comprehensive understanding and conceptualization: Part 1. International Journal of Mental Health Nursing (2013) 22, 558–567.

Dawson, N.L., Lachner, C., Vadeboncoeur, T.F., Maniaci, M.J., Bosworth, V., Rummans, T.A., Roy, A. & Burton, M.C. (2018). Violent behavior by emergency department patients with an involuntary hold status. American Journal of Emergency Medicine 36 (2018) 392–395.

d'Ettorre, G. & Pellicani, V. Workplace Violence Toward Mental Healthcare Workers Employed in Psychiatric Wards. Safety and Health at Work 8 (2017) 337-342.

Eie, B. (2017). På jobb med barn som vil/kan drepe. Om arbeidet med å sikre ansatte mot vold og trusler i en barnevernsinstitusjon med et traumebevisst fokus. Masteroppgave i Samfunnssikkerhet ved Universitetet i Stavanger, våren 2017.

Geoffrion S., Goncalves, J., Sader, J., Boyer, R., Marchand, A. & Guay, S. (2017). Workplace aggression against health care workers, law enforcement officials, and bus drivers: Differences in prevalence, perceptions, and psychological consequences. Journal of Workplace Behavioral Health, 32:3, 172-189.

Gillespie, G. L., Papa, A. M. & Gómez, L. C. (2017). Workplace Aggression in Cuban Health Care Settings. Journal of Transcultural Nursing 2017, Vol. 28(6) 558–565.

Gordon, H., Oyebode, O. & Minne, C. (1997). Death by homicide in Special Hospitals. Journal of Forensic Psychiatry, 8:3, 602-619.

Hahn, S., Müller, M. Hantikainen, V., Kok, G., Dassen, T. & Halfens, R.J.G. (2013). Risk factors associated with patient and visitor violence in general hospitals: Results of a multiple regression analysis. International Journal of Nursing Studies 50 (2013) 374–385.

Hassankhani, H., Parizad, N., Gacki-Smith, J., Rahmani, A. & Mohammadi, E. (2018). The consequences of violence against nurses working in the emergency department: A qualitative study. International Emer-

gency Nursing 39 (2018) 20–25.

Heie, Kjersti (2016). Styresak 67/16 Tiltaksplan vold og trusler. Helse Stavanger, Stavanger Universitetssykehus. Underlag til styremøte 20.09.16.

HOD (2010). NOU 2010-3: Drap i Norge i perioden 2004-2009. Utredning fra utvalg oppnevnt ved kongelig resolusjon 24. april 2009. Avgitt til Helse- og omrsorgsdepartementet 3. mai 2010.

Koukia, E., Mangoulia, P., Gonis, N. & Katostaras, T. (2013). Violence against health care staff by patient's visitor in general hospital in Greece: Possible causes and economic crisis. Open Journal of Nursing 3 (2013).

Kripos (2017). Nasjonal drapsoversikt 2017: Drap i Norge 2008-2017. Politiet, KRIPOS, Oslo.

Lau, J.B.C., Magarey, J. & Wiechula, R. (2012a). Violence in the emergency department: An ethnographic study (part I). International Emergency Nursing (2012) 20, 69-75.

Lau, J.B.C., Magarey, J. & Wiechula, R. (2012b). Violence in the emergency department: An ethnographic study (part II). International Emergency Nursing (2012) 20, 126–132.

Morken, T., Baste, V., Johnsen, G.E., Rypdal, K., Palmstierna, T. & Johansen I.H. (2018). The Staff Observation Aggression Scale – Revised (SOAS-R) – adjustment and validation for emergency primary health care. BMC Health Services Research (2018) 18:335.

McDermott, B.E., Dualan, I.V. & Scott, C.L. (2011). The Predictive Ability of the Classification of Violence Risk (COVR) in a Forensic Psychiatric Hospital. PSYCHIATRIC SERVICES, April 2011 Vol. 62 No. 4.

Nielssen, O. & Large, M.M. (2012). Homicide in psychiatric hospitals in Australia and New Zealand. Psychiatr Serv 2012;63:500-3.

Nijman, H.L.I., á Campo, J.M.L.G., Ravelli, D.P. & Merckelbach, H.L.G.J. (1999). A Tentative Model of Aggression on Inpatient Psychiatric Wards. PSYCHIATRIC SERVICES, June 1999 Vol. 50 No. 6.

Ramacciatia, N., Ceccagnoli, A., Addey, B. & Rasero, L. (2018). Violence towards Emergency Nurses. The Italian National Survey 2016: A qualitative study. International Journal of Nursing Studies 81 (2018) 21–29.

Ramesha, T., Igoumenoub, A., Montesc, M.V. & Fazela, S. (2018). Use of risk assessment instruments to predict violence in forensic psychiatric hospitals: a systematic review and meta-analysis. European Psychiatry 52 (2018) 47–53.

Roche, M., Diers, D., Duffield, C. & Catling-Paull, C. (2010). Violence Toward Nurses, the Work Environment, and Patient Outcomes. Journal of Nursing Scholarship, 2010; 42:1, 13–22.

Roche, M., Diers, D., Duffield, C. & Catling-Paull, C. (2010). Violence Toward Nurses, the Work Environment, and Patient Outcomes. Journal of Nursing Scholarship, 2010; 42:1, 13–22.

Shafran-Tikva, S., Chinitz, D., Stern, Z. & Feder-Bubis, P. (2017). Violence against physicians and nurses in a hospital: How does it happen? A mixed-methods study. Israel Journal of Health Policy Research (2017) 6:59.

Van Koningsveld, Colon & Raes (2001). Homocides commited in General Psychiatric Hospitals. A research study over the period 1988-1998. Tijdschrift voor Psychiatrie 43(1), pp. 49-53.

Wolf, L. A., Perhats, C., Clark, P. R., Moon, M. D. & Zavotsky, K. E. (2018). Workplace bullying in emergency nursing: Development of a grounded theory using situational analysis. International Emergency Nursing 39 (2018) 33–39.

Wolf, L. A., Perhats, C., Delao, A.M. & Clark, P. R. (2017). Workplace aggression as cause and effect: Emergency nurses' experiences of working fatigued. International Emergency Nursing 33 (2017) 48–52.

Annen relevant litteratur

Department of Veterans Affairs (2010). Design guide for Mental Health Facilities.

Department of Health (1993). Design guide. Medium secure psyciatric units. NHS Estates.

IAHSS (2012). Security design guidelines for healthcare facilities. International Association for Healthcare Security & Safety.

Nasjonal sikkerhetsmyndighet (NSM): Diverse veiledere på sikringsrelaterte tema. https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/

Veileder for sikring av bygg og infrastruktur
i sykehusbyggprosjekter