Prosjektoppgave i Risikobasert styring

Våren 2020

Universitetet i Stavanger

"Hvordan kan to forskjellige risikomodeller supplere hverandre ved analyse av sikring?"

Forfattere:

Gudmestad, Martine (1025)

Haakonsen, Geir (1039)

Hernes, Magne Misund (1026)

McCabe, Christopher (1033)

Midtlien, Caroline Seim (1028)

Mydland, Tyra (1004)

Øverland, Sunniva (1013)

Forord

Sommerferien 2020 har aldri vært nærmere, og vi kan med dette konstatere at prosjektoppgaven i risikobasert styring er ferdig. Semesteret har vært intenst, men det har gitt oss mye og vært utrolig lærerikt. I undervisningen tok faglærer flere ganger opp situasjonen som var i Kina og Italia. Vi ser alle nå at et trygt og lite land som Norge også kan bli rammet av farlige virus. Covid-19 medførte plutselige forandringer i studie og arbeidshverdagen for oss alle. Norge ble stengt ned, noe som aldri har skjedd før i freds tid. Situasjonen er enn så lenge stabil, og derfor ønsker vi å bruke tiden for takksigelser og godord.

Takk til alle på Universitetet i Stavanger, det er en flott arena for god kunnskapsutvikling.

Takk til Ove Njå, som kom opp med forslag til tema, og med gode tips i løpet av hele semesteret.

Stavanger, 2020

Sammendrag

Bakgrunn:

Den nye sikkerhetsloven har satt et større søkelys på hvordan man planlegger for sikring av objekter som huser samfunnskritisk infrastruktur og kritiske samfunnsfunksjoner. Å avdekke risiko og presentere risikobilde tilbys gjennom flere ulike analysemodeller. Hver og en av disse modellene forsøker å gi brukeren et mest mulig korrekt risikobilde av analyseobjektet. Prosjektgruppen har valgt ut to analyseverktøy, VTS og Grovanalyse, for å se hvilke risikobilder hver og en av disse belyser av et nylig ferdigstilt byggeprosjekt som inneholder offentlige kritiske samfunnsfunksjoner.

Formål:

Hensikten med prosjektoppgaven var å svare på følgende problemstilling:

"Hvordan kan to forskjellige risikomodeller supplere hverandre ved analyse av sikring?"

Med denne problemstillingen er formålet å se på resultatet av to ulike analyseverktøy. Vil de gi to ulike fremstillinger av risikobilde, eller danner fremgangsmåten et bedre grunnlag for sikring.

Metode:

For å svare på denne problemstillingen delte prosjektgruppen seg i to, og utførte hver sin risikoanalyse. Det var først når begge analysene var utført at disse ble presentert for den andre gruppen. Gruppene benyttet dokumentanalyse til funnene, metoden for sammenligning av analysene ble utført gjennom triangulering og komparasjon.

Konklusjon:

Våre funn baserer seg på den brede og sammensatte erfaringen prosjektgruppens medlemmer har om sikkerhetsarbeid, kombinert med tilgjengelige dokumenter og informasjon om Sola rådhus. Etter gjennomførte analyser, som hver og en danner et risikobilde basert på ulike fremgangsmåter, konkluderer prosjektgruppen med at det er en positiv side ved å benytte seg av flere analyseverktøy. Svakheter og styrker i hver av analysene utfyller hverandre på en positiv måte, og sammen presenterer de et bredere risikobilde. Vi vil imidlertid påpeke at ingen av de analysemetodene, som ble vurdert i dette arbeidet, sier noe om usikkerhetene i resultatene fra analysene.

Innholdsfortegnelse

1. Innledning

1.1 Bakgrunn

Prosjektoppgaven ser på to ulike analyseverktøy for å fremstille et risikobilde for et ferdigstilt byggeprosjekt, som inneholder offentlige kritiske samfunnsfunksjoner. Som objekt for analysen har vi valg det nye Sola rådhus.

Den nye sikkerhetsloven trådte i kraft 1. januar 2019, og skal jamfør § 1-1 bidra til å *"a) trygge Norges suverenitet, territoriell integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, b) forebygge, avdekke og motvirke sikkerhetstruende virksomhet og c) sikre at sikringstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn*" (Sikkerhetsloven, 2019). På bakgrunn av dette mener vi det er interessant å se hvordan nye moderne byggeprosjekter ivaretar sikring av verdier.

Med den nye sikkerhetsloven har det blitt et større søkelys på hvordan man sikrer samfunnskritisk infrastruktur og kritiske samfunnsfunksjoner. Noe som vil gi utslag i hvilke sikringstiltak som prosjekteres og må tas hensyn til.

For å besvare problemstillingen har vi valgt å innhente offentlig tilgjengelig informasjon, relevant teori og analysere dataene gjennom to ulike risikoanalyser. De to risiko-analysemodellene vi har valgt er sikringsrisikoanalyse (VTS) og en grovanalyse. Disse analysene er valgt da gruppen har en hypotese om at de supplerer hverandre.

1.2 Oppgavens relevans

I prosjekter hvor bygg skal huse kritiske samfunnsfunksjoner benyttes ulike analyseverktøy for å komme frem til hvordan en ivaretar sikkerheten. Utrykk som grovanalyse, Bow-tie og risikoanalyse er blitt allmenn kjente. Begrepene er utredet gjennom ulike veiledere, slik at ansatte ikke nødvendigvis må ha lang utdanning innenfor risikofagfeltet for å kunne gjennomføre en analyse. Denne utviklingen gjør det relevant å utforske analyseperspektivene og blant annet se på hva våre to utvalgte analyser kan gi svar på.

I et historisk perspektiv vil vi kunne finne argumenter for at et kommunehus ikke behøver sikres i større grad enn vanlig tyverisikring. I de senere år har vi derimot sett en dreining i aksjoner mot politiske mål i Norge, som f.eks. terrorangrepene 22.juli 2011 og aksjoner mot kommunene i forbindelse med utvidelse av bomringene på Nord-Jæren, som bl.a. resulterte i

at politiet måtte beskytte politikere mot demonstranter i bystyresalen (Munkvik & Norheim, 2018). Dagens situasjon, med en stadig mer truende klimatrussel og pågående global viruspandemi, kan det ikke utelukkes at lokaldemokratiske institusjoner, som et kommunehus, vil kunne bli rammet av ulike former for skadelig aktivitet.

I Sola kommune ligger det kritisk infrastruktur knyttet til bl.a. olje- og gassnæringen og transportsektoren (herunder Stavanger flyplass, Sola). Kunnskap om denne infrastrukturen kan være av interesse for fremmede stater, selskaper og aksjonister. Politisk saksbehandling og beslutninger knyttet til denne infrastrukturen kan bli behandlet i Sola rådhus, og disse prosessene kan være av interesse for trusselaktører.

Vi ønsker i denne oppgaven å se på hvilke funksjoner det nye rådhuset på Sola inneholder. Er det slik at flere av kommunens kritiske samfunnsfunksjoner er plassert under samme tak, og i hvilken grad spiller dette en rolle for risikoanalysene for rådhuset.

1.3 Problemstilling, forskningsspørsmål og avgrensning

Temaene sikring, verdier, trusler og sårbarhet videreføres fra prosjektoppgaven i faget SAM500. I denne prosjektoppgaven gjennomføres to dybdeanalyser. Analyse av verdi, trussel og sårbarhet (VTS) og analyse av sannsynlighet og konsekvens gjennom grovanalyse. For å belyse sentrale forskjeller eller likheter vil funnene fra hver analyse bli sammenlignet. Sola rådhus, et ferdigstilt prosjekt, benyttes som objekt i denne oppgaven.

Problemstillingen for oppgaven er:

"Hvordan kan to forskjellige risikomodeller supplere hverandre ved analyse av sikring?"

For å besvare problemstillingen har vi utformet følgende forskningsspørsmål:

1. Hvordan tilnærmer de forskjellige analysemetodene seg til sikring av et bygg?
2. Gir en av analysemodellene tilstrekkelige resultater til å overskygge den andre?
3. Hvilke svakheter og styrker fremkommer av å gjennomføre to forskjellige risikoanalyser?

For å avgrense oppgaven velger vi å fokusere på bygget i sin helhet og de verdiene som bygget innehar. Dette med tanke på publikum, ansatte og tjenestefunksjoner. Det vil derfor ikke gjennomføres analyser basert på Sola kommune i sin helhet. Data for oppgaven baserer seg på dokumentanalyse. På grunn av Covid-19 har mulighetene til å gjennomføre intervjuet

vært redusert. Aktørene som kan utføre uønskede hendelser, blir ikke spesifisert eller navngitt. Vi ønsker å oppnå et beskrivende sannsynlighetsgrunnlag istedenfor tallmessig vurdering av sannsynlighet. Oppgaven bygger derfor på kvalitativ metode.

1.4 Oppgavens struktur

I prosjektoppgaven starter vi med å beskrive bakgrunn for valg av tema og dens relevans i dagens samfunn. Systembeskrivelse for Sola rådhus (kapittel 2). Videre følger et teorikapittel (kapittel 3) med gjennomgang av relevant pensum for tema. I metodekapittelet (kapittel 4) går vi gjennom fremgangsmåten vår, her beskrives dokumentanalyse, analysemetodene VTS- og grovanalyse, metodetriangulering og til slutt komparativ metode. I kapittel 5 presenteres resultatene fra VTS- og grovanalysen. Våre funn analyseres i kapittel 6. I den avsluttende drøftingen (kapittel 7) tolkes og drøftes funnene gjort i oppgaven, sett opp mot eksisterende og relevant teori fra pensum. Arbeidet er oppsummert i konklusjonen (kapittel 8).

2. Systembeskrivelse

Vi har valgt å gjennomføre en VTS-analyse og en grovanalyse av nye Sola rådhus, oppført i Sola sentrum. Sola kommune har i overkant av 27 000 innbyggere.

2.1 Nytt Sola rådhus

Sola kommune sitt nye rådhus stod ferdig desember 2019 og er arbeidsplass for omtrent 345 ansatte (Sola kommune, 2020a). Rådhuset ligger i nærheten av spisesteder, hotellnæring, butikker, jordbruk, militær virksomhet, flyplass og annen næringsvirksomhet.

Bilde 1 Fasade mot nord med åpen plass og parkanlegg. Hovedinngang midt i bildet, på hjørne mellom fasade mot nord og fasade mot øst. Foto: Geir Haakonsen

Sola kommune og prosjektleder Magne Olav Bergesen var byggherre for rådhuset, og det er tegnet av Longva arkitekter AS, Oslo v/Knut Longva, Nils Köplin, Ewan Smith og Mille Mee Herstad som vant skissekonkurransen i 2015. Consto Sør har gjennomført prosjektet i en totalentreprise (Dale, 2020). Prosjektet innebar oppføring av nytt rådhus, som skulle knyttes sammen med eksisterende fløy D med Rådhusgaten og Rådhustorget. Fløy D har blitt totalrehabilitert (Longva arkitekter, 2015). Prosjektet omfattet et fire etasjers nybygg på 9500 kvadratmeter, rehabilitering på 2400 kvadratmeter og en parkeringsetasje på 5500 kvadratmeter. Ved siden av rådhuset er det bygget et offentlig parkeringsanlegg beregnet til

164 biler. Bygningsarbeidet begynte i april 2018 og ble ferdig november 2019 (Dale, 2020). Sola kommune beskriver bygget, som et åpent og tilgjengelig bygg, som bidrar til en positiv opplevelse i Sola sentrum (Sola kommune, 2020a). Det skal være en arena hvor befolkning, administrasjon og politisk ledelse møtes til hverdag og til fest (Longva arkitekter, 2015). Bygget har store rom med fleksibel utforming og er tilrettelagt for cellekontorer, teamkontorer, åpne landskap og minst mulig korridorer. Rådhuset skal være fleksibelt i bruk og robust for endringer (Longva arkitekter, 2015). Juryen for Nytt Sola rådhus kommenterte enkelte egenskaper ved organisering og utforming som er verdt å ta med seg:

"Servicetorget er plassert i foyeren, tett ved byggets hovedinngang og resepsjon. Plasseringen er synlig og god, men arealet er alt for lite og funksjonen antakelig ikke helt forstått. Husets hoveddisposisjon er god, ved at ***arbeidsplassene er godt skjermet fra publikumssonene****. Bystyresalen er plassert sentralt i nybyggets 1. etasje, med direkte kontakt med resepsjonsarealet og synlig eksponert mot rådhusplassen utenfor. Forfatteren har sett dette som et sentralt poeng, og betegner salen som "Solas hjerte", slik utkastets motto lyder. Juryen ser verdien i dette, men er likevel* ***noe i tvil om plasseringen er for fremskutt og med manglende vrimleareal, garderobe og forrom*** *(...)"* (Norske arkitekters landsforbund, 2015, ss. 10-13).

2.2 Samlokalisering av kritiske samfunnsfunksjoner

Rådhuset rommer kommunale kjernefunksjoner som kommunestyre- og formannskap, tjeneste- og koordineringskontoret (TKK), boligkontoret, servicetorget, politisk sekretariat, helsestasjon, familiesenter, ungdomsteam, PPT, barnevern og NAV (Sola kommune, 2020a). Fjorten kritiske samfunnsfunksjoner er definert av Direktoratet for samfunnssikkerhet og beredskap (DSB) i rapporten *Samfunnets kritiske funksjoner* (DSB, 2016). Som en følge av Covid-19-pandemien har departementene utarbeidet en liste som tydeliggjør sentrale personellgrupper og virksomheter for opprettholdelse av drift av kritiske samfunnsfunksjoner. Listen inkluderer bl.a. ansatte i barnevern, skole/barnehage, styring og kriseledelse, forsvar, lov og orden, helse og omsorg (Regjeringen, 2020).

På neste side lister vi opp funksjonene som er særlig kritiske tilknyttet Sola rådhus satt opp imot KIKS (DSB, 2016) og liste over samfunnsfunksjoner:

KIKS-kategori	Samfunnsfunksjon	Funksjon i Sola rådhus
Styringsevne og suverenitet	Styring og kriseledelse, herunder konstitusjonelle organer og forvaltningen samt Beredskap og kriseledelse	• Kommunestyret og politiske underorgan • Kommunens ledergruppe • Kommunens kriseledelse • Kommunens forvaltning for øvrig
Befolkningens sikkerhet	Helse- og omsorgstjenester, inkludert folkehelsearbeid	• Kommunestyret og politiske underorgan • Kommunens ledergruppe • Stab Levekår • Tjeneste- og koordineringskontor • Oppvekst og kultur • PPT • Boligkontor • Stab samfunnsutvikling • Barnevern • NAV Sola • Sektorovergripende folkehelseforum bestående av skolesjef, kultursjef, barnehagesjef, leder for barn, ungdom og familietjenesten, plan og bygningssjef, kommuneoverlege, NAV-leder, Folkehelsekoordinator/kommuneplanlegger
IKT-sikkerhet i sivil sektor	Sikre registre, arkiver, hendelseshåndtering i informasjons- og kommunikasjons-systemer, personvern	• Kommunestyret og politiske underorgan • Kommunens ledergruppe • IKT • Dokumentsenter • Kommunens forvaltning for øvrig • NAV Sola

Tabell 1 Liste over kritiske samfunnsfunksjoner tilknyttet Sola rådhus

2.2.1 Sola kommunes kriseledelse

I Sola kommunes overordnede beredskapsplan (Sola kommune, 2015) kommer det frem at kommunens strategiske kriseledelse består av rådmannens ledergruppe, ordfører, beredskapsleder og eventuelle rådgivere/ressurspersoner. Rådmannen leder kriseledelsen. Alle i kriseledelsen har stedfortredere hvis noen skulle være forhindret å møte opp.

Kriseledelsen mobiliseres i rådmannens møterom i 2. etasje i rådhuset, dersom annet ikke er kommunisert ut. Det er ikke å finne en alternativ mobiliseringsplan, hvis rådhuset skal være satt ut av drift. Det vil være nødvendig å se nærmere på hvor stedfortrederene har tilhold, og om alle har tilhold på rådhuset. Hvis en uønsket hendelse skulle skje på rådhuset, er det viktig å kartlegge hvem som eventuelt kan være satt ut av spill.

Videre fremkommer det av den overordnede beredskapsplanen at initiering av krisestab utføres av kriseledelsen. Dette er en støtteenhet som leder og koordinerer håndteringen av krisen. Krisestaben settes ut ifra hvilket tjenesteområde/virksomhet som blir berørt og består av stabssjef, leder for kommunikasjon, leder for operasjon og rådgivere tilpasset den aktuelle beredskapssituasjonen. Krisestab mobiliseres i formannskapssalen i rådhuset.

2.3 Sikringstiltak nye Sola rådhus

Sikringstiltak i det nye Sola rådhus er ikke et stort tema. I førstegangsbehandling av detaljregulering *Kommunehus, bypark og rådhusplass* fremkommer det ett spesifikt kriminalitetsforebyggende tiltak *"det skal sikres oversiktlige og godt belyste adkomstforhold, møteplasser, uteoppholdsarealer og gårdsrom"* (Sola kommune, 2016a). I samme dokument kommenteres følgende kriminalitetsforebyggende tiltak:

"Forslagstiller har ikke vurdert kriminalitetsforebyggende tiltak spesielt. Planen legger til rette for offentlig tjenesteyting/administrasjon og kontorer innenfor et sentrumsområde. De ulike funksjonene er plassert slik at det finnes god mulighet for sosial kontroll av både byhagen/byparken og gang- og sykkelveger, og bygninger (internt og eksternt). Rådmannen vurderer dette som svært positivt. Offentlige uterom får belysning i høy standard, og blir utformet i høy kvalitet, noe som skal forebygge kriminalitet. De ulike kriminalitetsforebyggende tiltak er tilfredsstillende. Rådmannen tolker bestemmelsene slik at formingsveileder og utomhusplaner, Solas hjerte og Juryrapporten for arkitektkonkurransen, samt godkjenning av planer ved Park og gravlund sikrer at belysning og beplantning blir

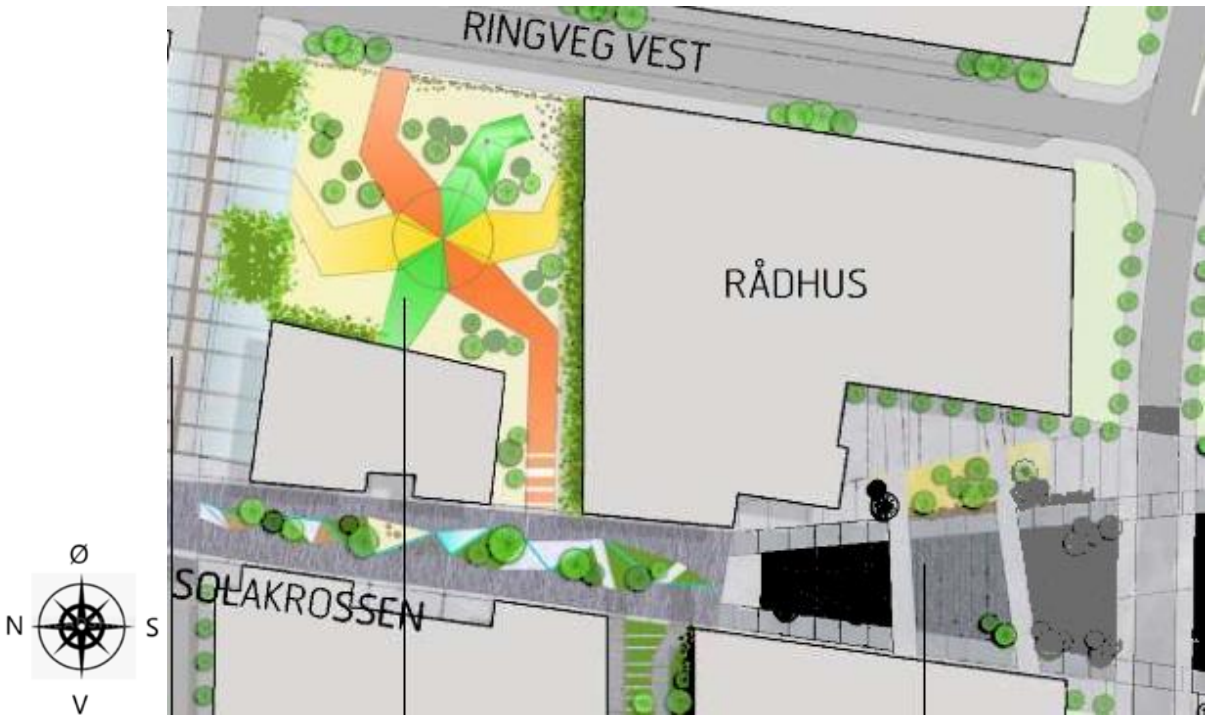
gjennomført slik at oppholdssoner og gangforbindelser oppleves som trygge" (Sola kommune, 2016b, s. 21).

Andre sikringstiltak som er iverksatt eller som planlegges er:

- Egen ansattinngang, egen publikumsadkomst for resepsjon, kantine og bystyresal, samt en skjermet adkomst for publikum til oppvekstenheten.
- Publikumsfunksjoner skal være adskilt fra rene kontorarbeidsplasser.
- Telenor har en fibersentral nær rådhuset (Dale, 2020).
- Det er etablert en ny nettstasjon som vil forsyne rådhuset med strøm. Det er Lyse som har ansvaret for denne (Sola kommune, 2016c).
- I kommunestyresalen er det en forgylt håndrekke som skiller publikum fra politikerne (Knutsen & Christensen, 2019)
- Det er kodelås på møterommene (Knutsen & Christensen, 2019)
- Hindring av påkjørsel av myke trafikanter på torget. *"Vegen over torget […] skal utformes som sambruksareal og avskjermes fra torget ved bruk av elementer som hindrer påkjørsel av myke trafikanter"* (Sola kommune, 2016a)
- Stenge Rådhusveien for trafikk. *"sikre tilfredsstillende fremkommelighet for kollektivtrafikk, skal V07 (Vestre Ringveg) i områdeplan 0442 være etablert, før det kan settes i gang tiltak som medfører permanent stenging av Rådhusvegen"* (Sola kommune, 2016a)
- Bilfritt torg. *"(Torg) skal være bilfritt, men kjørbart for utrykningskjøretøy, vedlikehold/service varelevering for tilstøtende byggeområder"* (Sola kommune, 2016a)
- Belysningsplan for uteområdet (Multiconsult, 2016)

I formingsveileder for Sola sentrum er det uttalt at rådhusplassen skal utformes med beplanting, kunstelementer og møblering (Multiconsult, 2016). Foran rådhuset vil det blant annet plasseres en lund med trær og møbler som er fastmonterte, samt et amfi i massivt tre. Det vil også monteres permanente stålrammer med utstillinger som er utskiftbare (se figur 3 for illustrasjon). Veien, som går mellom Rådhuset og kirken, skal være opphøyet og elementer på begge sidene av veiene vil hindre påkjørsel. Blokker i tre eller stein vil tas i bruk istedenfor å bruke pullerter. Dette skal ifølge (Multiconsult, 2016) være *"en integrert del av det arkitektoniske uttrykk"*. Ved gågaten på siden av rådhuset vil det også tas i bruk grøntarealer, samt vannelementer (Multiconsult, 2016). Dette er noe som kan sees på som

tiltak som innlemmes i byrommet, der funksjonen både kan være til bruk for allmennheten og kan fungere som sikringstiltak til selve rådhuset. "Superlekeplassen" på sørsiden av rådhusbygget skal ifølge (Multiconsult, 2016) sikres mot vei, noe som vil si at det ikke vil være mulig å komme nær denne siden av bygget med kjøretøy. Veiene rundt rådhuset og rådhusplassen vil ha opphøyet gangfelt, plantesone og møbleringssone, noe som kan virke effektivt mot at kjøretøy kommer nær rådhusbygget.



Bilde 2 Illustrasjon av rådhuset. Hentet fra (Multiconsult, 2016)

3. Teori

Teorikapittelet tar for seg ulike begrep, som er vesentlige for sikringsrisikoanalyse VTS-analyse og grovanalyse med bow tie-analyse. I det følgende vil begrepene risiko, usikkerhet, verdi, trussel og sårbarhet utdypes med utgangspunkt i både pensumlitteratur og annen relevant litteratur.

3.1 Risiko

Analysemodellene brukt i denne oppgaven kalles risikomodeller. Risiko er derfor et grunnleggende begrep og sentralt i denne oppgaven. Risikobegrepet er et anvendt uttrykk for hendelser som kan inntreffe oss i fremtiden, og det kan ha konsekvenser for noe vi mennesker anser som verdifullt. Begrepet risiko blir brukt som et uttrykk for *den fare som uønskede hendelser representerer for mennesker, miljø og økonomiske verdier"* (Aven T. , 2006, s. 8). I tillegg kan risikoen uttrykkes kvantitativt på flere måter ved å si at risiko er en kombinasjon av mulige konsekvenser og tilhørende sannsynligheter (Aven T. , 2006, s. 8). Aven (2006) uttrykker videre en mer generell definisjon av begrepet risiko som *"en kombinasjon av mulige konsekvenser og tilhørende usikkerheter om hva som vil bli konsekvensene"*.

Wennersten forklarer i boken *Risker i tekniska system* (2003) at risiko kan innebære hendelser på ulike nivåer i et system. Prosessen med å identifisere mulige uønskede hendelser, estimere hvor stor risikoen er, og avgjøre hvorvidt risikoen kan aksepteres eller ikke, kalles risikobedømming. Innen industriell virksomhet kan risikobedømmingen være vanskelig å gjennomføre hvis det mangler kunnskap og erfaring om sannsynligheter og konsekvenser av uønskede hendelser. Risikoen Wennersten beskriver her kalles *objektiv risiko*. Objektiv risiko handler om at *"vi har en oppfatning om at det med et tilstrekkelig godt grunnlag skal kunne avdekkes både sannsynlighet for at en hendelse inntreffer og konsekvensen. Ofte er det enklere å oppdage konsekvensen enn sannsynligheten"* (Wennersten, 2003, s. 236).

For å beskrive sannsynlighet benytter vi oss av Njå et. al (2020) sin fremstilling av standardiserte sannsynlighetsord, som vist i tabell 2 på neste side:

Grad av sannsynlighet	Beskrivelse
Meget sannsynlig	Det er meget god grunn til å forvente
Sannsynlig	Det er grunn til å forvente
Mulig	Det er like sannsynlig som usannsynlig
Lite sannsynlig	Det er liten grunn til å forvente
Svært lite sannsynlig	Det er svært liten grunn til å forvente

Tabell 2 Standardiserte sannsynlighetsord. Fritt gjengitt etter Njå, Sommer, Braut & Rake (2020)

I bunn og grunn handler risiko om hendelser (A) og konsekvenser (C), som kan skje i fremtiden. Vi vet ikke om hendelsene vil inntreffe, eller hva konsekvensene vil være hvis det skjer. Med andre ord er begrepet usikkerhet (U) knyttet til både A og C. At en hendelse (A) vil inntreffe, og at ulike konsekvenser (C) vil inntreffe kan vi utrykke ved hjelp av sannsynligheten (P). Det er med dette (A, C, U)– perspektivet, en sammenheng mellom risiko og usikkerhet (Aven T. , 2008).

Når risikoen er vurdert gjennom en verdivurdering, trusselvurdering og sårbarhetsvurdering tas det et valg på hvilke strategier som benyttes omkring hvorvidt risikoen skal aksepteres eller håndteres. Dersom den ikke aksepteres, kan ren risiko igjen håndteres gjennom ulike strategier. De tradisjonelle måtene å gjøre dette på kan deles opp i fire områder, unngå, akseptere, overføre eller fjerne/redusere (Stranden R. , 2019, s. 75). Å unngå en aktivitet som medfører avdekket risiko, kan enten gjøres i en tidsbegrenset periode eller helt permanent. Risikoen kan på den andre sider aksepteres. De to måtene dette kategoriseres på er aktivt og passivt. Ved passivt å akseptere risikoen tar man utgangspunkt i at noe kan oppstå. Når dette eventuelt skjer dekkes tapet da, og situasjoner håndteres fortløpende når de oppstår. Gjennom aktivt å akseptere risiko kan organisasjoner eksempelvis budsjettere inn eventuelle kostnader forbundet med risikoen. Avdekket risiko kan overføres delvis eller helt for å redusere at den uønskede hendelsen oppstår. Siste område er å fjerne risikoen helt eller redusere den. I enkelte tilfeller er det mulig å gjøre dette uten at det går utover produksjonen eller funksjonaliteten. I andre situasjoner vil bistand fra politi/forsvar være nødvendig for å bekjempe risikoen slik at den reduseres til et akseptabelt nivå. Risiko kan også fjernes eller reduseres ved forebyggende eller skadereduserende tiltak (Stranden R. , 2019).

3.2 Usikkerhet

Det eksisterer per i dag ikke en felles og omforent definisjon av begrepet usikkerhet. Aven definerer usikkerhet som mangel på kunnskap, spesielt observerbare størrelser (Aven T. , 2008). DSB har ikke en klar definisjon av begrepet, men oppgir at *"Usikkerheten knytter seg til om en bestemt uønsket hendelse vil inntreffe, og om hva konsekvensene av denne hendelsen i så fall vil bli"* (DSB, 2019, s. 8). Noen forskere velger å holde usikkerhetsbegrepet utenfor begrepet risiko og er når det gjelder kunnskapssyn langt mot den positivistiske siden, dvs. at de har entro på at man kan finne et klart svar på hvilken risiko som finnes. Dette står i kontrast til Aven sin tolkning, hvor han knytter usikkerhetsbegrepet tett opp til definisjonen av risiko, og har et pragmatisk forhold til risiko og også måten å se kunnskap på (Njå, Sommer, Rake, & Braut, 2020). Andre forskere knytter usikkerhet opp mot nøyaktigheten til en analyse, f.eks. modeller og eksperimentelle data (Njå, Sommer, Rake, & Braut, 2020).

Det er viktig å ha oversikt over usikkerheten, når en skal behandle risiko. Usikkerheten kan komme fra ulike plasser, noe som gjør at den behandles ulikt. Det er ifølge (Aven T. , 2010) viktig å ta hensyn til følgende når en skal planlegge prosjekter, som er knyttet til usikkerhet:

- Hva er de usikre størrelsene?
- Hvem er usikker?
- Hvordan bør vi representere usikkerheten?

Njå et al. har sett på ulike forståelser av begrepet *usikkerhet*, og konkluderer med at det får ulik betydning avhengig av om man ser på fortid, nåtid eller fremtid. I fortiden vil usikkerhet være knyttet til hvilke observasjoner, gjenkjennelser, fortolkninger som er gjort, og som har medført en gitt forståelse, altså er usikkerheten knyttet til de benyttede metodene. I nåtiden vil usikkerhet være knyttet til det vi vet om et system eller en samfunnsviktig funksjon, dvs. vår særskilte kunnskap om systemet og det vi vet om det. Hva som vil skje vil være det som preger usikkerhet for fremtiden. Vi ser at usikkerheten i våre analyser vil variere og endres i tråd med tid. Njå et al oppsummerer dette ved at *"Usikkerhet er en innebygd karakter"* (Njå, Sommer, Rake, & Braut, 2020, s. 45). De oppgir også at man kan uttrykke denne usikkerheten, men det er fare for en sammenblanding av de nevnte usikkerheter knyttet til nåtid og fortiden for å si noe om usikkerhet i fremtiden.

Wysocki (2011) oppgir at det kan skilles mellom ulike kilder til usikkerhet, for eksempel tvetydighet/ambiguitet, tilgjengelig informasjon kan tolkes på ulike måter av de som er involverte, noe som er avhengig av bakgrunnskunnskap som den enkelte innehar. Det må også

tas hensyn til kompleksiteten av at mange er involverte, samt at et prosjekt kan ha mange detaljer. Samt usikkerheten i form av mangel på informasjon (Wysocki, 2011).

Tre indikatorer kan benyttes for å vurdere usikkerhet i en analyse (Flage & Aven, 2009):

- Tilgang på relevante data og erfaringer
- Forståelse av hendelsen som analyseres
- Enighet blant ekspertene som deltar i risikoanalysen

Aven beskriver at risiko er epistemisk, dvs. *"et resultat av manglende kunnskap"* (Aven T. , 2007, s. 67). Dette står i kontrast til stokastisk eller aleatorisk usikkerhet, som betyr variasjoner innenfor en populasjon (Aven T. , 2007). Stokastisk usikkerhet modelleres ved å benytte sannsynlighetsmodeller (Aven T. , 2019).

3.3 Verdi

I begge analysemodellene defineres hvilke verdier som skal beskytte, er sårbare og kan være truet. Den innsatsen som legges i å sikre verdien vil påvirke selve sikkerhetstilstanden. Tap av en verdi, eller om en verdi skades så det oppstår en reduksjon av den, kan få konsekvenser på lang og kort sikt. Konsekvensene dette får vil variere avhengig av valgt verdi, og hvilke konsekvensreduserende tiltak som er iverksatt. Hvem trusselaktøren er, vil også påvirke hvordan verdien sikres. Det er derfor viktig å skaffe seg god kunnskap om hvilke verdier som er attraktive og hvem de er attraktive for (NSM, 2016). DSB definerer fem typer samfunnsverdier; 1) liv og helse, 2) natur og kultur, 3) økonomi, 4) samfunnsstabilitet og 5) demokratiske verdier og styringsevne (DSB, 2019, s. 19).

3.4 Trussel

Trussel defineres som *"mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet"* (Standard Norge, 2012, s. 4). En trussel kan både forekomme gjennom tilsiktede handlinger og ikke tilsiktede handlinger. I analysene i denne rapporten er det tilsiktede handlinger som er i fokus. Gjennom tilsiktede handlinger er trusselaktører bevisst ute etter verdier de anser som attraktive. Trusselaktørene (personer eller grupper) kan også ønske å påvirke noens verdier negativt (Stranden R. , 2019). Truslene kan være både reelle, dvs. at trusselaktørene har intensjon og kapasitet til å true en entitets sikkerhet, og potensielle,

dvs. at de har en mulig intensjon og kapasitet (Standard Norge, 2012). Eksempler på trusler kan være spionasje, terror, sabotasje eller annen kriminalitet (Busmundrud, Maal, Kiran, & Endregard, 2015).

Begrepet *security*, eller *sikring* på norsk, blir som regel brukt om forebygging og håndtering av tilsiktede, uønskede hendelser, som f.eks. terroranslag eller hendelser knyttet til innsidehandel i næringslivet (Njå, Sommer, Rake, & Braut, 2020). Njå et. al forklarer at det er *"[…] viktig å merke seg at […] sikring (security) […] har som mål å finne frem til tiltak som skal håndtere risikoene som er identifisert. Tiltakene kan grupperes i menneskelige-, teknologiske- og organisatoriske tiltak"* (Njå, Sommer, Rake, & Braut, 2020, s. 213). Stranden mener at security betyr å sikre seg mot tilsiktede uønskede handlinger (Stranden R. , 2019). Nasjonal sikkerhetsmyndighet (NSM), Politidirektoratet (Pdir) og Politiets sikkerhetstjeneste (PST) definerer sikring som *"bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger"* (NSM; POD; PST, 2015, s. 9).

3.5 Sårbarhet

Sårbarhet kan defineres som *"et uttrykk for et systems evne til å fungere og oppnå sine mål når det utsettes for påkjenninger"* (Aven T. , 2006, s. 13). Hvis en feil skulle oppstå i et system, og det ikke er effektive barrierer eller beredskapssystemer på plass, vil sårbarheten til systemet bli regnet som høy. For en trusselaktør kan disse sårbarhetene være medvirkende til at de kan nå sine mål om å gjennomføre tilsiktede uønskede handlinger. En annen måte å uttrykke sårbarhet på er gitt i *Veileder til helhetlig ROS i kommunen***.** Her defineres sårbarhet som *"et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet"* (DSB, 2014, s. 15). Altså sier sårbarhet både noe om evnen et system har til å motstå en hendelse, men også om et systems evne til å tåle en hendelse hvis den oppstår. Systemet kan være tekniske systemer eller større organisatoriske systemer. DSB definerer også sårbarhet i sin veileder for samfunnssikkerhet i kommunenes arealplanlegging. Her heter det at sårbarhet *"vurderer motstandsevnen til utbyggingsformålet, samfunnsfunksjonene og ev. barrierer, og evnen til gjenopprettelse"* (DSB, 2017, s. 20).

Sårbarhet defineres i standarden *NS 5814:2008 Krav til risikovurderinger* 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"* (Standard Norge, 2008, s. 6).

Analyseobjekt kan være geografiske, tekniske, organisatoriske, miljømessige eller menneskelige faktorer som omfattes av risikovurderingen (Standard Norge, 2008)**.** Også i denne definisjonen tar en både med objektets evne til å stå imot en hendelse, og deretter evnen til å komme tilbake til den originale tilstanden etter at hendelsen har inntruffet. Sårbarheter knyttet til sikkerhet kan være til stede gjennom menneskelige, teknologiske og organisatoriske årsaker (MTO) (NSM, 2016). I sitt årlige risikobilde for 2019 trakk NSM frem følgende sårbarheter, som de hadde sett i løpet av året; Digitale sårbarheter, sårbarheter i virksomheters sikkerhetsstyring, personellmessige sårbarheter og fysiske sårbarheter (NSM, 2019). Sårbarheter er ofte resultat av uhensiktsmessig eller mangelfull sikring av verdier (NSM, 2016)

4. Metode

I dette kapittelet redegjøres for de metodevalgene, som er gjort for å kunne svare på oppgavens problemstilling.

Sikringsrisikoanalysemodellen VTS og grovanalyse med sløyfediagram er valgt som metoder. Disse metodene benyttes for å gjøre en dybdeanalyse, med grunnlag i samme trussel, av nye Sola rådhus, de ansatte og publikum/besøkende i bygget. Analysemodellene er valgt, da de sammen dekker mange av de viktigste faktorene ved risikoidentifisering. Gjennom VTS og grovanalysen kartlegges momenter som verdi, trusler, sårbarhet og sannsynlighet- og konsekvensreduserende tiltak. Vi ønsker å se om det gir forskjellige resultater når disse to sikringsrisikoanalysemodellene benyttes. Komparativ analyse benyttes for å sammenligne analysemodellene. Triangulering som metode er også valgt, for å se om de to analysemetodene kan utfylle hverandre.

For denne oppgaven har vi valgt case-studie. En case-studie er ifølge Yin (2018) en metode for å belyse beslutninger, hvorfor de ble tatt, hvordan de ble implementert og hvilke resultater det gir. Yin beskriver at case-studie er en empirisk metode for å undersøke et fenomen (en case) i dybden (Yin, 2018, ss. 14-15). Vi benytter case-studie fordi vi vil forstå en realistisk case. Dette gir oss reell innsikt når vi skal analysere risiko ved bruk av to ulike risiko-modeller. Prosjektgruppen mener, at for at oppgaven skal kunne benyttes av andre er det viktig å relatere analysene til en realistisk case. På denne måten blir det enklere for andre å kunne tilpasse sin analyse av utvalgte analyseobjekt med en metode tilnærmet lik vår fremgangsmåte.

Det er ulike faktorer tilknyttet Sola rådhus som vi kan fokusere på. Noen av disse faktorene kan være selve bygget og det bygningstekniske, Sola kommune, plan- og bygningsprosessen, den politiske behandlingen og agenda, de som skal arbeide inne i bygget eller de som bare skal besøke bygget og de tjenestene som eksiterer i bygget. Vi landet på at vi ønsket å fokusere på Sola rådhus som et objekt og dermed inkluderer vi de ansatte og besøkende i bygget samt brukerne av tjenestene lokalisert på bygget. Dermed har vi ekskludert Sola kommune og de risikoene som kommunen står ovenfor. Vi begrenser oss derfor i analysene til å fokusere utelukkende på risiko tilknyttet bygget. Det har likevel vært nødvendig å nevne noen av de samfunnskritiske funksjonene som befinner seg i Sola kommune.

Denne oppgaven tar for seg en case som handler om å analysere risiko tilknyttet Sola rådhus.

4.1 Dokumentanalyse

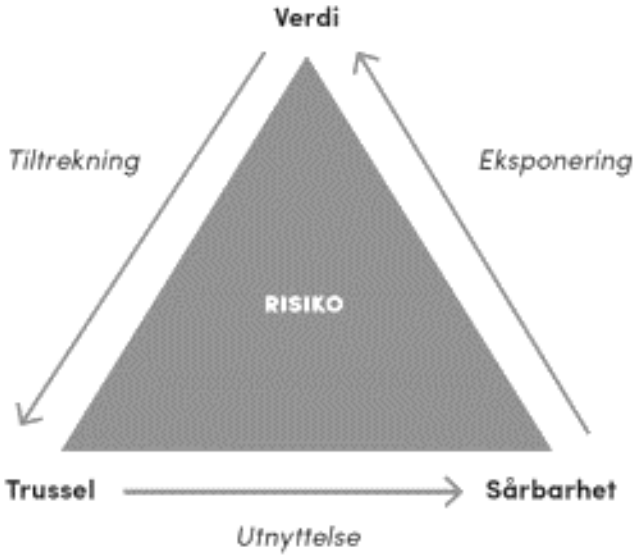
Dokumentanalyse er den valgte metoden for innhenting av data i denne prosjektoppgaven (se vedlegg 2) og hovedsakelig skriftlige og tekstbaserte dokumenter vil bli analysert. På grunn av omstendighetene knyttet til Covid-19 pandemien er dokumentanalyse utgangspunktet i prosjektoppgaven. Informasjon fra dokumentanalysen benyttes i de valgte risikoanalysene. Dette inkluderer subjekt-spesifikke bøker, artikler, offisielle publiseringer, statistikker, sakspapirer, rapporter, lover, informasjon fra nettsider, informasjonsbrosjyrer og forskrifter (O'Leary, 2004, ss. 67-68). Sola kommune har selv vedtatt at sakspapirene relatert til byggeprosjektet skal være offentlige i tråd med Lov om rett til innsyn i dokument i offentlig virksomhet (Offentleglova, 2006) (Sola kommune, 2016b). Vi har derfor hatt muligheten til å innhente dokumentasjon via nettsiden til Sola kommune. Dokumentanalyse er definert av (Bowen, 2009) som en systematisk prosess for å gjennomgå eller evaluere dokumenter. Som andre analytiske metoder i kvalitativ forskning, krever dokumentanalyse at data blir undersøkt og tolket for å få frem mening, oppnå forståelse og for å utarbeide empirisk kunnskap. Dokumenter gir bakgrunn og kontekst for temaet som undersøkes, samt gir supplerende data og kan hjelpe med å verifisere andre funn fra andre kilder (Bowen, 2009).

4.2 VTS-analyse

NS 5832:2014 *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse* beskriver en standardisert prosess for sikringsrisikoanalyser. Sikringsrisikoanalyse ses på som vesentlig for å kunne forstå og håndtere risiko knyttet til tilsiktede uønskede handlinger. Det tas høyde for at analytikerne har god tid, god tilgang på data samt kompetanse for å gjennomføre en slik sikringsrisikoanalyse. Sikringsrisikoanalyse kalles også VTS-analyse. VTS-analysen er en kvalitativ analyse, men kvantitative tall kan benyttes som supplement. Standarden anbefaler at analysen påbegynnes enten før eller samtidig med planleggingen av byggeprosessen og følger fremdriftsplan og beslutningene som tas. En sikringsrisikoanalyse skal ideelt sett påbegynnes tidlig, sånn at funnene kan påvirke valg av risikoreduserende tiltak (Standard Norge, 2014a).

Begrepet total risiko ligger til grunn for denne tilnærmingen. Total risiko er definert som forholdet mellom tre variabler; *1) verdi, 2) trussel og 3) sårbarhet*, og brukes for å beskrive den aktuelle totale risikoen (Njå, Sommer, Rake, & Braut, 2020, s. 211). Verdier **tiltrekker**

seg trusler og trusler **utnytter** sårbarhet og sårbarhet **eksponerer** verdier. Kombinasjonen av dette danner en sikringskontekst (Midtgaard, 2018) som illustrert i figur 1 nedenfor.



Figur 1 Forholdet mellom variablene verdi, sårbarhet og trussel. Hentet fra Midtgaard (2018)

Målet med VTS-modellen er å redusere arealet i trekanten så mye som mulig og dermed redusere risikoen. Dette gjøres ved å redusere én eller flere av variablene. Tilsvarende vil en økning av en eller flere variabler øke risikoen. Reduksjon eller økning av risiko kan begrunnes i iverksatte sikringstiltak eller mangel på slike tiltak (Njå, Sommer, Rake, & Braut, 2020, s. 212). Denne oppgaven baserer seg på kvalitative analyser, og det eksisterer dermed ikke et kvantitativt tallgrunnlag som supplement for å avgjøre størrelsen på trekanten eller variablene. Vi har derfor tatt utgangspunkt i, at trekanten hypotetisk sett reduseres/forstørres i takt med iverksatte og ikke iverksatte tiltak basert på de vurderingene som er gjort i analysen.

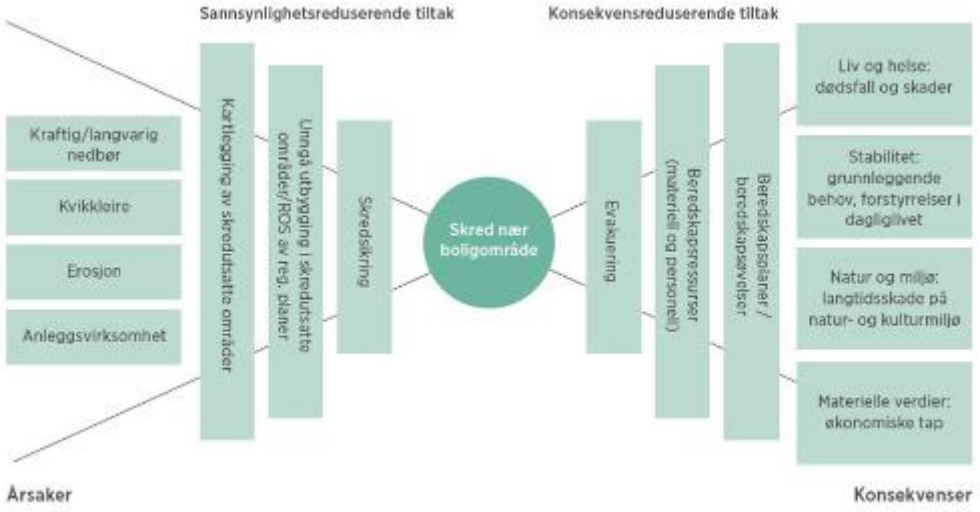
I VTS-analyse kartlegges, vurderes rangeres verdier i en verdivurdering. Dette brukes for å prioritere ressursbruk i forhold til sikring. Det fastsette sikringsmål, dvs. hva er akseptabel tilstand for virksomhetens verdier under eller etter en uønsket hendelse. Det gjennomføres trusselvurderinger og får dermed frem et trusselbilde, med informasjon om hva den trenger/ønsker å beskytte seg mot. Basert på verdi- og trusselvurderingene utarbeides scenarioer, som anses som relevante for videre analyse. På bakgrunn av verdi- og trusselvurderingene vil virksomheten gjennomføre en sårbarhetsvurdering, som avdekker på hvilken måte virksomhetens verdier er sårbare ut fra de valgte scenarioene. Virksomheten vurderer om det er behov for ytterligere barrierer eller sikringstiltak for å stå imot en uønsket

handling. Etter å ha vurdert verdi, trussel og sårbarhet sammenstilles informasjonen i en vurdering av ren risiko for hvert scenario, slik at hvilken risiko virksomheten er eksponert for blir tydeliggjort (Standard Norge, 2014a).

4.3 Grovanalyse med Bow-tie

En grovanalyse brukes som en systematisk metode for å kartlegge farer knyttet til en aktivitet. Ifølge Aven utføres grovanalysen *"fortrinns i en tidlig fase av et prosjekt"*, men analyseformen *"kan også brukes i andre faser"* (Aven T. , 2006, s. 83). Metoden innebærer at det lages en oversikt over mulige hendelser, og at det utarbeides en analyse av disse (Aven T. , 2006, s. 83). I dette prosjektet, hvor gruppen skal bruke grovanalyse til å analysere sikringsrisikoer knyttet til Sola rådhus, er det identifisert uønskede hendelser, som kan relateres til PST sin trusselvurdering for 2020. I neste steg har gruppen identifisert mulige årsaker til hendelsene, med tenkte sannsynlighetsreduserende- og konsekvensreduserende barrierer. Med barrierer menes forsvar som skal redusere eller hindre konsekvensene av uønskede hendelser (Reason, 1997, s. 7) Siste steg i prosessen er å se på mulige konsekvenser ved brudd på samtlige barrierer (Aven T. , 2006, s. 83). Alle dataene som samles inn i grovanalysen systematiseres i et grovanalyseskjema, og klassifiseres etter sannsynlighet og konsekvens. Grovanalysen danner grunnlag for utvelgelse av de mest kritiske risikoene, og videre arbeid med disse i risikostyringsprosessen.

For å visualisere stegene i grovanalysen har gruppen valgt å bruke sløyfediagram eller "bow-tie". Ved bruk av denne modellen kan hver enkelt uønsket hendelse vurderes med hensyn til mulige årsaker som kan føre til hendelsen, mulige konsekvenser som hendelsen kan føre til, samt sannsynlighetsreduserende- og konsekvensreduserende barrierer (DSB, 2017). Man vil da kunne få en oversikt over tiltak, som kan iverksettes for både å redusere sannsynligheten og redusere konsekvensen for at den gitte uønskede hendelsen inntreffer (Engen, et al., 2017). Ved bruk av bow-tie-diagram er det mulig å visualisere barrierer på en god og oversiktlig måte. Man vil også kunne se hvordan disse barrierene i serie kan forsterke hverandre i form av de sannsynlighetsreduserende barrierene i forkant av en uønsket hendelse og konsekvensreduserende barrierene i etterkant av en uønsket hendelse. FFI vektlegger også at en positiv effekt ved bruk av sløyfediagram er at man kan få frem spredningen i mulige årsaker som kan gi en uønsket hendelse, samt spredning i mulige konsekvenser (Busmundrud, Maal, Kiran, & Endregard, 2015).



Figur 2 Bow-tie. Hentet fra (DSB, 2014)

Figur 2, ovenfor, er gjengitt fra DSB sin veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen (DSB, 2014). Sirkelen som er markert midt i figuren, representerer en gitt uønsket hendelse. Årsakene som kan føre til denne uønskede hendelsen er plassert i boksene helt til venstre i figuren, mens de sannsynlighetsreduserende barrierene er plassert imellom årsakene og den uønskede hendelsen. Boksene helt til høyre i figuren representerer konsekvensene den uønskede hendelsen kan føre til, mens de konsekvensreduserende barrierene er plassert imellom den uønskede hendelsen og konsekvensene.

I sløyfediagrammet er man også nødt til å ta med usikkerhetsmomentet, da det vil være usikkerhet knyttet til hvorvidt den uønskede hendelsen vil inntreffe, samt hva de eventuelle konsekvensene vil bli (DSB, 2017).

4.4 Metodetriangulering

For å øke gyldigheten og troverdigheten til data og konklusjoner kan vi kombinere ulike metoder, observasjoner og analyser av data. Dette kalles å triangulere (Jacobsen, 2005, s. 229). Metodetriangulering innebærer, at bestemte fenomener studeres fra ulike synsvinkler og synspunkter, og at problemstillingen belyses ved hjelp av forskjellige metoder. Vi ønsker å triangulere resultatene fra analysemodellene. Dette for å se hvordan andre kan benytte en kombinasjon av disse modellene til å danne seg et beslutningsgrunnlag i andre bygge-prosjekter i fremtiden.

Prosjektgruppens medlemmer delte seg opp i to grupper, som skulle gjennomføre hver sin analyse. Dette for at analysene ikke skulle påvirke hverandre. Systematiske analyser av risiko setter krav til planlegging, gjennomføring og bruk. Planlegging innebærer å definere formål og systemet (analyseobjektet), organisering og tidsplanlegging av arbeidet. Gjennomføring krever en beskrivelse av systemet (analyseobjektet), identifisering av uønskede hendelser, forutsetninger og antagelser, årsaksanalyse og konsekvensanalyse, datainnsamling- og analyse samt presentasjon av resultatene. For å kunne benytte resultatene fra analysene som beslutningsgrunnlag for innføring av sikringstiltak er det behov for noen risikovurderinger (Aven T. , 2006, ss. 21-22). I denne prosjektoppgaven består slike vurderinger av resultater fra sammenligning av VTS- og grovanalysen.

4.5 Komparativ metode

I oppgaven har vi valgt å gjennomføre en sammenligning av de to analysemodellene, gjennom en komparativ metode. På NUPI sin internettside vedrørende teori og forskning heter det at *"Komparativ metode handler om å relatere et studieobjekt til et annet"* (NUPI, u.å.). Både kvalitative og kvantitative metode for sammenligning kan benyttes. NUPI oppgir videre at *"Den komparative metode anvendes ofte når man er ute etter mønster av likheter og ulikheter, som kan forklare kontinuitet og endring"* (NUPI, u.å.).

I denne oppgaven er komparativ metode brukt ved at det systematisk er sett på hvordan ulike nøkkelbegrep brukes og kan forstås i de ulike analysene, for å finne likheter og forskjeller i metodene. Det er også gjort vurderinger av om, selv om et begrep ikke nødvendigvis er brukt i den enkelte analyse, allikevel kan være dekket i analysen. De utvalgte nøkkelbegrepene er verdi, trussel, sårbarhet, scenarioer, konsekvens og sannsynlighet.

5. Resultatene av VTS-analyse og grovanalyse med sløyfediagram

Prosjektgruppen delte seg inn i to undergrupper for gjennomføring av analysene. Analysene ble gjort uavhengig av hverandre. På denne måten har vi sikret at analysenes resultater ikke har påvirket hverandre, og dermed danner er bedre sammenligningsgrunnlag. Den ene undergruppen gjennomførte en VTS-analyse hvor en av gruppens medlemmer har erfaring med å gjennomføre slike analyser. Den andre undergruppen gjennomførte en grovanalyse. Flere av undergruppens medlemmer har erfaring med å gjennomføre slike analyser. Det var strategisk å fordele prosjektgruppen slik at begge analysene kunne være noe erfaringsbasert og uavhengige av hverandre. Erfaring er en forutsetning for å gjennomføre slike analyser, og har nok påvirket analysene på en positiv måte.

5.1 Sikringsrisikoanalyse – VTS

Undergruppen som ser på problemstillingen gjennom en VTS-analyse har tverrfaglig yrkesbakgrunn og utdanning. Gruppen består av kompetanse fra Tolldirektoratet, riggselskap og IT-selskap. Kompetansen og erfaringen for deltagerne i denne gruppen er variert og består bl.a. av sikkerhet og beredskapsarbeid, objektsikkerhet, arbeidsmiljø, kvalitetssikring, granskningsmetodikk, politikk og prosjektkoordinering. Gruppemedlemmene mener denne kombinasjonen av kompetanse vil redusere usikkerhetsmomentet i analysen, siden gruppen har relevant innsikt i de aktuelle problemstillingene.

Nedenfor presenteres risikobildet fra analysen. Risikobildet baserer seg på faktorene verdi, trusselvurdering, scenariobeskrivelse og sårbarheter. Se vedlegg 3 og 4 for gjennomført VTS-analyse.

Verdier: I analysen er følgende *verdier* identifisert: a) Liv og helse, b) Materiell og bygninger, c) Operativt tjenestetilbud og d) Sensitiv informasjon.

Trusselvurdering: Følgende *trusselaktører* er identifisert: a) Fremmede makter, b) Organiserte kriminelle, c) Person eller gruppe med intensjon om å utføre en kriminell handling, d) Intern utro tjener, e) Person eller gruppe med intensjon om å utføre en terrorhandling og f) Aksjonsgrupper.

Scenariobeskrivelse og sårbarhet: I tabell 3, under, vises hvilke *scenarioer* som er valgt med tilhørende sårbarhet. Sårbarheten er fremkommet i den gjennomførte analysen.

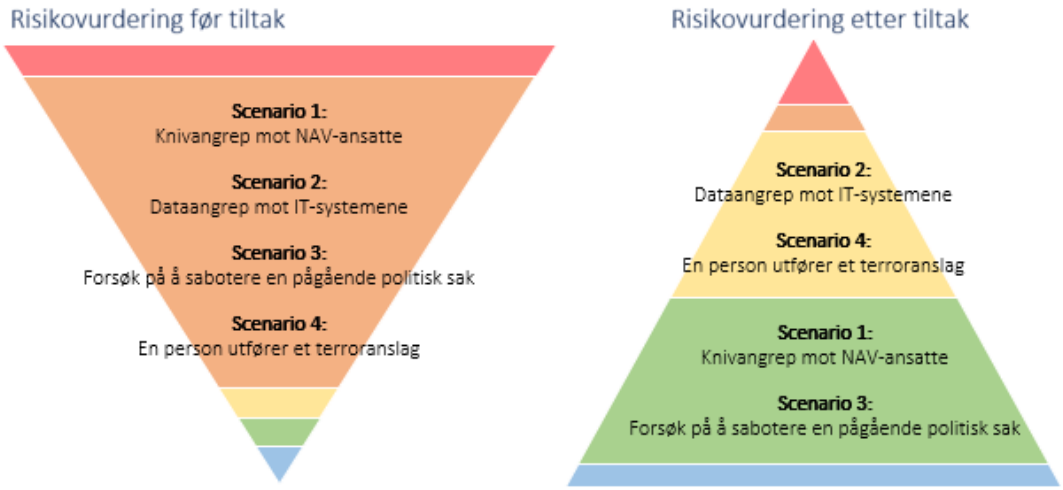
Scenario	Beskrivelse	Sårbarhetsvurdering
1	Knivangrep mot en NAV-ansatt	Moderat
2	Datainnbrudd	Moderat
3	Forsøk på å sabotere en pågående politisk sak i kommunen	Høy
4	En person utfører et terroranslag mot rådhuset	Svært høy

Tabell 3 Oversikt over valgte scenario og tilhørende sårbarhetsvurdering

5.1.1 Risikovurdering

I risikovurderingen trekkes frem det vi ser på som sannsynlige verdier for objektet Sola Rådhus. Scenarioene er valgt ut fra historiske hendelser, informasjon fra internett og tilgjengelig dokumentasjon fra Sola kommune. Først presenteres risikovurderingene for de fire utvalgte scenarioer, deretter fremlegges noen anbefalte sikringstiltak, som bør vurderes iverksatt. For sikringstiltak se vedlegg 3. Til slutt tar vi en ny risikovurdering basert på de fremlagte sikringstiltakene.

Som beskrevet i metodekapittelet, er målet med å sammenstille variablene *verdi, trussel* og *sårbarhet* å kunne belyse det totale risikobildet for sikringsobjektet. Dette for å kunne anbefale videre tiltak for å redusere risiko. Ved å innføre sikringstiltak basert på det fremlagte risikobildet vil man kunne redusere den totale risikoen ved at en eller flere variabler blir redusert (Njå, Sommer, Rake, & Braut, 2020). Dette er illustrert til slutt i dette kapittelet ved at risikovurdering av scenarioene før og etter iverksetting av supplerende tiltak er vist, se også Figur 3. Vi har ikke sett en økning av noen av variablene ved innføring av supplerende tiltak, det kan derimot være en usikkerhet i seg selv, at flere tiltak medfører større krav til oppfølging og vedlikehold av disse.



*Figur 2 Visuell fremstilling av risikovurderingen før og etter tiltak, der fargen rød illustrerer **svært høy** risiko, oransje **høy**, gul **moderat,** grønn **lav** og blå **ubetydelig/ikke relevant***

Risikovurderingen etter iverksettelse av anbefalte tiltak viser at scenarioene som var risikovurdert til høy, har blitt fordelt på moderat, lav og ikke betydelig risiko. Iverksettelse av de anbefalte sikringstiltak medfører derfor en redusert risiko.

På de neste sidene vil vi fremlegge de vurderinger som ligger til grunn for hvert scenario brukt i VTS-analysen.

Scenario Nr. 1	Knivangrep mot en NAV-ansatt				
	Ubetydelig/Ikke relevant	Lav	Moderat	Høy	Svært høy
Verdivurdering					**X**
Trusselvurdering				**X**	
Sårbarhet			**X**		
Risikovurdering				**X**	

Risikovurdering: Risiko i dette scenarioet vurderes som høy. Verdivurderingen Liv og helse tillegges spesielt stor vekt. Da dette er en av kommunens viktigste verdier, da skade på ansatte eller besøkende ikke aksepteres. Videre vurderes det, at selv om det ikke er kjente trusselaktører til stede, er det historikk nasjonalt knyttet til at enkeltpersoner uten forvarsel og med enkle og lett tilgjengelige midler, kan ramme verdien liv og helse. En trusselaktør kan benytte seg av sårbarheten som ligger i systemet, og dermed gå til angrep.

Sammenfattet viser analysen: En svært viktig verdi (liv og helse) er berørt. Eksisterende sikringstiltak vil ikke være i stand til å forhindre trusselaktør(er) i å utføre og lykkes med et angrep.

Det gjøres oppmerksom på at det er flere usikkerhetsmomenter i analysen, noe som også kan sies å representere en risiko i seg selv.

Scenario Nr. 2	**Dataangrep mot kommunens IT-systemer**				
	Ubetydelig/Ikke relevant	Lav	Moderat	Høy	Svært høy
Verdivurdering					**X**
Trusselvurdering				**X**	
Sårbarhet			**X**		
Risikovurdering				**X**	

Risikovurdering: Basert på en svært høy verdivurdering, høy trusselvurdering, men moderat sårbarhetsvurdering konkluderer vi med en høy risikovurdering.

Sammenfattet viser analysen: Verdivurderingen i dette scenarioet er satt til svært høy, da det involverer sensitiv informasjon, som det ikke er akseptert kan havne hos uønskede aktører. Trusler tiltrekkes av verdien. Trusselvurderingen viser at det er en høy trussel. Trusler utnytter sårbarheter. Basert på analysen er det moderat sårbarhet på Sola rådhus grunnet, at det er tiltak til stede for å ivareta informasjonssikkerheten. Sårbarhetene bør analyseres og utbedres.

Scenario Nr. 3	**Forsøk på å sabotere en pågående politisk sak i kommunen**				
	Ubetydelig/Ikke relevant	Lav	Moderat	Høy	Svært høy
Verdivurdering				**X**	
Trusselvurdering				**X**	
Sårbarhet				**X**	
Risikovurdering				**X**	

Risikovurdering: Verdivurderingen for dette scenario er satt til høy med bakgrunn i forsøk på sabotasje av demokratiske prosesser. Sårbarheten er vurdert til høy på bakgrunn av byggets utforming og åpenhet for publikum. Dette gjør det enkelt å hente informasjon om objektet. Sårbarheten settes også til høy på bakgrunn av manglende dokumentasjon på analyser, øvelser og menneskelige tiltak.

Sammenfattet viser analysen: Samlet risikovurderingen for scenario settes til høy, både fordi det er historie der aksjonsgrupper har tatt seg inn tidligere, og at det ikke ser ut til å foreligge dokumentasjon og sikringstiltak som kan forhindre dette i fremtiden.

Scenario Nr. 4	**En person utfører et terroranslag mot rådhuset**				
	Ubetydelig/Ikke relevant	Lav	Moderat	Høy	Svært høy
Verdivurdering					**X**
Trusselvurdering			**X**		
Sårbarhet					**X**
Risikovurdering				**X**	

Risikovurdering: Trusler tiltrekkes av verdi, som i dette scenario er vurdert til svært høy. Videre utnytter truslene sårbarhetene, som i dette scenario er vurdert som svært høy. Trusselvurderingen er i derimot vurdert som moderat og basert på sannsynlighet har vi vurdert risikoen til høy.

Sammenfattet viser analysen: En svært viktig verdi (liv og helse) er berørt. Eksisterende sikringstiltak utomhus vil ikke være i stand til å forhindre trusselaktør(er) i å utføre og lykkes med et angrep. Verdivurderingen for liv og helse tillegges spesielt stor vekt, da dette er en av kommunens viktigste verdier. Skade på ansatte eller besøkende akseptere ikke. Trusselvurderingen er vurdert som moderat, siden det ikke er kjent, at det er trusselaktører til stede med planer om å utføre terroranslag mot rådhuset på Sola, ei heller er det historikk som støtter opp om dette. Sårbarheten er vurdert til svært høy på bakgrunn uteområdets utforming og åpenhet for publikum.

5.2 Grovanalyse

Vi har gjennom vårt analysearbeid funnet frem til flere uønskede hendelser som kan inntreffe Sola rådhus, samt andre lignende organiserte bygg og strukturer. Gjennom grovanalysen (vedlegg 5) vil man kunne gå igjennom de uønskede hendelsene, som gruppen mener er aktuelle scenarioer for denne type virksomhet, med sammenslåtte etater i ett bygg. Vurderingene er sett i lys av rapporter fra PST, NSM, samt en erfaringsbasert vurdering fra representantene i gruppen. Det vi finner av funn i grovanalysen er at den store trusselen blir ofte vurdert til lite sannsynlig at kommer til å skje, og at de hendelsene med liten til mindre konsekvens har en større risiko for at kan oppstå. Man ser at det er viktig at man får inn erfaring- og kunnskapsbasert informasjon rundt hvilke hendelser som kan oppstå.

Vi har valgt å ta ut fire av de uønskede hendelsene som vi har funnet. Tre av disse er valgt i henhold til at de er på PST sin trusselvurderingsliste for 2020. Den siste, *kriminalitet,* har vi tatt med på grunnlag av hva man ser, som mest sannsynlig av uønsket hendelse ovenfor sikring av bygg, inventar og ansatte. Ut over de fire eksemplene vi viser til under i denne skriftlige analysedelen vil man også kunne gå inn i grovanalysen og se på andre uønskede hendelser som kan inntreffe Sola Rådhus. Her vil det også fremkomme våre erfaringsbaserte rådgivende tiltak for å forhindre og forminske konsekvensene av de forskjellige uønskede hendelsene.

Uønsket hendelse 1: Terror

Terrorangrep utført mot Sola rådhus er noe vi i grovanalysen anser som svært lite sannsynlig vil skulle skje. Derimot ville det fått svært alvorlige konsekvenser hvis et vellykket angrep hadde blitt gjennomført, og kunne ført til flere døde og skadde, og store materielle ødeleggelser. Tenkelige angrepsmåter er bombeangrep (f.eks. kjøretøybåren bombe eller improviserte eksplosiver) og angrep med skytevåpen eller stikkvåpen der terroristen tar seg inn i bygget. Begrunnelsen for at denne hendelsen blir vurdert som *svært lite sannsynlig* er at Sola rådhus vil ha liten symbolverdi, og vurderes som et ikke spesielt utsatt eller "attraktiv" mål. Likevel kan man med 22.juli-angrepet i bakhodet og PSTs vurderinger, ikke utelukke at politiske mål kan bli rammet. Årsaken vi legger til grunn for at Sola rådhus skulle blitt rammet av et terrorangrep, er "politiske mål for å skape endringer", der man blant annet kan ha som mål å påføre skade på demokratiet ved å angripe folkevalgte. Risiko-klassifiseringen ender med bakgrunn i sannsynlighets og konsekvensvurderingen, på gul (5), men ettersom

konsekvensene ved et terrorangrep er vurdert som såpass store, velger vi å gå mer i dybden på denne hendelsen. Ingen av de andre uønskede hendelsene, som er identifisert, har en høyere konsekvensvurdering enn terrorangrep, med *svært alvorlige konsekvenser* av et gjennomført angrep. Av sannsynlighetsreduserende barrierer har vi identifisert følgende: Dialog med PST for oppdatert informasjon vedrørende endring i trusselbilde for politiske mål, adgangskontroll, kjøretøyssperrer, nøkkelkort og kode, kameraovervåkning, og inndeling av bygget i soner. Av konsekvensreduserende barrierer har vi lagt til grunn krise- og beredskapsplanverk, som også omfatter varsling og innsats ved slike hendelser.

Uønsket hendelse 2: Etterretning – spionasje og digital kartlegging

Med digital kartlegging på Sola rådhus antar vi at vi vil ha med personer som gjennom IKT-systemene innhenter data på ulovlig måte. Aktørene kan være knyttet til fremmede staters etterretningsorganisasjoner eller industrispionasje knyttet til næringsinteressene i kommunen. Digital kartlegging kan også ha utspring i økonomisk kriminalitet og ønske om å sabotere politiske beslutninger. Eksemplet fra grovanalysen vi ønsker å vise til er hvor en aktør innhenter data og anskaffer seg informasjon på en ulovlig måte. Gjennom vår erfaring i gruppen, mener vi at de sannsynlighetsreduserende tiltakene bør være en god og grundig opplæring innen sikkerhetskultur, men også kurs og opplæring via NSM innen datasikkerhet og informasjonssikkerhet. Vi mener at det er nødvendig, ikke bare opp mot terror, men også opp mot våre andre eksempler av uønskede hendelser, at kommunen og rådhuset har en informert og erfaren sikkerhetsansvarlig, som kan være bindeleddet mellom kommunen og andre sikkerhetsrådgivende etater. Opprettelse av et krise- og beredskapsplanverk er svært nødvendig for en virksomhet som dette. Det er også i alles interesse, at dette planverket blir oppdatert og revidert etter endringer i samfunnet og internt i kommunen. En annen vesentlig oppgave vil være, at ansatte trener og øver på bruken av krise- og beredskapsplanverket. Bruken av krise- og beredskapsplanverket vil være en del av de konsekvensreduserende tiltakene for å minske konsekvensene av en slik handling. Vi legger til grunn at konsekvensene av godt planlagt spionasje og digital kartlegging gjennom kriminelle aktører, vil være tap av kritisk informasjon og omdømme. Vi finner derfor at sannsynlighet lander på *sannsynlig* og konsekvens på *moderat*, som til sammen i risikoklassifiseringen blir rød (9). Det vil etter denne analysen være nødvendig å gå tilbake til tiltakene for å utbedre forholdene slik at vi har flere og sterkere barrierer.

Uønsket hendelse 3: Sabotasje av kritisk infrastruktur

Sola kommune har som omtalt tidligere kritisk infrastruktur knyttet til olje og gass, samt LNG anlegg i Risavika. Sola har også en regional flyplass med stor offshoretrafikk. Det er planer om å utvide både industriområdet i Risavika og flyplassen. Samtidig finnes det lokal motstand til disse byggeplanene og mot fortsatt drift av LNG-anlegget i Tananger. Beslutninger knyttet til utbygginger og drift av infrastruktur i kommunen fattes på politisk nivå. I prosjektet er det identifisert, at det med ganske *høy grad av sannsynlighet*, kan komme til å inntreffe ulike former for sabotasje for å stoppe aktivitet knyttet til denne infrastrukturen, som kan ses på som kritisk for transport og energisektoren på Nord-Jæren. Aksjoner kan komme i form av fysisk sabotering av møter på rådhuset, ved at aksjonister for eksempel tar seg inn i kommunestyresalen under møter hvor saker knyttet til kritisk infrastruktur behandles. Blokkering av innganger, garasjeanlegg og adkomstveier, kan være en annen måte å sabotere politiske møter og saksbehandlingsprosesser på. Dette gjør at vi da ender på en risikoklassifisering på rød (12).

En annen trussel for kritisk infrastruktur kan være fremmede makters ønske om å sabotere denne for å oppnå egne fordeler. I denne sammenheng vil rådhuset og de ansatte som jobber der være av interesse for innhenting av informasjon. Slike operasjoner vil falle inn under etterretningsaktivitet, hvor det endelige målet for operasjonene kan være sabotasje av kritisk infrastruktur. Målet til aktøren kan i slike tilfeller være å ikke bli oppdaget, slik at den som blir utsatt for sabotasjevirksomhet fra etterretningsaktører ofte ikke vil merke, at de er utsatt for dette, før det er for sent. Målet for sabotasjen og hvem som står bak vil kunne være uklart, i alle fall i den første fasen etter sabotasjen har funnet sted. Denne type operasjoner vil falle inn under hybride trusler, hvor målet vil være å villede og skape handlingslammelse. Sabotasje av kritisk infrastruktur kan påvirke myndighetenes responsevne. Når det er sagt spørs det hvor høy sannsynligheten er for at Sola rådhus vil være av interesse, i dette tilfelle vil beredskapen i Sola kommune bli satt på prøve. Konsekvensen av denne type sabotasjer kan være alvorlig for kommunen og staten, og kan være ledd i en større hybrid krigførings-operasjon. Ut ifra den kunnskapen prosjektgruppen sitter på i dag, vurderes sannsynligheten for at Sola rådhus kan bli ut satt for denne typen hendelser som lav, men konsekvensene kan bli store hvis det skulle skje.

Sannsynlighetsreduserende tiltak for å hindre sabotasje av kritisk infrastruktur knyttet til Sola rådhus, kan være å sette inn barrierer innen fysisk sikring, personellsikkerhet og IKT-sikkerhet. Kompetansehevende tiltak innen sikring og aktuelle trusler vil være aktuelt overfor

de ansatte, mens gode rutiner og kontinuerlig arbeid for fysisk sikring og IKT-sikkerhet må på plass. System for vurdering og kontroll i forbindelse med utro tjenere bør også etableres, som en forebyggende barriere på dette området.

Konsekvensreduserende tiltak i forbindelse med sabotasje av kritisk infrastruktur, vil i første omgang kunne iverksettes gjennom deteksjon og varsling av sabotasje. Dette kan skje gjennom manuelle prosedyrer eller automatiserte. Etter deteksjon og varsling vil kommunen kunne iverksette sin beredskapsplan, og iverksette definerte tiltak/aktivere ytterligere barrierer for å stoppe sikkerhetsbruddet. Løpende overvåkning av situasjonen vil gi beredskapsledelsen informasjon, som kan støtte videre beslutninger. Tiltakene som iverksettes skal minimere konsekvensene for menneske, stabilitet, kritisk infrastruktur og økonomi.

Uønsket hendelse 4: Kriminalitet

Dette punktet inneholder naturligvis mange mulige typer hendelser og årsaker. For å begrense vår analyse har vi tatt ut noen årsaks-punkter på hvorfor annen kriminalitet vil kunne bli begått på Sola Rådhus. Resterende årsaker vil man finne i grovanalysen (vedlegg 5). Det vi i stor grad har sett på i grovanalysen er bevisste og ubevisste voldshandlinger mot ansatte, psykisk og fysiske trusler mot ansatte og ansatt tatt som gissel. Slik vi har blitt kjent med denne type problematikk, er dette det scenarioet vi antar er mest sannsynlig kan skje i Sola rådhus. Historikken over lignende uønskede hendelser mot tilsvarende eller lignende etater, som Sola rådhus har under sitt tak, har forekommet ved flere anledninger i Norge. Et eksempel er drapet på en saksbehandler på NAV kontoret på Grorud, Oslo i 2013. Året før, i 2012 avfyrte en 61 år gammel mann et skudd inne på NAV kontoret på Tøyen, Oslo. Vi ser med bakgrunn av hvilke etater som ligger under Sola rådhus, og historikken og alvorlighetsgraden av de tidligere hendelsene at det er *svært sannsynlig* at dette vil kunne også skje inne på Sola Rådhus. Og skulle dette skje, så mener vi at konsekvensen vil være på et *moderat* nivå. Dette gjør, at vi ender på en risikoklassifisering på rød (15). Det vil etter denne analysen være nødvendig å gå tilbake til tiltakene for å utbedre forholdene slik at vi har flere og sterkere barrierer.

6 Analyse

I dette kapittelet vil vi presentere funn og data gjennom en komparativ analyse. Vi ser nærmere på de spesifikke faktorene som VTS- og grovanalysemodellen inneholder. Videre blir forskningsspørsmålene også analysert opp mot risikometodene vi har benyttet.

Vi ser at det kan være utfordrende å skille mellom noen av forskningsspørsmålene når man skal analysere dem opp mot risikometoden. Men vi mener også at forskningsspørsmålene er forskjellige og gir relevante svar.

6.1 Komparativ analyse

I dette kapittelet analyseres funnene fra VTS- og grovanalyse ved hjelp av komparativ analyse. Begge metodene har en systematisk fremgangsmåte, og det er en fordel for begge metodene, at det nedsettes en tverrfaglig arbeidsgruppe, som sammen kan belyse de ulike faktorene som kreves for å finne frem til risikobildet. Utgangspunktet for analysene er forskjellig. Der grovanalysen tar utgangspunkt i faktorene konsekvens og sannsynlighet for å beskrive risikobildet, vil VTS-analysen ta utgangspunkt i faktorene verdi, sårbarhet og trussel. Imidlertid er det en del likheter og overlappinger som beskrives under.

Verdivurdering: En forutsetning for VTS-analysen er at den beskriver hvilke verdier som skal beskyttes. Verdivurderingen gjøres på bakgrunn av en skala fra svært høy til lav verdi.

En slik systematisk verdivurdering er ikke til stede i grovanalysen. Imidlertid er en forutsetning for grovanalysen, at det foretas en objekt kartlegging/verdivurdering, en såkalt systembeskrivelse. Her vil også kritiske objekter, skjermingsverdig informasjon kartlegges (Busmundrud, Maal, Kiran, & Endregard, 2015). I vår oppgave ser vi at verdivurderingen også er implisitt i konsekvensvurderingen ved at hovedgrupper, som sikringshendelsen vil ramme, identifiseres.

I våre to analyser fremkommer *verdiene* i VTS-analysen og *hovedgruppene som vil rammes* i grovanalysen omtrent som like, men med ulik ordlyd. For VTS-analysen er verdiene liv og helse, materiell og bygning, operativt tjenestetilbud og sensitiv informasjon. Grovanalysen nevner i sin konsekvensvurdering liv og helse, stabilitet (grunnleggende behov, forstyrrelser i dagliglivet, negative konsekvenser for lokaldemokratiet), kritisk infrastruktur og materielle

verdier som hovedgrupper av konsekvenser. For grovanalysen er ikke sensitiv informasjon eksplisitt nevnt, imidlertid er dette studert i analysen.

Trusselvurdering: For begge analysemetodene vil trusselaktørene og aktuelle uønskede hendelser identifiseres. I VTS-analysen kommer trusselaktørene klart frem, og er fremmede makter, organiserte kriminelle, personer/grupper av personer med intensjon om å utføre en kriminell handling, intern utro tjener, personer/gruppe med intensjon om å utføre terrorhandling og aksjonsgrupper. Grovanalysen har identifisert mange av de samme aktørene, men gir ikke en så klar beskrivelse av disse. Det kan skyldes valg av oppsett brukt i grovanalysen. Hovedfokus i grovanalysens trusselvurdering har vært å identifisere sikringstrusler. Disse er spionasje, digital kartlegging og sabotasje, terrorangrep og kriminalitet. De samme truslene er identifisert i VTS-analysen, i denne analysen fremkommer sikringshendelsene når de ulike trusselaktørene studeres, i tillegg til at de viktigste sikringshendelser identifiseres ved valg av scenarioer.

VTS-analysen har egen skala, som benyttes til å vurdere tilstedeværelse av trusselaktør, noe som mangler i grovanalysen. Begge analysene har i stor grad identifisert de samme trusler og trusselaktører, imidlertid er systematikken og dokumentasjonen av funnene ulik.

Sårbarhetsvurdering: I sårbarhetsvurderingen, som gjøres systematisk i VTS-analysen, avdekkes sårbarheter analyseobjektet innehar når det gjelder MTO-sikringstiltak. Sårbarheter studeres for de valgte scenarioer. Sårbarhetsvurderingen baseres på en skala fra svært høy, der det ikke eksisterer sikringstiltak, til ubetydelig/ikke relevant, der det ikke er behov for sikringstiltak.

I grovanalysen gjøres ikke en tilsvarende sårbarhetsvurdering, men sikringstiltak fremkommer i analysen av sannsynlighets- og konsekvensreduserende tiltak og barrierer. Styrken til sikringstiltakene synliggjøres ikke, men det er å anta at dette er noe som vil diskuteres i analysegruppen. Busmundrud et al. omtaler sårbarhetsvurdering i grovanalyse som *"en beskrivelse og vurdering av i hvilken grad det er mulig for ulike trusselaktører å utføre en uønsket handling, uten å bli stanset eller påvirket. Et sentralt begrep i vurderingen er mulighet, dvs. i hvilken grad det er mulig for en trusselaktør å forsere virksomhetens sikringstiltak"* (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 29). I NS5814 tilsvarer

"analyse av årsaker og sannsynligheter" en sårbarhetsvurdering (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 29).

Sannsynlighet- og konsekvensvurdering: Grovanalysen legger opp til en systematisk gjennomgang av sannsynligheter for at en uønsket hendelse vil kunne skje. Sannsynlighet fastsettes etter en skala der sannsynlighet rangeres fra svært høy til ubetydelig. Da sannsynligheten i vår grovanalyse ikke kan baseres på tallmateriell, vil sannsynligheten fastsettes på bakgrunn av kunnskap og faglig skjønn, såkalt kunnskapsbasert sannsynlighet (Busmundrud, Maal, Kiran, & Endregard, 2015). Ved fastsettelse av sannsynlighet i denne oppgaven er bl.a. PSTs trusselvurdering en viktig kilde.

VTS-analyse legger ikke opp til en slik systematisk vurdering av sannsynlighet, men dette vil være implisitt i risikovurderingen, som gjøres av de ulike scenarioene, etter at verdi-, trussel- og sårbarhetsvurderingen er gjennomført.

I grovanalysen vurderes konsekvensene av en eventuell uønsket hendelse, altså hvilken effekt konsekvensene har (Busmundrud, Maal, Kiran, & Endregard, 2015). Konsekvensene vurderes etter en skala, som i vårt eksempel spenner i 5 nivåer mellom ufarlig og katastrofal. Når både sannsynlighet og konsekvens er identifisert kombineres disse i en matrise, for å vurdere hvilken risiko som er forbundet med den uønskede hendelsen.

En slik matrise benyttes ikke i VTS-analysen. Her vil konsekvensene i vår analyse fremkomme i selve scenariobeskrivelsen for det enkelte scenario. I Busmundsrud et al. sin rapport diskuteres at det i VTS-modellen ikke forekommer en egen vurdering av muligheten for at en trussel vil materialiseres og lykkes. Her konkluderes med at en mulighetsvurdering vil fremkomme når man velger scenarioer, og når det man vurderer trussel og sårbarhet, slik at det ikke vil være store forskjeller for dette i de to ulike metodene (Busmundrud, Maal, Kiran, & Endregard, 2015).

Scenariobeskrivelse: I VTS-analysen har scenariobeskrivelse en viktig plass. I disse beskrives aktuelle sannsynlige hendelser, gjerne detaljert. I VTS-analysen i denne oppgaven er scenarioene *Knivangrep mot en NAV-ansatt*, *datainnbrudd*, *forsøk på sabotasje i forbindelse med politisk sak* og *terroranslag fra en person*. Vi finner også scenarioer i grovanalysen, men her er de ikke nødvendigvis utfyllende beskrevet og mange kan listes opp, som eksempelvis er gjort i risikovurdering skjemaet for Sola rådhus. Listen kan ikke være

uttømmende, så også i grovanalysen vil man tvinges til å gjøre noen avveininger av hvilke scenarioer som er de viktigste. I vår grovanalyse er det, uavhengig av VTS-analyse, valgt å se på noen scenarioer mer inngående. Dette er terror, etterretning – spionasje og digital kartlegging, sabotasje og kriminalitet. Valg av scenarioer i begge analysene sammenfaller, men for grovanalysen er det ikke nødvendigvis ett enkelt scenario, som beskrives under hver av disse uønskede hendelsene, f.eks. inneholder sabotasje både politisk sabotasje og etterretning.

Oppsummering

Vår sammenligning av grovanalyse og VTS-analysen, som er gjennomført, sammenfaller med Busmundrud et al. sine funn, og forskjellene kan oppsummeres som *"i den første tilnærmingen foretas det en systematisk vurdering av konsekvensen av et angrep og muligheten for at det finner sted, som så settes sammen til en risiko, mens trefaktormodellen ikke inneholder noen anvisning på hvordan man kommer fra de tre faktorene over til risikoen"* (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 37). Nedenfor (Tabell 4) oppsummeres sammenligningen mellom modellene i tabellform:

Grovanalyse			**VTS-analyse**	
Inngangsparameter	**Delresultat**	**Resultat**	**Inngangsparameter**	**Resultat**
Verdi Trussel Sårbarhet	Konsekvens Sannsynlighet	Risiko	Verdi Trussel Sårbarhet	Sikringsrisiko

Tabell 4 Komparasjon av de 2 analysemetodene oppsummert basert på (Busmundrud, Maal, Kiran, & Endregard, 2015).

6.2 Hvordan tilnærmer de forskjellige analysemetodene seg til sikring av et bygg?

Grovanalysen og VTS-analysen, som er gjennomført for Sola rådhus, har begge hatt fokus på sikringshendelser (security). Sikkerhet (safety) er ekskludert fra begge analysene. Resultatet fra analysene viser at grovanalysen fremstår som en bred og åpen analyse med fokus på å sammenfatte de ulike faktorene tidlig ved bruk av bow-tie (sløyfediagram). Grovanalysen gir analytikerne anledning til å danne seg et mer helhetlig bilde av potensielle hendelser/trusler/risiko, ved å ikke henge seg opp i enkeltscenarioer. I en skjematisk risikovurdering skisseres flere uønskede hendelser med varierende tilhørende årsaker. Denne fremstillingen gjør det enkelt for analytikeren siden alt er samlet på en plass. På den andre

siden baserer VTS seg på kunnskapen man besitter på gitte tidspunkt når scenariene utarbeides. Deretter har undergruppen for grovanalysen valgt ut fire uønskede hendelser til nærmere studie. Istedenfor å velge et konkret scenario som VTS-analysen gjør, er det her blitt utført en bredere tilnærming i analysen. Dette vises igjen ved å se på valg av uønskede hendelser i tabell 5.

VTS-analyse	Grovanalyse
Knivangrep mot NAV-ansatte	Kriminalitet
Dataangrep mot IT-systemene	Etterretning – spionasje og digital kartlegging
Forsøk på å sabotere en pågående politisk sak	Sabotasje av kritisk infrastruktur
En person utfører et terroranslag	Terror

Tabell 5 Komparasjon av de uønskede hendelsene som fremkommer i de valgte analysemetodene

VTS-analysen er opptatt av sikring av verdiene, mot truslene og sårbarhetene i direkte tilknytning til sikringsobjektet og analysen kan derfor fremstå som veldig konkret. Samtidig gir VTS-analysen analytikerne en oversikt over og bevissthet om de viktigste verdiene og trusselaktørene knyttet til analyseobjektet. Det at sårbarhetene vurderes ut fra valgte scenarioer, krever at scenariene er realistiske og treffer bestillingen på selve analysen. Det vil alltid være en svakhet i, at et scenario kan utfolde seg på ulike måter, så bevissthet om hva som analyseres og det å være tro til verdien, som skal beskyttes, er essensielt. En annen svakhet og et usikkerhetsmoment i VTS-analysen, kan være at konkrete tiltak utelukkes fordi de ikke anses som relevante for det valgte scenario. Det kan derfor være viktig å avgrense omfanget av vurderingen, dersom kunnskapen man besitter er mangelfull eller hvis det er knyttet stor usikkerhet til konsekvensene. Styrken til VTS-analysen er det spesifikke fokuset på enkelte scenarioer og konkrete sikringsmål, istedenfor den generelle tilnærmingen andre analysemodeller benytter seg av. Hensikten med risikobilde som presenteres er å gi en forståelse av hvilken risiko man er eksponert for. De eller den som skal ta en beslutning kan ut ifra dette risikobilde velge de strategier som er mest riktig, og tiltakene som er mest effektive for videre håndteringer (NSM, 2016, s. 23).

Grovanalysen tar mer hensyn til at det er flere måter å oppnå et mål, dette kan være en styrke når det er flere scenario relevant å undersøke.

Det kan virke som VTS-analyse er en analyse, som er bedre tilpasset spesifikke scenario/trusler, ved at den begynner bredt og spisser seg etter hvert. Grovanalysen er i større grad tilrettelagt for en bredere tilnærming. Den tar for seg flere mulige scenarioer gjennom at man først finner den uønskede hendelsen man skal se på, så finner man hvilke barrierer som vil kunne hindre/minske konsekvensene av den uønskede hendelsen. VTS-analysen må først finne hvilken verdi man skal beskytte før man kan finne de andre elementene.

Rangeringsskalaene i analysene tar utgangspunkt i ulike skalaer. Grovanalysen benytter seg av sannsynlighet, konsekvens og risikobilde, og VTS-analysen har i tillegg til rangeringen av risiko, skalaer som ser på trussel, sårbarheter, indikatorer og verdier. Til tross for dette ender analysene opp i tilnærmede like vurderinger når de ulike trusselaktørene og trusselen analyseres. Eksempel på dette er følgende:

Begge analysene ser på kriminalitet som en trussel. Grovanalysen beskriver med sine to rangeringskalaer at sannsynligheten for dette er høy, og konsekvensene ville vært svært kritisk. VTS-analysen benytter seg av fire skalaer for å belyse samme trussel. Resultatet er omtrent det samme som i grovanalysen, og det totale risikobilde før tiltak foreslås rangeres til *høy*.

Begge analysene legger opp til anbefalte sikringstiltak basert på avdekte sårbarheter i VTS-analysen og sannsynligheter i grovanalysen. VTS-analysen spesifiserer sikringstiltakene tilknyttet MTO, og kan fremstå som mer detaljert i sin tilbakemelding. Samtidig konkluderer begge analysene med en risikovurdering som rangeres til *lav* når anbefalte tiltak iverksettes.

Ut fra risikoanalysene til begge gruppene samsvarer funnene med hverandre, og det er ingen store avvik i resultatene, til tross for ulike rangeringsskalaer.

6.3 Hvilke svakheter og styrker fremkommer av å gjennomføre to forskjellige risikoanalyser?

Begge analysene har både styrker og svakheter når det angår risikovurdering av tilsiktede uønskede hendelser.

En svakhet med grovanalysen kan være, at bruk av kombinasjonen sannsynlighet og konsekvens, i vår analyse, gir et tall mellom 1 og 25 for den enkelte uønskede hendelse som studeres. Dette kan gi et inntrykk av det i analysen fremkommer en fasit ift. risiko. For uønskede tilsiktede hendelser, som f.eks. etterretning – spionasje og digital kartlegging rettet

mot Sola rådhus, vil en sannsynlighet være svært vanskelig å konkludere med absolutt sikkerhet. Vurderingen av disse, og da særlig etterretning og terrorisme, vil i stor grad være basert på historikk, nasjonale trusselvurderinger fra PST, NSM osv. Sannsynligheten for slike hendelser er i mindre grad knyttet til historikk, da endring i risikobildet plutselig kan skje. Det kan også være vanskelig å hensynta usikkerhet i den vurderingen som gjøres, og konklusjonen, selv om den er enkel og forståelig fremstilt, kan fremstå mer sikker enn den egentlig er. I tillegg kan fremstillingen overforenkle risikoen. Dette er også funn som tidligere er gjort i FFIs rapport *Tilnærming til risikovurderinger for tilsiktede uønskede handlinger* (Busmundrud, Maal, Kiran, & Endregard, 2015).

En styrke ved grovanalysen er at den er forholdsvis enkel å gjennomføre, og ikke krever spesialisert kompetanse. Metoden er systematisk, men den håndterer ikke usikkerhet (Busmundrud, Maal, Kiran, & Endregard, 2015).

En svakhet med VTS-analysen er, som nevnt over, at når sårbarheter identifiseres kan noen scenarioer utelukkes, som ville kunne ha betydning for hvilke reelle sårbarheter som finnes for et analyseobjekt.

I tillegg kan det oppleves som en svakhet at metoden ikke sier noe om sannsynlighet og usikkerhet. Den sier heller ikke noe om prioritering av tiltak, og sluttresultatet kan være vanskelig å kommunisere visuelt på en enkel måte (Busmundrud, Maal, Kiran, & Endregard, 2015).

Det er flere positive trekk med VTS-analysen. Busmundsrud et. al oppgir at modellen medfører at virksomheter må prioritere hva som skal beskyttes og blir bevisst på at verdier kan være sårbare overfor en gitt trussel. Til sammen kan dette gi positive kvalitative aspekter, som er verdifullt for virksomheten å ta stilling til. Fokus på verdi oppgis også å være positiv med tanke på bruk av prioritering av sikringstiltak. I tillegg henvises det i denne rapporten til, at en grundig verdivurdering kan gi et klarere bilde av hva som skal prioriteres av sikringstiltak for å styre risikoen (Busmundrud, Maal, Kiran, & Endregard, 2015).

Ved å kombinere de ulike analysemetodene åpner det for at det først foretas en bred analyse gjennom grovanalysen, for så at det kan gjennomføres en VTS-analyse basert på de utvalgte uønskede hendelsene. På denne måten kan det gjennomføres analyser, som går mer i dybden på valgte scenario. Det kan godt være, at det gjennom grovanalysen fremkommer, at enkelte tilsiktede hendelser kan behøve et dypdykk for å se hvordan de faktiske tiltak vil fungere. Samt at det åpner for en nærmere analyse av om de iverksatte tiltakene er tilstrekkelig.

6.4 Gir en av analysemodellene tilstrekkelige resultater til å utelukke den andre?

I våre analyser konkluderer vi med at grovanalysen gir et mer generelt bilde av den totale risikoen gjennom flere risikoområder. VTS-analysene spisser seg i mye større grad mot ett spesifikt området. En konkret verdi som skal beskyttes fra en trussel gjennom å ha så liten/lav sårbarhet som mulig. Ved at man selv kan velge hvilke uønskede hendelser man skal se på i en Bow-tie og grovanalyse vil denne være mindre konkret enn VTS-analysen. Grovanalysen gir da en større bredde i sine risikoområder.

Dokumentanalyser viser at ingen av de to analysemodellene som studeres, gir gode nok resultater alene til å kunne gi et fullverdig risikobilde. Dette er funn fra både rapporten *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* (Busmundrud, Maal, Kiran, & Endregard, 2015) og masteroppgaven *Modeller for risikoanalyse i Norge* (Kjelsaas, 2020). Kjelsaas (2020) oppgir at ingen av analysemodellene tilfredsstiller kravet gitt i virksomhetssikkerhetsforskriftens (2018, §12) knyttet til vurdering av risiko fullt ut. Som en konsekvens av dette vil trolig en endring av enten ROS (grovanalyse) eller VTS-modellen tvinge seg frem, alternativt at modellene fusjonerer fra to- og trefaktormodell til en fem-faktormodell (Kjelsaas, 2020).

Ved at våre to analyser i all hovedsak ser på forskjellige elementer i sine vurderinger mener vi at hver av dem har fordeler og ulemper som den andre analysen ikke har. Dette gjør at hver av dem har faktorer, som kan utelukke den andre. Imidlertid får vi en kombinasjon av styrkene til hver av dem når de brukes sammen, og svakhetene reduseres. Det vil for eksempel være en løsning å benytte grovanalysen for å identifisere ulike uønskede hendelser som kan ramme en organisasjon. Her vil man også da kunne se hvilke sannsynlighets-reduserende og konsekvensreduserende tiltak (barrierer), som sammen viser hvilke sårbarheter som finnes i organisasjonen. Så kan man videre gå inn med en mer spisset tilnærming mot verdi, trussel og sårbarhet.

Et interessant funn fra dokumentanalysen viser at valg av analysemetode ikke nødvendigvis er det viktigste. Hvor bevisst man er ift. hensikten med metoden, deltakernes kompetanse og hvordan analysegruppen er satt sammen kan være mer vesentlig enn valg av metode (Busmundrud, Maal, Kiran, & Endregard, 2015).

7. Drøfting

I dette kapittelet drøftes ulike elementer fra våre funn opp mot teori fra pensum direkte knyttet til oppgaven, og teori knyttet til faget SAM 510. I tillegg benyttes også supplerende litteratur for å belyse prosjektets problemstilling og forskningsspørsmål.

7.1 Sannsynlighetsteori og funn fra VTS- og grovanalyse

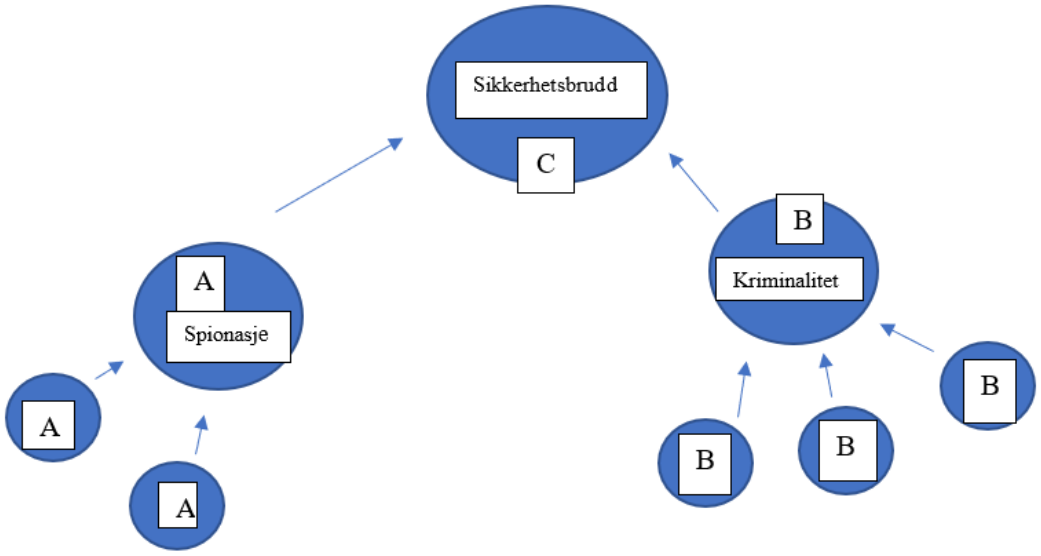
I analysene har vi gjennomført risikovurderinger og sett på mulige årsaker og deres konsekvenser. Analysene belyser sannsynligheter på ulike måter. Betingede sannsynligheter tar utgangspunkt i at sannsynligheten for at hendelse A blir påvirket dersom hendelse B skjer. Det vil si at A er avhengig av B og visa versa. Formelen for betinget sannsynlighet defineres i formelen P(A \ B) = P(A og B)/P(B) (Aven, Røed, & Wiencke, s. 206).

Det motsatte omtales for uavhengige hendelser der sannsynligheten for at hendelse A ikke vil påvirke hendelse B. Gjennom funnene våre fra begge analysene, VTS- og bow-tie/grovanalyse kan det argumenteres for betingede sannsynligheter. Eksempel på dette fra VTS-analysen er at den i seg selv handler om den avgjørende sammenhengen og avhengigheten mellom verdi, trussel og sårbarhet. Scenariobeskrivelsene i VTS-analysen illustrerer også betinget sannsynlighet godt ved å belyse sårbarhetene gjennom sannsynligheten for at en hendelse oppstår som påvirker hendelse B på en negativ måte. I motsetning til Bow-tie beskriver ikke VTS-analyse sannsynlighetsreduserende barrierer. Funnene våre tilsier at dette ikke har det store utsalget på betingede sannsynlighet, i og med at analysene samlet sett oppsummerer et risikobilde.

I Bow-tie blir betingede sannsynligheter illustrert ved å vise til de sannsynlighetsreduserende og konsekvensreduserende tiltakene. For en mer kompleks vurdering enn Bow-tie kunne alternativt Bayes nettverk som metode vært benyttet. Felles for begge metodene er den visuelle effekten og studie av betingede sammenhenger hvor et utfall avhenger av andre utfall. I flere metoder for analyse av risiko gjøres en oppdateringer av risikobildet når ny informasjon eller ny kunnskap fremkommer. Styrken med å bruke Bayes nettverk er at sammenhenger visualiseres klart og at betingede sammenhenger dermed klargjøres. Bayes nettverk kan benyttes på tross av manglende data, og gir mulighet for å kombinere kvalitative og kvantitative data. Både ekspertkunnskaper og informasjon fra historiske data kan inkludere i nettverket. Gjennom den såkalte Bayes formel oppdateres sannsynlighetene når det tilkommer ny informasjon og kunnskap (Aven T. , 2006, ss. 27-28). For en videre analyse

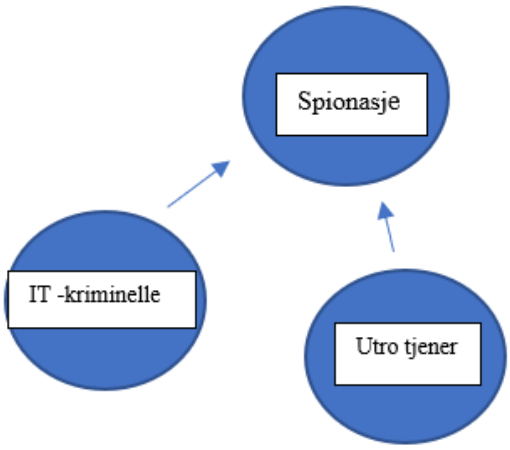
av det problemkomplekset som behandles i oppgaven, kunne alternativt Bayes nettverk benyttes.

Illustrasjonen i bilde 3 under viser Bayes nettverk der hendelsene er beskrevet som *noder* og pilene illustreres som *avhengighetene*:



Bilde 3 Bayes nettverk

I eksempelet er spionasje og kriminalitet det som beskrives som *foreldrenoter* til noden *sikkerhetsbrudd*. Hendelsene er hentet fra grovanalysen beskrevet i oppgaven. Dersom det fremkom ny kunnskap utover det som allerede var beskrevet i analysen, kunne denne visuelt være med på å beskrive dette (Aven T. R., 2008).



Figur 3 Tentativ ny kunnskap til analysen tilkommer, og blir en del av det opprinnelige nettverket i Bayes nettverk.

VTS-analysen ser primært på tilsiktede og ondsinnede handlinger. Grovanalyse kan og se på problemstillinger som dreier seg om ulykker som følge av naturkatastrofer o.l. Når vi utførte analysene om sikringstiltak ved Sola rådhus valgte begge gruppene å se på tilsiktede uønskede hendelser og ondsinnede handlinger. På den ene siden er det muligens her VTS-analysen egner seg bedre enn en grovanalyse. Årsaken til dette mener vi, er sannsynlighets-elementet i grovanalysen. I scenariene vi valgte, og scenarier generelt er det å vurdere sannsynlighet for et angrep vanskelig. Som beskrevet i teorikapittelet om risiko, er det enklere å oppdage konsekvenser enn sannsynligheter. Når leseren/mottakerne av analysen leser sannsynlighetsvurderingene, må dette sees i rett sammenheng. Eksempel på dette er benyttet i begge analysene gjennom PST sine trusselvurderinger vedrørende terror. I grovanalysen vurderes denne som lite sannsynlig. Ved å lese dette ut av en analyse kan det være en falsk trygghet og konkludere med at det er lite sannsynlig å bli utsatt for terror. Det er derfor viktig å reflektere over at når PST og andre arbeidsgrupper gjør disse beregningene kan to mulige forutsetninger ligge til grunn for denne sannsynligheten. Den ene kan være mangelen på oversikt, og tilstrekkelig etterretning, over aktører som har kapasitet og intensjon om å utføre en terrorhandling. Den andre kan være at man nettopp har god oversikt og kontroll over potensielle trusselaktører og kjenner godt til kapasitet og intensjon. Det vil si at to helt motsatte årsaker kan ligge til grunn for samme sannsynlighetskonklusjon.

7.2 Sikkerhetsinformasjonssystemer (SIS)

Når vi ser på sikkerhetsinformasjonssystemer (SIS) tilknyttet til Sola rådhus og hindring av uønskede hendelser må dette knyttes opp mot sikkerhetskultur, og ikke minst informerende kultur (Reason, 1997, s. 195). Reason identifiserer fire topologier som består av rapporterende-, fleksible-, rettferdige- og lærende kultur. Sammen virker de på hverandre som en informerende kultur. Denne kulturen blir viktig når man skal sørge for at SIS blir implementert inn i organisasjonen. Det vil være til liten hjelp å ha utviklet et godt informasjonssystem hvis ikke den informerende sikkerhetskulturen er til stede.

I kompendiet *Samfunnssikkerhet* (2020) av Njå, Sommer, Rake og Braut, forteller de at SIS har blitt et selvsagt element i den moderne sikkerhetsstyringen. *"Informasjon om uønskede hendelser (ulykker/nestenulykker) blir registrert, analysert og benyttet som grunnlag for å utvikle og implementere risikoreduserende tiltak"* (Njå, Sommer, Rake, & Braut, 2020, s. 131). Videre legger de frem at gjennom bruk av SIS og effekten av tiltakene kan man

registrere eventuelle reduksjoner i antall hendelser eller alvorligheten av hendelsene. På denne måten vil man kunne bruke resultatene av registreringene til å kontinuerlig forberede sikkerhetsnivået eller tiltakene i organisasjonen (Njå, Sommer, Rake, & Braut, 2020). Dette står i god sammenheng med funnene fra begge analysene, der risikoen reduseres ved implementering av risikoreduserende tiltak. Teorien om strategier for valg av risikohåndtering kan også støtte den risikoreduserende effekten som beskrives gjennom SIS. I begge analysene valgte gruppen å ikke akseptere risikoen, men håndtere den ved å presentere tiltak.

Knytter vi det vi vet om SIS opp mot de kritiske samfunnsfunksjonene som Sola rådhus og kommunen er en del av, vil det være nødvendig at man har en god rapporterende kultur. Bruk av SIS vil være en vesentlig faktor når man ser på problemstillingen vi har valgt i oppgaven. Sikringsanalysene vi har benyttet oss av inneholder faktorer som sårbarhet hos VTS-analysen, og sannsynlighetsreduserende tiltak og konsekvensreduserende tiltak gjennom bow-tie og grovanalysen. For at disse faktorene skal ha noe troverdighet er det viktig å benytte rapporter fra SIS om hvor manglene, sårbarhetene og usikkerheten ligger i organisasjonen. Dette handler om innsamling, analyse og bruk av erfaringsdata, som er hovedhensikten med SIS.

"*Resultatene fra SIS analysene – og i noen tilfeller rådata, for eksempel informasjon om enkelthendelser – blir spredt til beslutningstakere i ulike deler av organisasjonen. Det blir så utarbeidet tiltak som blir implementert i produksjonssystemet. Tiltakene, for eksempel sikkerhetskampanjer, endring av sikkerhetsdesign, opplæring av personell, sammen med enkelte analyseresultater, for eksempel utvikling i antall Lost Time Accidents (LTA) er den viktigste tilbakemeldingen til produksjonssystemet fra SIS*" (Njå, Sommer, Rake, & Braut, 2020).

Vi kan av beskrivelsen ovenfor tolke det slik at tiltakene som blir utarbeidet etter SIS, er de samme tiltakene vi benytter oss av når vi ser på VTS-analysen sin sårbarhet og Bow-tie sine barrierer for at en uønsket hendelse skal oppstå. Funnene om identifiserte sårbarheter i VTS-analysen, baserte seg på gruppens tolkning av den tilgjengelige informasjonen om trusselaktørene. Ytterligere informasjon via SIS kunne økt troverdigheten til analysen. Bow-tie på den andre siden legger opp til idemyldring knyttet til funn om sårbarheter. Her hadde SIS kunnet vært supplerende informasjon, uten at det nødvendigvis gikk ut over analysens troverdighet av funnene om sårbarheter. Dersom vi samlet skal presentere et eksempel fra

funn som går på tvers av analysene ser vi at eksempelvis terror rangeres som en høy sårbarhet i begge analysene. Her knyttes dette opp til sårbarheten for liv og helse, og hvilke konsekvenser det kan få for de som rammes. I og med at liv og helse er en verdi som rangeres høyt i de fleste risikoanalyser, er det ikke for en slik verdi avgjørende med rapporter fra SIS.

7.3 Risikomodellering

Risikoanalyser er kort oppsummert en systematisk studie av risiko. Det finnes ulike modeller for risikoanalyser (Aven T. , 2006), og valg av metode bestemmes ut fra hva som skal studeres. Risikoanalyser kan være modellert basert på kvantitative eller kvalitative data. Kvantitative data er data i form av tall eller andre mengdetermer, mens kvalitative data består normalt av tekst (Grønmo, 2020). Risikoanalyser kan benyttes som beslutningsstøtte når det skal treffes valg av løsninger og tiltak knyttet til risiko. Slike analyser gir bl.a. nyttig informasjon om prioritering av løsninger og tiltak, om risikoen er akseptabel for systemet som ses på, og gir økt forståelse for systemet, samt samvirke mellom ulike deler av systemet (Aven T. , 2006). Ved valg av metode for risikoanalyse er det viktig at sluttresultatet skal kunne gi en robust beslutningsstøtte. Dette vil også påvirkes av rammebetingelsene til virksomheten, og ved valg av metode spiller faktorer som tilgjengelige ressurser, problemsstilling som skal studeres, risikoakseptkriterier, metodikk for risikohåndtering og hvilken tilgang man har på data inn (Standard Norge, 2008). Felles for risikoanalyser er at de gjennomføres etter hovedtrinnene; 1) planlegging, 2) risikoanalyse og 3) Risikoevaluering (Standard Norge, 2008). Allerede i planleggingsfasen velges type analysemodell, som passer det som skal studeres. Prosjektgruppen har fulgt disse trinnene i gjennomføringen av VTS- og grovanalyse i denne oppgaven.

Prosjektgruppen har sett nærmere på enkelte kvalitative metoder som feilmodi- og feileffektanalyse (FMEA), hazard and operability studier (HAZOP), feiltreanalyse (FTA, kan også være semikvantitativ), ROS-analyse, verdi-trussel-sårbarhet (VTS) og grovanalyse, og semikvantitative metoder (kombinerer kvalitative og kvantitative) som grafisk feilutviklingsanalyse (GFUA) og hendelsestreanalyse (kan også være ren kvantitativ metode). Avhengig av hva som skal studeres vil det også være aktuelt å kombinere ulike analysemetoder, inkludert kvalitative og kvantitative analyser.

I case-studiet for oppgaven studeres tilsiktede uønskede handlinger, inkludert kriminell aktivitet. Dette har være styrende for valg av analysemodell. FMEA, FTA og GFUA i

kombinasjon med hendelsestrær er analysemetoder som passer godt til analyser av tekniske systemer. I tillegg krever disse analysene stor tilgang på data. En styrke med disse metodene er at de gir detaljerte oversikt over og kunnskap om systemene som studeres, og gir god læring (Aven T. , 2006). Imidlertid anses metodene som uegnet for vårt case- studie. Dette både fordi tekniske systemer og komponenter ikke studeres i detalj, og at det i prosessen med oppgaven har vært begrenset tilgang på data.

HAZOP kan beskrives som *"en systematisk analyse av hvorledes avvik fra konstruksjonsbetingelsene for et system kan oppstå, og hvorvidt disse avvikene kan forårsake risikoforhold"* (Aven T. , 2006, s. 89). Heller ikke denne metoden anses som relevant, da denne metoden også er mer rettet mot tekniske systemer.

Grovanalyse, der farer analyseres ut fra sannsynlighet og konsekvens, er en metode både brukt for sikkerhet- og sikringshendelser. Når det gjelder tilsiktede uønskede hendelser kan det være problematisk å hensynta sjeldne, overraskende hendelser, såkalte sorte svaner[1], i denne metodikken, da det er vanskelig å kvantifisere sannsynligheten for at slike hendelser vil skje. Dette kan ha vært en av årsakene til valg av hendelser og hendelsesscenario. VTS-analyse er utarbeidet for sikringshendelser, og var således et naturlig valg når metode ble valgt. Teorien om trusler og tilsiktede handlinger baserer seg på begrepet security. Dette er direkte knyttet til av verdi, trussel og sårbarhet og støttes av funnene i vår oppgave. I denne prosjektoppgaven har vi valgt å triangulere disse to risikomodellene for å studere analyse-objektet vårt fra to ulike perspektiv. For sikringshendelser er det ikke nok at man f.eks. bruker grovanalyse som eneste metode, da denne som nevnt ikke vil kunne si noe om sannsynlighet for sikringshendelser.

Positive sider med alle risikoanalyser er at metodene er systematiske, bevisstgjør involvert personell og vil kunne gi økt forståelse for systemene som studeres. I tillegg vil de kunne være en god beslutningsstøtte, forutsatt at sluttresultatet er riktig. Kvalitative metoder, der systemet og risiko beskrives med tekst, kan være enklere for mange involverte å forstå, sammenlignet med kvantitative metoder der risiko presenteres ved hjelp av tall og frekvenser.

[1]Metaforen *sorte svaner* ble introdusert av Nassim Taleb i 2007, og er et bilde på store og alvorlige hendelser som kommer helt overraskende på, altså hendelser som er veldig sjeldne. Hendelsene anses som umulige og skjer helt uventet, de har voldsomme følger og selv om de anses som umulige, så kan de forklares sett i retrospekt med den kunnskapen som var til stede på tidspunktet på hendelsen, men ingen så betydningen av denne kunnskapen (Justis- og beredskapsdepartement, 2016).

Dersom man ikke hensyntar usikkerhet i både kvalitative og kvantitative metoder vil begge fremgangsmåtene kunne gi et misvisende risikobilde.

7.4 Ekspertvurderinger

Ved gjennomføring av risikoanalyser vil bruk av ekspertise (fagkunnskap) kunne bidra med verdifulle innspill til analysen. Formålet med risiko- og sårbarhets- analyser er å finne feil og svakheter ved en spesiell løsning eller tiltak. Eksperten vil i slik analyser, bl.a. kunne belyse hvordan noe fungerer, forstå hva som medfører at noe ikke fungerer samt finne ut hvor stor sannsynligheten er for at dette skal kunne skje (Njå, Sommer, Rake, & Braut, 2020). I utviklingen av nasjonalt risikobilde i 2009 ble det benyttet eksperter. Erfaringer viste at eksperter kan benyttes til å tildele sannsynligheter til basishendelser, adressere og tildele sannsynlighetsfordeling til parametere, etablere passende modeller av "den virkelige verden", bidra i beskrivelser av scenario, sette prognose for utvikling og gjøre antagelser og formidle anbefalinger til beslutningstakere (Njå, Vastveit, Braut, & Holte, 2012).

Vurderinger fra eksperter går utover åpenbare uttalelser av fakta, data eller konvensjonene om disiplin (Njå, Vastveit, Braut, & Holte, 2012). Eksperter har som oftest særegne fagområder vedkommende kjenner inngående, og som vedkommende er ekspert innenfor. Eksperter innehar noe mer enn faglig kompetanse. De kjenner fagfeltet sitt så godt at de bl.a. kan foreta beslutninger basert på intuisjon (Njå, Sommer, Rake, & Braut, 2020).

I våre analyser har vi ikke hatt tilgang til eksperter, som f.eks. teknisk personell med inngående kunnskap om rådhuset, personell som kunne vært med å vurdere aktuelle scenarioer fra f.eks. NAV eller personell som kunne bidratt i trusselvurderingen, f.eks. ansatte i politiet. Dette gir klare svakheter ved gjennomføring av vår analyse, og har påvirket funnene i begge analysene. Teorien vår om risiko beskriver vanskeligheter med risikobedømming, dersom det er manglende kunnskap og erfaring knyttet opp mot sannsynligheter og konsekvenser. Dette gjenspeiler begge analysene.

Eksempelvis har det i de gjennomførte analysene vært utfordrende å vurdere sannsynlighet for at de tilsiktede uønskede hendelsene vil kunne skje. Vår vurdering av risikobilde er basert på erfaringer fra prosjektgruppens medlemmer, tilgjengelig informasjon funnet på internett, og er ikke nødvendigvis basert på informasjon fra regionen analyseobjektet tilhører. I denne vurderingen ville det ha vært fordelaktig om ekspertise fra f.eks. politi eller forsvar kunne

bidratt. De hendelsene, som vi har studert, er gjerne karakterisert ved at de inntreffer sjelden, og det har ikke vært mulig eller fornuftig å bruke statistikk for å sannsynliggjøre om og når tilsiktede uønskede hendelser kan inntreffe. Dette er funn som samsvarer med studien av nasjonalt risikobilde i 2009 nevnt over. Selv om denne analysen foregår på et landsdekkende nivå, mener vi det vil være paralleller til vårt analyseobjekt. Her fremkommer at ekspertise kan være nyttig der det er ingen eller lite historiske data tilgjengelig vedørende tekniske, menneskelige eller organisatoriske feil og deres konsekvenser på storulykkescenarioer. Når hendelsene, som studeres, er så sjeldne at lite eller ingen statistiske bevis er mulig å få tak i, argumenteres det for at det kan være nødvendig å ha eksperter til å ekstrapolere sannsynligheter, fysisk kvantiteter eller påvirkning på ekstreme hendelser fra eksperimentelle resultater eller simuleringer (Njå, Vastveit, Braut, & Holte, 2012).

Hvis vi skulle trukket inn eksperter i våre analyser kunne vi raskt ha støtt på utfordringer med å identifisere hvem disse er, og hva de skal velges ut på bakgrunn av. Dette også med tanke på at vi ikke har kjennskap til kvalifikasjoner, som ansatte i Sola rådhus eller i andre aktuelle organisasjoner har. Dette ville krevd at vi kartla aktuelle personer. Njå et al beskriver fem områder som eksperten kan vurderes ut fra: personlig kunnskap, informasjonskildene til eksperten, hvordan eksperten kan påvirke faktorer, som kan dominere vurderingsevnen (såkalte biaser), personlige interesse og tidligere erfaringer (Njå, Sommer, Rake, & Braut, 2020). Prosjektgruppen ser behov for at ekspertvurderinger, herunder valg av eksperter, blir standardisert. Dette var også konklusjonen i vurderingen av bruk av eksperter ved utvikling av nasjonalt risikobilde i 2009 (Njå, Vastveit, Braut, & Holte, 2012).

Det er viktig å være klar over at det kan være heuristikker som påvirker eksperten, dvs. at ulike faktorer kan påvirke eksperten, såsom tilgjengelighet i minnet, ankring og tilpasning og representativitet, slik at man kommer til en feil vurdering (såkalt bias). Eksperter kan også blir overkonfidente (Njå, Sommer, Rake, & Braut, 2020). På tross av dette mener prosjektgruppen at eksperter kan og bør bidra i risikoanalyser.

7.5 Risikoindikatorer

I kompendiet *Samfunnssikkerhet* av Njå et al., omhandles risikoindikatorer i liten grad, men det henvises til Helene Kjær Thorsen sin masteroppgave fra 2013 (Njå, Sommer, Rake, & Braut, 2020). I denne oppgaven trekkes det fram at indikatorer ofte har vært brukt til å måle

allerede inntrufne hendelser, som antall personskader og fraværsskader. I oppgaven undersøker Thorsen om ledende risikoindikatorer kan brukes som en feedbackmekanisme, for å predikere storulykker i olje- og gassindustrien (Thorsen, 2013). En risikoindikator kan være "*en målbar eller observerbar størrelse som kan gi informasjon om risiko*" (Vinnem, 2003). For å finne risikoindikatorer knyttet til sikringsforhold ved Sola rådhus, kan man ta utgangspunkt i de risikoene som er identifisert gjennom de to analysemodellene. Det er brukt to analysemodeller som vektlegger ulike perspektiver ved risiko. Komparasjonen skal gi oss et bedre bilde over sikringsrisikoene. På grunn av lav frekvens i antall sikringshendelser knyttet til kommunehus og offentlige bygg, kan det være vanskelig å knytte risikoindikatorene til sammenlignbare hendelser. Samtidig kan forhold knyttet til vurdering av verdier, trusler og sårbarhet, som beskrevet under VTS analyse, påvirke valg av indikatorer. Det samme kan funn fra grovanalysen som viser høy grad av risiko på beskrevne områder. Ekspertvurderinger kan også gi informasjon om hvilke indikatorer som kan fungere som en feedbackmekanisme for å predikere sikringshendelser. For eksempel kan NSM ha etterretninger om cyberangrep mot norske kommuner. Da kan vurderinger av forhold knyttet til sannsynlighet, konsekvens, verdier, trusler, sårbarheter og usikkerheter, være faktorer som kan gi informasjon om hvilke indikatorer som bør velges i forhold til IKT-trusselen mot rådhuset.

7.6 Ytelse

Ytelse i samfunnssikkerhetsperspektiv knyttes til beredskap og krav til pålitelighet, effektivitet (kapasitet, tid) og sårbarhet, i de forebyggende- og skadebegrensende beredskapstiltakene som blir brukt (Njå, Sommer, Rake, & Braut, 2020).

Krav til ytelse innen beredskapen identifiseres gjennom risikostyringsprosessen, og knyttes til de spesifikke fare- og ulykkessituasjonene. Njå et al. 2020 poengterer at *"Ytelseskravene formuleres for å sikre at beredskapssystemet holder en tilstrekkelig høy ytelse til å kunne møte relevante fare- og ulykkessituasjoner"* (Njå, Sommer, Rake, & Braut, 2020, s. 171). Beredskapsnivået bestemmes gjennom ytelseskravene og ikke de identifiserte fare- og ulykkessituasjonene (Njå, Sommer, Rake, & Braut, 2020).

I oppgaven er det brukt to ulike metoder i risikostyringsprosessen. Funn fra grovanalysen har gitt gruppen et bredt perspektiv på risikoene, med utgangspunkt i den nasjonale

risikovurderingen til PST. VTS analysen på en annen side, har gitt oss dybdekunnskap om de mest alvorlige risikoene. Gruppen mener at denne variasjonen av bredde og dybde i kunnskapen, har gjort oss i bedre stand til å sette konkrete krav til pålitelighet, effektivitet og sårbarhet, i beredskapssystemene knyttet til rådhuset. Det gir og et bilde av fordelene med å benytte analyser som kan supplere hverandre ved sikring.

7.7 Risikostyring (Aven T, 2007, kapittel 1-3)

I denne oppgaven har gruppen valgt å studere hvordan to ulike risikomodeller kan supplere hverandre, i arbeidet med styring av sikringsrisikoer knyttet til bygging av nytt rådhus i Sola. I Aven sin bok Risikostyring, skriver han at det *"altfor ofte må en alvorlig hendelse til for at risikostyringen skal komme i fokus, og da blir konsekvensene gjerne overreaksjoner og uheldige prioriteringer"* (Aven T. , 2007). Fem år etter Aven skrev dette gikk en bombe av i regjeringskvartalet, med fatale konsekvenser for mennesker og infrastruktur. Sola rådhus stod ferdig våren 2020. Aven skriver videre at utviklingen i samfunnet har ført til *"større grad av sårbarheter og risikoer, men styringen av disse sårbarhetens og risikoene er i mange henseende ufullstendige eller ikke-eksisterende"* (Aven T. , 2007, s. 13). I tiden etter terrorangrepene den 22. juli 2011, har antiterror tiltak blitt mer og mer synlige på offentlige steder og rundt ulike bygg. Prosjektgruppen har opplevd, at informasjon utenom det som ligger offentlig tilgjengelig på nett, er vanskelig å få tak i. Dette gjør det utfordrende å etterprøve Aven sin påstand om at terrortiltakene bærer preg av overreaksjoner og uheldige prioriteringer vedrørende sikring av bygg. Det blir også vanskelig å vurdere om risiko-styringen rundt de tiltakene som er iverksatt har vært ufullstendig eller fraværende.

Aven beskriver risikostyring som *"alle de tiltak og aktiviteter som gjøres for å styre risiko"* (Aven T. , 2007, s. 13). Risikostyring dreier seg om å skaffe seg innsikt i risikoforhold, effekt av tiltak og vurdering av hvilken grad risiko lar seg styre. Metoder, prosesser og strategier for å kunne kartlegge og styre risikoene, er også en del av risikostyringen. Aven skriver også at: *"Formålet med risikostyringen er å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap"* (Aven T. , 2007, s. 15). Når man skal veie mulige gevinster mot mulige risikoer, handler risikostyring om verdispørsmål og politikk.

I denne oppgaven har prosjektgruppen valgt å bruke to analyseteknikker, for å studere hvordan disse kan supplere hverandre i risikostyring av sikring. I forbindelse med

gjennomføring av analysene har det vært et poeng at undergruppen som jobbet med VTS-analyse ikke hadde kontakt med gruppen som jobbet med grovanalyse. Hensikten med dette har vært å studere hvordan de ulike metodene og perspektivene på risikostyring, vil påvirke resultatene av prosessene. Ulikheter i funnene til de to gruppene, kan således argumentere for at metode og perspektiv påvirker utfallet av prosessen.

Et annet poeng er at grovanalyse tilnærmingen legger til grunn et syn på risiko som et produkt av sannsynlighet og konsekvens, som tar utgangspunkt i et realistisk/positivistisk syn på risiko som er forankret et naturvitenskapelig syn på verden (Engen, et al., 2017). VTS analysen har på en annen side et konstruktivistisk kunnskapssyn som er forankret i de samfunnsfaglige og historisk filosofiske perspektivene på risiko (Engen, et al., 2017). Ved en komparasjon av disse metodene vil målet være å få frem synspunkter som er forankret i to ulike grunnsyn på risiko.

Forventningen til utfallet av en aktivitet som innebærer risiko vil variere ut ifra hvilket perspektiv de som vurderer risikoen bruker (Aven T. , 2007). Kommunikasjon rundt de ulike perspektivene vil være viktig for å forhindre uenigheter mellom undergruppene som jobber med VTS og grovanalyse.

7.8 Reflections on the Ontological Status of Risk (Artikkel: Solberg og Njå)

Artikkelen "Reflections on the Ontological Status of Risk" tar for seg risikobegrepet i et ontologisk perspektiv, med utgangspunkt i eksisterende metodiske og epistemologiske påstander om risiko. Prosjektgruppen skal drøfte den ontologiske vurderingen av risikobegrepet i artikkelen, i sammenheng med komparasjon av analyseteknikkene VTS- og grovanalyser ifm. sikringsanalyse av nytt rådhus i Sola. Begrepet ontologi blir beskrevet som læren eller studiet av hva som er og eksisterer. Det handler om verden og hva den inneholder, mens epistemologi handler om menneskets kunnskap og hvordan vi tilegner oss kunnskapen.

Rosa beskriver begrepet risiko som "*et stadium i verden hvor det er en sammenheng mellom usikkerhet om utfall og menneskelig bekymring for utfallet*". Usikkerheten må settes i en kontekst og relateres til noe som har verdi for mennesker, for å kunne gi risikobegrepet en ontologisk status (Rosa, 1998).

I artikkelen trekkes det videre frem to ulike tilnærminger for å svare på hva risiko er: For det første kan risiko beskrives som alle logiske mulige fremtidige tilstander. Med dette perspektivet vil risiko være objektivt sett reell og noe vi alltid står overfor, og kan komme med epistemologiske påstander om. Dette positivistiske synet på risiko passer med grovanalyse tilnærmingen i oppgaven, hvor grovanalysen tar sikte på å avdekke alle logiske hendelser som kan inntreffe med utgangspunkt i PST sin risikovurdering. På den andre siden står det i artikkelen til Solberg og Njå at risikobegrepet er åpent for tolkning, og det er opp til den enkelte å definere betydningen av risiko i relasjon til den enkelte kontekst. Artikkelen argumenterer for denne subjektive tolkningen av riskobegrepet. I dette tilfellet er risiko knyttet til våre verdier og hva vi verdsetter, og vil derfor påvirke hvordan vi vurderer og tar beslutninger knyttet til fremtiden. Denne tolkningen passer inn med et konstruktivistisk syn på risiko, som kommer til uttrykk i VTS-analysen gjennom vurderinger av verdier, trusler og sårbarhet.

Ved en komparasjon av to metoder som tar utgangspunkt i to ulike ontologiske perspektiver på risiko, ønsker prosjektgruppen å vise at analyseresultatene kan supplere hverandre. Målet er at komparasjonen vil gi en dypere innsikt og kunnskap om risikoene, knyttet til sikring av offentlige bygg i Norge.

8. Konklusjon

Målet med prosjektet er å vurdere om to forskjellige risikomodeller kan supplerer hverandre ved analyse av sikring. Problemstillingen er belyst ved å undersøke følgende forskningsspørsmål:

Hvordan tilnærmer de to analysemetodene seg til sikring av et bygg?

Vår analyse viser at det er en del likheter mellom VTS- og grovanalyse. Imidlertid har metodene noen klare forskjeller når det gjelder fremgangsmåte for sikring av bygg.

Grovanalysen har bred tilnærming ved at det kartlegges flere scenarioer for uønskede hendelser enn i VTS-analysen. Grovanalysen gir oversikt over både små og store potensielle hendelser mot en virksomhet. Den viser dermed et mer komplett bilde av potensielle hendelser/trusler/risiko tidlig i prosessen, da analysen ikke begrenser seg til enkeltscenarioer. Ved å benytte matrisen sannsynlighet/konsekvens vil det tidlig synliggjøres risiko ved at denne beskrives i trafikklysfargene grønn, gul og rød. Dette gjør at analytikeren lett kan oppfatte hvilke scenarioer som har høyest risiko, og dermed kan studeres nærmere. Grovanalyseskjemaet gir også en enkel oversikt over sannsynlighets- og konsekvensreduserende barrierer. Tilnærmingen til dybdestudie av de utvalgte scenarioer i vår analyse har også vært bredere, og mindre detaljfokusert, enn resultatet i VTS-analysen. Grovanalysen anbefaler sikringstiltak basert på sannsynligheter.

VTS-analysen gir klare føring for oppbygging av og informasjonsbehov i analysen, ved at verdi, trusler og sårbarheter direkte knyttet til sikringsobjektet kartlegges i en gitt rekkefølge. Analysen kan derfor fremstå, som veldig konkret. Samtidig gir VTS-analysen analytikerne oversikt over og bevissthet om de viktigste verdiene og trusselaktørene. Siden sårbarhetene vurderes ut fra valgte scenarioer, må valget av disse være relevante. VTS-analysen har et spesifikt fokus på enkeltscenarioer og konkrete sikringsmål, noe som kan være en styrke i metoden. VTS-analysen benytter gitte vurderingsskalaer for verdi og trussel, og har i tillegg egne indikatorer for trussel- og sårbarhetvurdering, som benyttes for å etablere det endelige risikobildet. Risikobildet vil vise beslutningstakerne hvilken risiko et bygg er eksponert for.

VTS-analysen anbefaler sikringstiltak basert på avdekte sårbarheter, og spesifiserer tiltakene knyttet til Mennesker, Teknologi og Organisasjon. Tiltakene kan fremstå som mer detaljert.

Selv om fremgangsmåten er ulik for VTS- og grovanalyse med sløyfediagram, viser våre analyser, at tilnærmet lik konklusjon trekkes når det gjelder risikobildet for Sola rådhus.

Gir en av analysemodellene tilstrekkelige resultater til å utelukke den andre?

Ut fra de områdene begge undergruppene har valgt å risikoanalyse ser vi at resultatene av risikovurderingene er relativt like. Sånn sett kan det sies at man kun behøver å benytte en av analysene. Går man derimot mer i dybden på hver av analysene vil det imidlertid oppdages flere forskjeller, da risikoen søkes identifisert på forskjellige måter. Prosjektgruppen mener derfor, at en av analysemodellene ikke overskygger den andre. Vi mener at å kombinere de to analysene vil gi et bedre sluttresultat, og høyne kvaliteten på analysene. Dette vil igjen gi bedre kunnskap til organisasjonen om usikkerhet, sårbarhet, sannsynlighet, konsekvens, verdi og trussel.

Hvilke svakheter og styrker fremkommer av å gjennomføre to forskjellige risikoanalyser?

Prosjektgruppen vurderer begge analyseverktøyene som gode, spesielt på hvert sitt område. Imidlertid har begge metodene styrker og svakheter når det gjelder risikovurdering av tilsiktede uønskede hendelser.

Grovanalysen gir et bredt spekter på hva som kan analyseres, mens VTS-analysen vurderes som mer spesifikk. Det er med andre ord opp til analysegruppen hvilken kunnskap og informasjon man kan innhente som vil avgjøre mengden og størrelsen på en slik analyse. Det er viktig å avgrense analysen til spesifikke områder eller rutiner for å begrense omfanget av analysene.

Grovanalysen gir mulighet til å se på risiko gjennom sannsynlighet og konsekvens. Dette er en svakhet for tilsiktede uønskede hendelser, da sannsynlighet vil være veldig vanskelig å anslå. VTS-analysen er et mye mer konkret verktøy for å lokalisere en risiko i et område med en verdi. Denne modellen er avhengig av at det eksisterer en verdi, trussel og en sårbarhet for at man skal kunne gjennomføre analysen. VTS-analysen har noen styrker og svakheter som spesielt kommer frem i denne analysen. Det første man ser er at man bør/må ha tilstrekkelig informasjon om faktorene som skal vurderes, hvis ikke så blir denne “spissede” analysen vanskelig å gjennomføre. Det kan være vanskelig å vite om man har fått god nok informasjon til å svare ut risikoanalysen. På den andre siden, hvis det er gode informasjonskilder vil resultatet bli av god kvalitet, og kunne skape en bevissthet i virksomhetene om verdier som skal beskyttes og prioritering av sikringstiltak. En annen styrke er at analysen er skjematisert,

som gjør at alle medlemmene i gruppen ikke trenger å være eksperter på gjennomføring av en VTS-analyse.

En svakhet med begge metodene er at de ikke sier noe om usikkerhet. Ved bruk av metodene er det også vanskelig å vurdere om hendelser er betinget av hverandre, og her kan man ved å inkludere et Bayes nettverk, klargjøre eventuelle betingede sammenhenger.

Hvordan kan to forskjellige risikomodeller supplere hverandre ved analyse av sikring?

Sola rådhus er et nytt bygg med moderne arkitektur i flotte omgivelser. Med et objekt som er så nyetablert vil det kunne være mange ″barnesykdommer″. Det er derfor viktig å gå bredt ut for å finne hva det skal sikres mot og hvordan sikring av bygget skal gjennomføres. Grovanalysen vil være et godt utgangspunkt for dette, da det kan gjennomføres en risikoanalyse av hvilke uønskede hendelser man kan se for seg, opp mot sannsynlighet og konsekvens. Etter gjennomføring av grovanalysen og resultatene foreligger, vil man kunne trekke ut de viktigste områdene med høyest verdi eller fare for trussel. Disse områdene kan overføres til en VTS-analyse for å gå nærmere inn i risikoarbeidet. Her blir oppgaven å beskytte verdien fra en trussel, ved å sørge for at sårbarheten er minst mulig.

Arbeidsoppgavene ansatte er satt til gjennom sitt daglige virke er ikke påvirket av at de nå er plassert i et nytt rådhus. Her vil de ansatte sannsynligvis være mer kjent med risikobilde opp mot de eventuelle kritiske ansvarsområdene man behandler. Dette gjør at risikovurdering av Sola rådhus er komplekst og krever en mer detaljert analyse som kan ta for seg alle aspekter. Man må se på alt fra objektets "barnesykdommer" når det kommer til sikring av bygg, til at ansatte fra tidligere er kjent med saksbehandling opp mot kritisk infrastruktur.

8. Referanser

Aven, T. (2006). *Pålitelighets- og risikoanalyse.* Oslo: Universitetsforlaget.

Aven, T. (2007). *Risikostyring. Grunnleggende prinsipper og ideer.* Oslo: Universitetsforlaget.

Aven, T. (2008). *Risk analysis : assessing uncertainties beyond expected values and probabilites.* John Wiley & Sons.

Aven, T. (2010, mars). Some reflections on uncertainty analysis and management. *Reliability Engineering & System Safety, 3*(95), ss. 195-201. Hentet fra https://www.sciencedirect.com/science/article/abs/pii/S0951832009002300?via%3Dihub

Aven, T. (2019, september 24). Usikkerhet. *Store norske leksikon*. Hentet mai 24, 2020 fra https://snl.no/usikkerhet

Aven, T. R. (2008). *Risikoanalyse.* Universitetsforlaget.

Aven, T., Røed, W., & Wiencke, H. S. (2017). *Risikoanalyse* (2. utg.). Oslo: Universitetsforlaget.

Bechensten, A. H. (2018, mai 25). Stavanger kommune utbetalte en halv million til svindlere. *Dagsavisen*. Hentet fra https://www.dagsavisen.no/rogalandsavis/stavanger-kommune-utbetalte-en-halv-million-til-svindlere-1.1149100

Borch, O. J. (2020, januar 10). Hybride trusler. *Nordnorsk Debatt*. Hentet fra https://nordnorskdebatt.no/article/hybride-trusler-0

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40. Hentet fra http://ngsuniversity.com/pluginfile.php/134/mod_resource/content/1/DocumentAnalysis.pdf

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* Forsvarets forskningsinstiutt (FFI). Hentet fra https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

Dale, O. H. (2020, februar 12). Sola rådhus. *Byggeindustrien*. Hentet fra http://www.bygg.no/article/1423548

DSB. (2014). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen.* Direktoratet for samfunnssikkerhet.

DSB. (2016). *Samfunnets kritiske funksjoner.* Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

DSB. (2017). *Samfunnssikkerhet i kommunens arealplanlegging.* Hentet fra https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/samfunnssikkerhet_i_kommunens-arealplanlegging_metode-for-risiko_og_saarbarhetsanalyse.pdf

DSB. (2019, Oktober). Risikoanalyse på samfunnsnivå: Metode og prosess ved utarbeidelsen av "Analyser av krisescenarioer (AKS)". Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/metode_og_prosess_ved_utarbeidelsen_av_aks.pdf

Engen, O. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E., & Pettersen, K. A. (2017). Perspektiver på samfunnssikkerhet. Cappelen Damm.

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). *Reliability: Theory & Applications, 2*(2), ss. 9-18. Hentet fra http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.568.7306&rep=rep1&type=pdf

Fondenes, E., Svendsen, R. H., & Bolstad, J. (2019, mai 29). Drapstrusler, trafikksabotasje og hærverk. *NRK*. Hentet fra https://www.nrk.no/vestland/drapstrusler_-trafikksabotasje-og-haerverk_-slik-er-den-skitne-siden-av-bompengeopproret-1.14567366

Fossum, E., & Børresen, M. F. (2013, oktober 19). Ansatte i barnevernet slått ned. *NRK*. Hentet fra https://www.nrk.no/innlandet/ansatte-i-barnevernet-slatt-ned-1.11306571

Geard, K. (2020, 01 24). Nær en av tre ansatte i barnevernet har vært utsatt for vold mer enn to ganger de siste to åra. *Fagbladet*. Hentet fra https://fagbladet.no/nyheter/nar-en-av-tre-ansatte-i-barnevernet-har-vart-utsatt-for-vold-mer-enn-to-ganger-de-siste-to-ara-6.91.674228.a1c6ba5476

Grønmo, S. (2020, mai 28). *Kvantitativ metode.* Store norske leksikon. Hentet fra https://snl.no/kvantitativ_metode

Husøy, E. (2019, Januar 09). PST tror statlig aktør kan ha stått bak cyberangrep mot fylkesmenn. *Aftenposten*. Hentet fra https://www.aftenposten.no/norge/i/vmorO4/pst-tror-statlig-aktoer-kan-ha-staatt-bak-cyberangrep-mot-fylkesmenn?

Hvistendahl, N. E. (2014, august 25). Dømt til tvungen psykisk helsevern. *NRK*. Hentet fra https://www.nrk.no/osloogviken/domt-til-tvungen-psykisk-helsevern-1.11896834

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser?* Høyskoleforlaget AS.

Jupskås, S. H. (2018, oktober 29). Nok er nok inntok bystyresalen. *Aftenbladet*. Hentet fra https://www.aftenbladet.no/lokalt/i/1kJGRG/nok-er-nok-inntok-bystyresalen

Justis- og beredskapsdepartement. (2016). *Meld. St. 10 (2016 –2017). Risiko i et trygt samfunn. Samfunnssikkerhet.* Oslo: Justis- og beredskapsdepartement.

Kjelsaas, B. M. (2020). *Modeller for risikoanalyse i Norge.* Oslo: (Masteroppgave) Høgskolen i Innlandet. Hentet fra https://brage.inn.no/inn-xmlui/handle/11250/2653397

Knutsen, K. A., & Christensen, P. (2019, desember 18). Flytter inn i forgylt rådhus i Sola. *Stavanger Aftenblad*. Hentet fra https://www.aftenbladet.no/lokalt/i/RR2jpa/flytter-inn-i-forgylt-radhus-i-sola

Krokfjord, T. P. (2014, januar 2). - Skjøt i taket på NAV-kontoret og holdt NAV-ansatt fanget på kontor. *Dagbladet*. Hentet fra https://www.dagbladet.no/nyheter/skjot-i-taket-pa-nav-kontoret-og-holdt-nav-ansatt-fanget-pa-kontor/61619489

Longva arkitekter. (2015, September). *Solas hjerte: arkitektkonkurranse nye Sola rådhus.* Hentet fra Nytt rådhus i Sola: https://nyttraadhussola.files.wordpress.com/2015/09/solas-hjerte-a1-plansjer.pdf

Martinsen, E. (2014, august 17). NAV-ansatte utsettes stadig for vold og trusler. *NRK*. Hentet fra https://www.nrk.no/osloogviken/opplever-mer-vold-og-flere-trusler-1.11882839

Midtgaard, A. K. (2018, september 26). *Risikoanalyser innen safety og security på samfunnsnivå - hva er likt og hva er ulikt?* Hentet fra https://esra.no/wp-content/uploads/2018/09/2.Risikoanalyser-for-safety-og-security-p%C3%A5-et-samfunnssikkerhetsniv%C3%A5_AnnMidtgaard.pdf

Moe, S. (2018, juni 9). Sikkerhetsekspert bekymret for norske kommuner. *E24*. Hentet fra https://e24.no/teknologi/i/VbgRWW/sikkerhetsekspert-bekymret-for-norske-kommuner-skremmende-daarlige-paa-it-sikkerhet

Multiconsult. (2016, September). *Formingsveileder for Sola sentrum.* Hentet fra https://docplayer.me/42968912-Formingsveileder-for-sola-sentrum-september-2016.html

Munkvik, C., & Norheim, H. J. (2018, Oktober 31). Politiet oppretter sak etter at bom-motstandere avbrøt bystyremøte. *Aftenbladet*. Hentet fra https://www.aftenbladet.no/lokalt/i/0EdA0A/politiet-oppretter-sak-etter-at-bom-motstandere-avbrt-bystyremte

NAV. (2019). *Vold og trusler mot ansatte i NAV 2019.* Oslo: NAV.

NAV. (u.å.). *Sikkerhet i NAV*. Hentet fra 10.06.2020 https://www.nav.no/no/nav-og-samfunn/samarbeid/noindex/sikkerhet-i-nav.

NAV; KS. (2014, desember 10). *Minimumsstandard med krav til fysisk utforming og sikring av NAV-kontor*. Hentet fra http://einnsyn.fosendrift.no/Bjugn/registryentry/ShowDocument?registryEntryId=20356&documentId=33610.

Njå, O., Aven, T., & Rettedal, W. (1998). *Subjective probability assignment in QRAs for offshore construction and cessation projects.* Sørco.

Njå, O., Sommer, M., Rake, E. L., & Braut, G. S. (2020). *Samfunnssikkerhet - analyse, styring og evaluering.* Oslo: Universitetsforlaget.

Njå, O., Vastveit, K. R., Braut, G., & Holte, M. R. (2012). A discussion on expert judgements in national risk analyses. *Advances in Safety, Reliability and Risk Management*.

Norske arkitekters landsforbund. (2015, november 18). Åpen plan- og designkonkurranse. *Norske Arkitektkonkurranser*(462).

NSM. (2016, mars). *Håndbok: Risikovurdering for sikring.* Hentet fra https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/risikovurdering-handbok/

NSM. (2019). *Risiko 2019 Krafttak for et sikrere Norge.* Nasjonal sikkerhetsmyndighet. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

NSM. (2020). *Risiko 2020.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm-risiko-2020.pdf.

NSM, E-tjenesten, DSB, PST. (2017). *Risiko 2017. Risiko og sårbarheter i en ny tid. En vurdering av sårbarheter og risiko i Norge.* Oslo. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

NSM; POD; PST. (2015). *Terrorsikring: En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger.* Oslo: Nasjonal Sikkerhetsmyndighet, Politidirektoratet & Politiets sikkerhetstjeneste. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder_terrorsikring_2015_enkelts_final.pdf

NTB. (2018, august 23). Bompengestriden. *Aftenposten*. Hentet fra https://www.aftenposten.no/norge/i/jPj5Ez/bompengestriden-stavanger-kommune-innfoerer-vakthold-paa-politiske-moeter?

NTB. (2018, august 17). Skoleelev varslet om datahull i Bergen. *VG*. Hentet fra https://www.vg.no/nyheter/innenriks/i/EoAnPA/skoleelev-varslet-om-datahull-i-bergen

NTB. (2020, mai 20). Bergen kommune vedtar rekordstor bot. *VG*. Hentet fra https://www.vg.no/nyheter/innenriks/i/0n2jaE/bergen-kommune-vedtar-rekordstor-bot

NUPI, N. U. (u.å.). *Komparativ metode*. Hentet fra https://www.nupi.no/Vaar-forskning/Temaer/Teori-og-metode/Komparativ-metode

O'Leary, Z. (2004). *The essential guide to doing reserach.* SAGE Publications.

Offentleglova. (2006, mai 19). I *Lov om rett til innsyn i dokument i offentlig verksemd (LOV-2006-05-19-16).* Hentet fra https://lovdata.no/lov/2006-05-19-16/§16

Personopplysningsloven. (2018). I *Lov om behandling av personopplysninger (LOV-2018-06-15-38).* Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=lov%20om%20behandling%20av%20personopp: https://lovdata.no/lov/2018-06-15-38

PST. (2019). *Temarapport: Hvilken bakgrunn har personer i høyreekstreme miljøer i Norge?* Oslo: Politiets sikkerhetstjeneste. Hentet fra https://www.pst.no/globalassets/artikler/utgivelser/temarapport_pst_-hvilken-bakgrunn-har-personer-i-hoyreekstreme-miljoer-i-norge.pdf

PST. (2020). *Nasjonal trusselvurdering 2020.* Hentet fra www.pst.no: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* New York: Routledge.

Regjeringen. (2020, 05 05). *Liste over virksomheter med kritisk samfunnsfunksjon og nøkkelpersonell som kan få tilbud om plass i barnehage og barneskole (oppdatert*. Hentet fra https://www.regjeringen.no/contentassets/8da70b8196a24296ae730eaf99056c1b/liste-over-kritiske-samfunnsfunksjoner-tabell.pdf

Rosa, E. A. (1998). *Metatheorethical foundations for post-normal risk.* . Journal of Risk Research 1, no. 1: 15-44.

Sikkerhetsloven. (2019). I *Lov om nasjonal sikkerhet (LOV-2018-06-01-24).* Hentet fra https://lovdata.no/lov/2018-06-01-24

Skjetne, O. L. (2017, september 26). E-tjenesten advarer om russiske aktører. *VG*. Hentet fra https://www.vg.no/nyheter/innenriks/i/zadVO/e-tjenesten-advarer-om-russiske-aktoerer-sabotasje-av-stroem-og-infrastruktur

Sola kommune. (2015, november 19). *Overordnet bereskapsplan: Administrativ del.* Hentet fra https://www.sola.kommune.no/_f/p1/i277bd24f-e2fb-42f8-9c1a-69fddee209aa/beredskapsplan.pdf

Sola kommune. (2016a, november 18). *Reguleringsbestemmelser i tilknytning til detaljplan for 0562 Kommunehus, torg og park.* Hentet fra http://webhotel3.gisline.no/GisLinePlanarkiv/1124/0562/Dokumenter/P3%20planbestemmelsene%2018.11.2016.pdf

Sola kommune. (2016b, desember 14). *1. Gangsbehandling detaljregulering kommunehus, bypark og rådhusplass - Plan 0562.* Hentet fra http://webhotel3.gisline.no/GisLinePlanarkiv/1124/0562/Dokumenter/saksfremlegg%201.gangsbehandling%20Kommunehus,%20bypark%20og%20r%C3%A5dhusplassen.pdf

Sola kommune. (2016c, oktober 28). *Merknader ved varsel om oppstart.* Hentet fra http://webhotel3.gisline.no/GisLinePlanarkiv/1124/0562/Dokumenter/P4%20merknader%20ved%20varsel%20om%20oppstart.pdf

Sola kommune. (2020a, 02 13). *Planer og rapporter - nytt rådhus*. Hentet fra Sola kommune: https://www.sola.kommune.no/planer-og-rapporter/nytt-radhus/

Sola kommune. (2020b). *Årsrapport 2019*. Hentet fra https://www.sola.kommune.no/_f/p1/icda311bd-3e80-4ea4-a7c7-8174bee82022/Årsrapport%202019%20Sola%20komune%20med%20kommunale.pdf

Sola kommune. (u.å.). *Personvernerklæring*. Hentet fra 10.06.2020 https://www.sola.kommune.no/personvernerklaring/.

Solli, M. (2020, Mai 08). Prøver å svindle skoleelever. *Nettavisen*. Hentet fra https://www.nettavisen.no/okonomi/prover-a-svindle-skoleelever-teams-og-office-under-angrep/3423962728.html

Standard Norge. (2008). *Krav til risikovurderinger (NS 5814:2008).* Oslo.

Standard Norge. (2012). *Samfunnsikkerhet: Beskyttelse mot tilsiktede uønskede handlinger - terminologi (NS 5830:2012).* Oslo.

Standard Norge. (2014a). *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse (NS 5832:2014).* Oslo.

Standard Norge. (2014b). *Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger: Krav til sikringsrisikostyring (NS5831:2014).* Oslo.

Stranden, A. L. (2018, juni 19). Slik har terrorister siktet seg inn mot myke mål. *Forskning.no*. Hentet fra https://forskning.no/kriminalitet-juridiske-fag-ny/slik-har-terrorister-siktet-seg-inn-mot-myke-mal/259457

Stranden, R. (2019). *Sikring. En innføring i teori og praksis.* Oslo: Gyldendal Norsk Forlag.

Thorsen, H. K. (2013). *Monitorering av storulykkesrisiko i drift av offshore installasjoner. En studie av ledende indikatorer.* (Masteroppgave) Universitetet i Stavanger. Hentet fra https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/182267/Masteroppgave%2030.06.pdf?sequence=1&isAllowed=y

Vinnem, J. E. (2003). *Structured approach to risk indicators for major hazards.* ESRL.

Virksomhetsikkerhetsforskriften. (2018). I *Forskrift om virksomheters arbeid med forebyggende sikkerhet (FOR-2018-12-20-2053).* Hentet fra https://lovdata.no/forskrift/2018-12-20-2053

Wennersten, R. (2003). Industriell riskhantering. I G. Grimvall, P. Jacobsson, & T. Thedéen, *Riskar i tekniska system* (ss. 235-252). Lund: Studentlitteratur.

With, M. L. (2017, august 15). Politiske ressurser og deltakelse. Hentet fra Slik har vi det – livskvalitet og levekår: https://www.ssb.no/sosiale-forhold-og-kriminalitet/artikler-og-publikasjoner/politiske-ressurser-og-deltakelse

Wysocki, R. K. (2011). *Effective Project Management: Traditional, Agile, Extreme* (6. utg.). John Wiley & Sons.

Yin, R. (2018). *Case study research and applications: Design and methods* . Los Angeles: Sage publishing.

Øyvann, S. (2020, Mai 04). Phishingkampanje mot kommuneansatte og andre på hjemmekontor. *Computerworld*. Hentet fra https://www.cw.no/artikkel/it-sikkerhet/phishingkampanje-mot-kommuneansatte-andre-pa-hjemmekontor

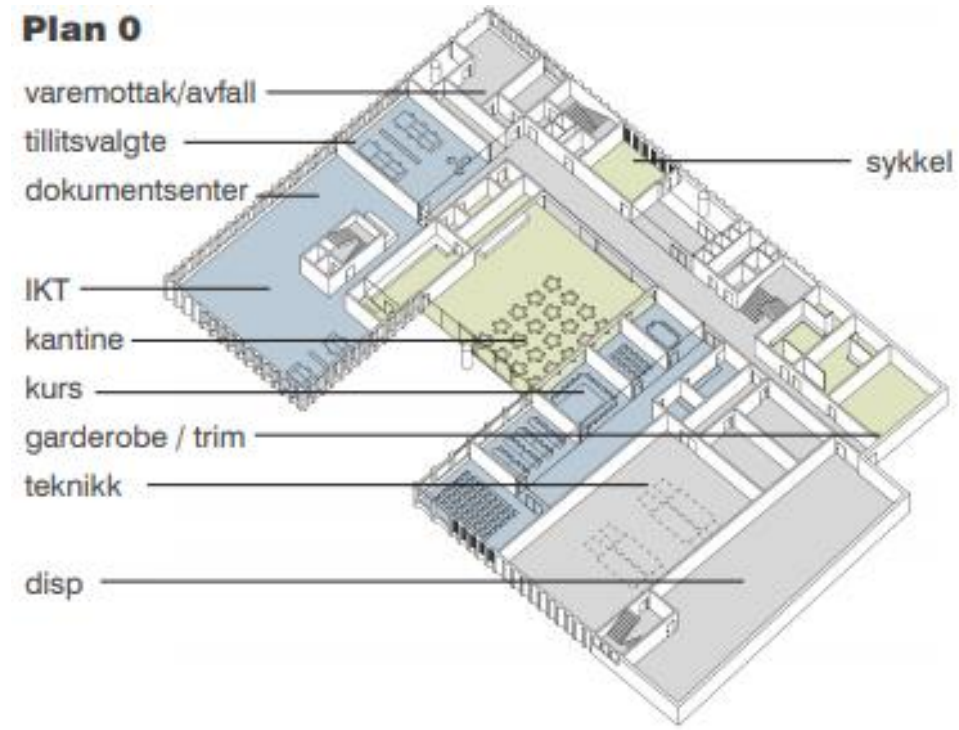
9. Bilde, Tabell- og Figur-liste

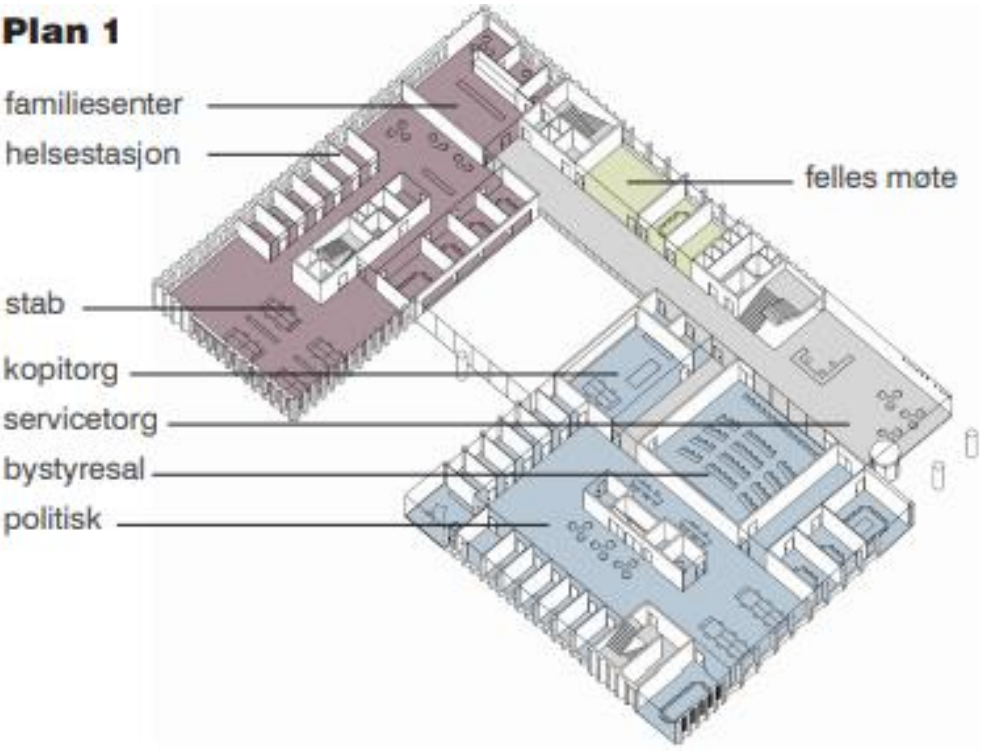
Bilder

Tabeller

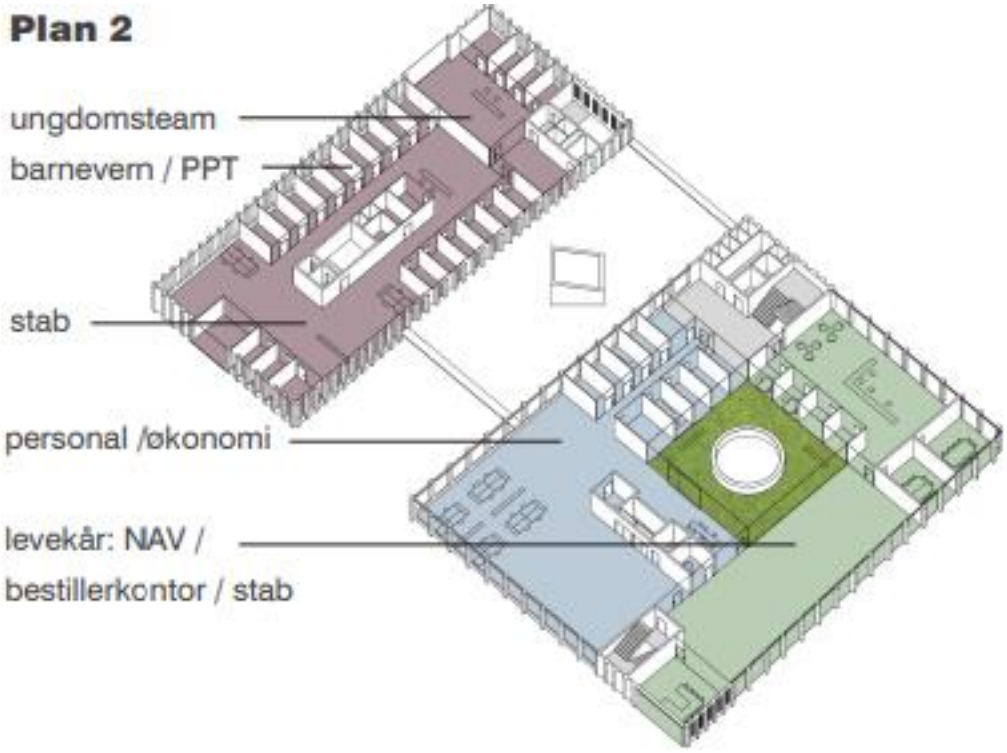
Figurer

Vedlegg 1. Skisseplantegninger

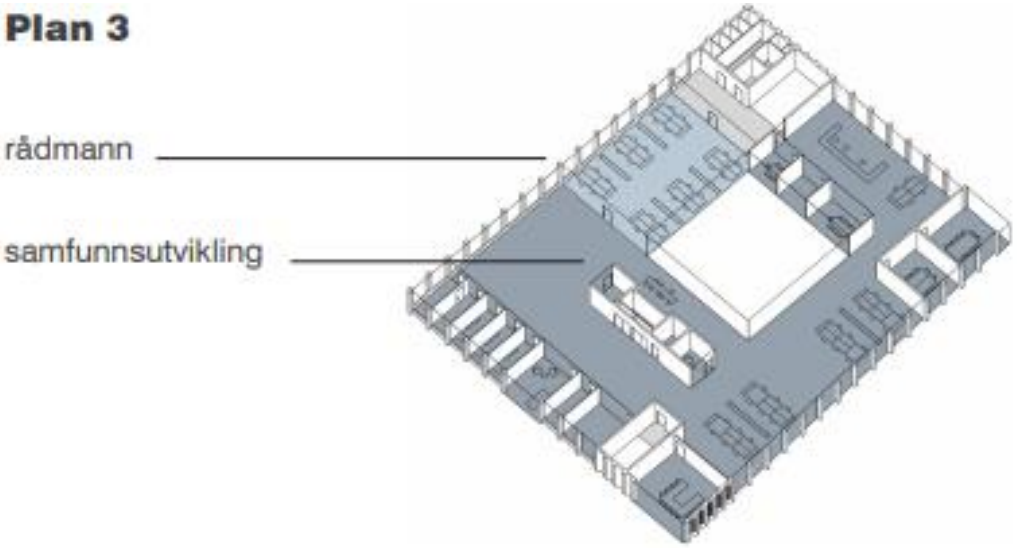




Plan 2


ungdomsteam
barnevern / PPT
stab
personal /økonomi
levekår: NAV /
bestillerkontor / stab

Plan 3


rådmann
samfunnsutvikling

Vedlegg 2. Dokumentanalyse

Tidligere forskning	• Bjørn Melandsø Kjelsaas, iNN, Masteroppgave: *"Modeller for risikoanalyse i Norge"*
Offisielle publiseringer	• Sola kommune, 2020: Informasjonsbrosjyre for det nye rådhuset *"Sola rådhus"* • *Sola kommune, 2020, nettside med info om nytt* rådhus • Sikkerhetsloven, 2019 • Sola kommune, 18. november 2016: *"Reguleringsbestemmelser i tilknytning til detaljplan for 0562 Kommunehus, torg og park"* • Sola kommune, 14. Desember 2016: *"1. gangsbehandling detaljregulering kommunehus, bypark og rådhusplass - Plan 0562"* • Multiconsult, september 2016: *"Formingsveileder for Sola sentrum".* • Sola kommune, 28. Oktober 2016: *"Merknader ved oppstart"* • Sola kommune, 19. november 2015: *"Overordnet beredskapsplan: administrativ del. Versjon 1.0"* • Longva arkitekter, skisseprosjekt, september 2015: *"Solas hjerte: Arkitektkonkurranse om nye Sola rådhus"* • Sola kommune, 14. april 2020: *"Årsrapport 2019 – Et godt år"* • DSB, 2016: "Samfunnets kritiske funksjoner" • NSM, håndbok, mars 2016: *"Risikovurdering for sikring"* • Odd Busmundrud, Maren Maal, Jo Hagness Kiran og Monica Endregard, Forsvarets forskningsinstitutt (FFI), 8. juni 2015: *"Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger"*
Annet	• Planskissene fra Longva Arkitekter, 2015, Plan 0-3
Artikler	• Kjell Arne Knutsen og Pål Christensen, aftenbladet.no, 18. desember 2019: *"Flytter inn i forgylt rådhus i Sola"* • Stein H. Jupskås, aftenbladet.no, 29. oktober 2018: *"Nok er nok inntok bystyresalen"* • Ole Harald Dale, Byggeindustrien (Bygg.no), 12. Februar 2020: *"Sola rådhus"* • Norske arkitekters landsforbund, åpen plan- og designkonkurranse utgivelse nr. 462/2015: *"Nytt Sola rådhus"*
Lover, forskrifter og standarder.	• LOV-2018-06-01-24. Lov om nasjonal sikkerhet (sikkerhetsloven) • LOV-2006-05-19-16. Lov om rett til innsyn i dokument i offentleg verksemnd

	• Norsk standard 5832:2014: *"Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse"*
VTS-analyse (verdivurdering og scenariobeskrivelse)	• LOV-2018-06-15-38. Lov om behandling av personopplysninger (personopplysningsloven) • Kathrine Geard, Fagbladet, 24. januar 2020: *"Ny undersøkelse avslører utstrakt vold: Nær en av tre ansatte i barnevernet har vært utsatt for vold mer enn to ganger de siste to åra"* • Sola Kommune, 5. desember 2019, personvernerklæring • Elin Fossum og Mette F. Børresen, NRK.no, 19. oktober 2013: *"Far angrep barnevernsansatte på Otta"* • Nora E. Hvistendahl, NRK.no, 25. august 2014: *"Dømt til tvungen psykisk helsevern"* • PST, 1. mars 2019: *"Temarapport: Hvilken bakgrunn har personer i høyreekstreme miljøer i Norge?"* • Mari Lande With, Statistisk Sentralbyrå (SSB), 15. august 2017: *"Politiske ressurser og deltakelse"* • Stein H. Jupskås, aftenbladet.no, 29. oktober 2018: *"Nok er nok inntok bystyresalen"* • NTB, VG.no, 17. august 2018: *"Skoleelev varslet om datahull i Bergen"* • Stig Øyvann, Computerworld, 4. mai 2020: *"Phishingkampanje mot kommuneansatte og andre på hjemmekontor"* • Morten Solli, Nettavisen.no, 8. mai 2020: *"Prøver å svindle skoleelever: Teams og Office under angrep"* • Andreas H. Bechensten, Dagsavisen.no, 25. mai 2018: *"Stavanger kommune utbetalte en halv million til svindlere"* • Eirik Husøy, Aftenposten.no, 9. januar 2019: *"PST tror statlig aktør kan ha stått bak cyberangrep mot fylkesmenn"* • NTB, VG.no, 20. mai 2020: *"Bergen kommune vedtar rekordstor bot* på grunn av svikt i appen Vigilo*"* • NAV, 10. desember 2014: *"Minimumsstandard med krav til fysisk utforming og sikring av NAV-kontor".* Dette er et dokument som revideres hvert år, men vi har ikke funnet et nyere dokument som er tilgjengelig • NAV.no og temasiden om *"Sikkerhet i NAV"* • NAV, 31.12.2019: "Vold og trusler mot ansatte i NAV 2019" • Plantegning av Plan 0 "A2-000 – Plan 0 – oversikt" • NSM, 2019: "Risiko 2019. Krafttak for et sikrere Norge" • NSM, PST og POD, 2015: "Terrorsikring: En veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger"
Grovanalyse	• PST, 4. februar 2020: *"Nasjonal trusselvurdering 2020"* • NSM, 17 april 2020: *"Risiko 2020"*

	• Norsk standard 5831:2014: *"Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikostyring"* • Anne Lise Stranden, forskning.no, 19 juni 2018: *"Slik har terrorister siktet seg inn mot myke mål"* • Sigrid Moe, e24, 9 juni 2018: *"Sikkerhetsekspert bekymret for norske kommuner: - skremmende dårlige på IT-sikkerhet"* • Oda Leraan Skjetne, VG.no, 26 september 2017: *"E-tjenesten advarer om russiske aktører: Sabotasje av strøm og infrastruktur"* • Jon Bolstad, Roy Svendsen, Eivind Fondenes, NRK.no, 29 mai 2019: *"Drapstrusler, trafikksabotasje og hærverk: Slik er den skitne siden av bompengeoppgjøret"* • Elin Martinsen, NRK.no, 17 august 2014: *"NAV-ansatte utsettes stadig for vold og trusler"* • Torgeir Krokfjord, Dagbladet.no, 2 januar 2014: *"-Skjøt i taket på NAV-kontoret og holdt NAV-ansatt fanget på kontor"*

Vedlegg 3. VTS-analyse av Sola rådhus

Bakgrunn

Vår analyse ble gjort i etterkant av iverksatte tiltak og ferdigstillelse av bygg. Dette er motsatt i forhold til hvordan analyseverktøyet er tiltenkt, hvor en VTS-analyse gjennomføres før eller fra begynnelsen av et byggeprosjekt. Basert på at vi gjennomfører denne analysen i etterkant av byggeprosjektet vil våre vurderinger og tiltak være basert på eksisterende og iverksatte tiltak. Vi har hatt tilgang på noe dokumentasjon på tiltak og vurderinger som er gjort, i tillegg har vi tatt egne fysiske undersøkelser av bygget fra utsiden. Det vil være interessant å finne ut hvorvidt denne typen analyse kan benyttes i etterkant av at byggeprosjekter er ferdige.

VTS-analysen av sikringsobjektet Sola rådhus gjennomføres for å kunne beskrive risikobildet for objektet basert på dagens trusselnivå. En slik sikringsrisikovurdering vil skildre risiko som knyttes til en uønsket handling. Det vil foreligge et forsett og en vilje bak handlingene, som potensielt kan ramme rådhuset, i denne analysen.

Etter gjennomført analyse vil resultatene av VTS-analysen sammenlignes med resultatene fra grovanalysen av sikringsobjektet for å identifisere styrker og svakheter med analysemodellene.

Definisjoner brukt i VTS-analysen

I tabell 6, under, har vi samlet noen definisjoner som blir brukt i analysen. Det er viktig for oss å definere disse slik at det blir tydeligere hva vi ønsker å få frem.

Spionasje	Målrettet informasjonstyveri der trusselaktøren bruker fordekte metoder (NSM, 2016).
Sabotasje	Skade på data eller infrastruktur, som er målrettet (NSM, 2016).
Terrorhandling	Innebærer bl.a. fare for liv og helse, ødeleggelse av eller alvorlig skade på eiendom, prosesser eller systemer knyttet til demokratisk styre eller samfunnets økonomiske velferd og virkemåte (NSM, 2016).

Annen alvorlig kriminell aktivitet	Inkluderer andre straffbare handlinger som får alvorlige konsekvenser for mennesker, virksomheter eller samfunnet (NSM, 2016).
Hybride trusler	Trusler som benytter flere ulike militære og ikke-militære virkemidler for å oppnå sine mål (definisjon basert på (NSM, E-tjenesten, DSB, PST, 2017). Eksempler på virkemidler er økonomisk og politisk press, skarpe våpen, cyberangrep, falske nyheter, metoder for skremsler og påvirkning (Borch, 2020) .
Scenario	DSB definerer scenario som *"en detaljert og konkretisert beskrivelse av en uønsket hendelse; en beskrivelse av en framtidig tilstand og den serien av handlinger og/eller hendelser som leder dit"* (DSB, 2012a:14) (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 23).

Tabell 6 Begreper og definisjoner relevant for VTS-analysen

Verdivurdering

En VTS-analyse starter med å identifisere verdier. Dette gjøres for å kartlegge konsekvenser av uønskede handlinger. Vi antar det vil være en rekke ulike verdier tilknyttet vårt sikringsobjekt. Identifiserte verdier er valgt på bakgrunn av teori om VTS, inkludert eksempler benyttet i teorien, undergruppens fortolkning av informasjon vedrørende Sola rådhus og prosjektgruppens tidligere erfaring med VTS-analyser.

I FFI-rapporten *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* deles verdier inn i fire kategorier: Liv og helse, operativ evne, sensitiv informasjon og omdømme (Busmundrud, Maal, Kiran, & Endregard, 2015). Vi har valgt å dele opp "operativ evne" i to kategorier, materiell og bygning og operativt tjenestetilbud. Vi mener dette gir et bedre beskrivende verdigrunnlag. I tillegg har vi valgt å ikke ta med verdien omdømme, da dette ikke anses som en relevant verdi for rådhuset, men heller en verdi som kunne være knyttet til Sola kommune som organisasjon.

I verdivurderingen i denne rapporten rangerer vi verdiene ut fra deres kritikalitet. Figur 5, under, benyttes for å rangere verdiene samt å beskrive disse.

Verdi:	Beskrivelse:
Svært høy	Tap eller reduksjon av verdi *har umiddelbare og svært alvorlige konsekvenser*
Høy	Tap eller reduksjon *har store konsekvenser*
Moderat	Tap eller reduksjon av verdi *kan ha* store konsekvenser
Lav	Tap eller reduksjon av verdi *har* små konsekvenser

Figur 4 Tilnærming til risikovurdering for tilsiktede uønskede handlinger. Hentet fra FFI-rapport 2015/00923

Sikringsmålene, som er oppgitt i verdivurderingene er sikringsmål satt av under undergruppen basert på egne vurderinger. Verdiene er vurdert og rangert på de neste sidene og danner grunnlaget for denne VTS-analysen:

Verdi: Liv og helse
Beskrivelse og vurdering: Angår ansatte, folkevalgte og besøkende. Sola kommune har ansvar for liv og helse, sikring og sikkerhet generelt for ansatte og besøkende til rådhuset. De ulike avdelingene som arbeider på Sola rådhus er avhengige av sine ansatte for å kunne utføre sine oppgaver, noe som krever at kommunen ivaretar folk i rådhuset, både i forhold til opplevd og reel sikkerhet. Flere ansatte har samfunnskritiske funksjoner gjennom sitt arbeide.
Rangering av verdien: Svært høy
Sikringsmål: Det aksepteres ikke tap av liv og helse

Verdi: Materiell og bygning
Beskrivelse og vurdering: Angår rådhuset som objekt. Rådhuset er avhengig av å ha arealer, som utfører sitt samfunnsoppdrag, uavhengig om det er saksbehandling eller ivaretagelse av publikum. Kommunen har ansvar for å ivareta og vedlikeholde rådhuset for at det skal kunne benyttes som planlagt og unngå bortfall eller nedetid av tjenester. Rådhusets utforming baserer seg på åpenhet og tilgjengelighet. Dersom bygningen blir ute av drift vil de ulike etatene/avdelingene tvilsomt kunne etablere midlertidige løsninger raskt for å kunne opprettholde sin funksjon.
Rangering av verdien: Moderat
Sikringsmål: Aksepterer ikke store materielle skader utenpå eller inne i bygningen.

Verdi: Operativt tjenestetilbud
Beskrivelse og vurdering: Angår tjenester som barnevernet, PPT, ungdomsteam, servicetorg, familiesenter og helsestasjon. Politisk ledelse, politisk sekretariat, folkevalgte og kommunestyret. Det er en verdi for Sola Rådhus og kunne opprettholde operativt tjenestetilbud, som en del av samfunnets kritiske funksjoner til enhver tid. Eksempel er NAV, en statlig etat med lokalt kontor lokalisert på rådhuset. Kommunen har ansvar for å ivareta at tjenestetilbudet er operativt. Dette inkluderer evne til å forhindre/begrense bortfall eller nedetid. Spesielt tjenestetilbud som barnevern, PPT og deler av NAV kan beskrives som kritiske samfunnsfunksjoner med et tjenestetilbud som retter seg mot spesielt sårbare grupper i samfunnet. NAV er en statlig etat og sikkerhet og tilrettelegging koordineres mellom Arbeids- og velferdsdirektoratet og KS. NAV-kontoret er selv ansvarlig for å ta i bruk og operasjonalisere tiltak utenom de tiltakene som standardiseres for hele bygget.
Rangering av verdien: Høy
Sikringsmål: Aksepterer ikke brudd på skjerming av barn og ungdom, samt nedetid av behandlingstilbud for sårbare og utsatte grupper som benytter tjenestene. Aksepterer ikke brudd på eller forhindring av demokratiet.

Verdi: Sensitiv informasjon
Beskrivelse og vurdering: Angår IKT, IT, personvern, datalagring og teknisk infrastruktur. Kommunen og kommunens tjenestetilbud har ansvar for å ivareta publikum/besøkende og ansattes personvern. Kommunen benytter brannmurer og kontrollerer hvem som har tilgang på bygningene for å beskytte personvern, i tillegg til tekniske sikkerhetssystemer. Det er uklart om kommunen lagrer data sentralt på en server i bygget eller eksternt på servere på andre lokasjoner. Vi antar at NAV benytter egne systemer for databehandling enn resten av kommunens tjenestetilbud. Behandling av personopplysninger i kommunen er underlagt personopplysningsloven. Det er kommunedirektøren som er øverste ansvarlige for behandling av personopplysninger i kommunen.

I Sola kommunes personvernerklæring står det at *"Sola kommune samler inn og behandler personopplysninger for å være i stand til å utføre lovpålagte oppgaver, andre ytelser og for å kunne saksbehandle henvendelser. Vi har også ansvar for å følge opp og kontrollere tjenester, ytelser og utbetalinger. Når vi behandler personopplysningene, betyr det at vi samler inn opplysningene, registrerer dem, setter dem sammen, lagrer eller utleverer dem. […] Vi har tekniske sikkerhetsløsninger som skal sikre at: uvedkommende ikke får tilgang til dine opplysninger, opplysningene ikke kan endres eller manipuleres, opplysningene om deg er tilgjengelige ved behov. Alle opplysninger som overføres mellom din datamaskin og vår server foregår over sikker kryptert linje (SSL). Løsningen tilsvarer sikkerheten som er brukt i nettbankene".*
Rangering av verdien: Svært høy
Sikringsmål: Aksepterer ikke at personvernsopplysninger kommer på avveie, at kommunikasjonssystemer faller bort og forhindrer kritiske samfunnsfunksjoner, cyber angrep eller trusselaktører som truer demokratiet.

Trusselvurdering

En trusselvurdering beskriver det aktuelle trusselbildet for det som ønskes beskyttet, og gir en vurdering av hvordan trusselbildet kan utvikle seg. Det ses *"på reelle og potensielle trusselaktørers intensjon om og kapasitet til å ramme virksomheten"* (NSM; POD; PST, 2015, s. 17). Hovedhensikten med å utarbeide en trusselvurdering er å identifisere trusselaktørenes kapasitet og handlingsmønster for å kunne utarbeide gode trusselscenarioer og korrekt dimensjonere sikringstiltak. På grunn av begrensninger i tilgang på relevant informasjon og begrenset kapasitet er det knyttet usikkerhet til deler av denne vurderingen.

Følgende trusselaktører som eventuelt kan være ute etter de identifiserte verdiene er:

- Fremmede makter
- Organiserte kriminelle
- Person eller gruppe med intensjon om å utføre en kriminell handling
- Intern utro tjener
- Person eller gruppe med intensjon om å utføre en terrorhandling
- Aksjonsgrupper

I NSM, PST og POD sin veileder *Terrorsikring: En veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger* (NSM; POD; PST, 2015, s. 17) fremkommer det at relevante faktorer som danner trusselvurderingen kan være:

- Tilstedeværelse (Er det noen aktører i dette område som er etablert?)
- Kapasitet (Er aktører til stede i stand til/har evne til å gjøre det?)
- Intensjon (Har aktører vilje (herunder uttalt eller antatt ønske) til å gjøre det?)
- Historie (Har det skjedd tidligere mot egen eller lignende virksomheter?)
- Målvalg (Er det noe som tyder på at det kan skje snart? Har trussel aktøren valgt ut verdier som et direkte eller indirekte mål ("sannsynlighet")).

I trusselvurderingen benyttes skalaen for trusselvurdering (vedlegg 4), denne skalaen er vår tolkning av NS5830:2012 og Standardiserte sannsynlighetsord hentet fra (Njå, Sommer, Rake, & Braut, 2020, s. 212). Skalaen har dermed en direkte sammenheng mellom skalaen for verdivurdering. Hendelsene vi ønsker å se på i dette overordnede perspektivet er noe vi som samfunn har grunn til å forvente at vil skje. Det er lite hensiktsmessig å angi sannsynlighet i form av tallmessige estimater, derfor vil vi beskrive i hvilken grad vi kan ha "grunn til å forvente" at en hendelse vil skje. Trusler kan f.eks. være spionasje, sabotasje eller annen kriminalitet.

Følgende trusler og trusselaktører er vurdert og rangert:

Trusselaktør:	**Fremmede makter**			
A) Tilstedeværelse	B) Intensjon	C) Kapasitet	D) Historie	E) Målvalg
X	**-**	**x**	**-**	**-**
Vurdering: A) Det kan argumenteres for at fremmede makter som Russland og Kina er til stede. Dette gjelder både når det gjelder fysisk tilstedeværelse i Norge og at de er til stede på internett. Det siste er spesielt relevant for eventuelle operasjoner som kan gjennomføres mot IKT systemer. Mange av avdelingene i Rådhuset har systemer som er koblet til internett. B) Det kan argumenteres for at ulike fremmede makter, som for eksempel Russland og Kina, kan ha en intensjon om å ramme verdier direkte eller indirekte. I NSMs rapport, Krafttak for et sikrere Norge fra 2019, oppgis at offentlige virksomheter som forvalter eller støtter bl.a. kritisk infrastruktur, nasjonale funksjoner, eller høyteknologi kan være et				

potensielt mål for fremmede makters etterretning. For Sola Rådhus har vi for denne vurderingen ingen tilgjengelig informasjon som støtter opp under dette.

C) Det er godt dokumentert at fremmede makter, som blant annet Russland og Kina, har store ressurser og kapasitet til å gjennomføre angrep på blant annet politiske verdier. Med denne typen aktør snakker man om det høyeste nivået av kapasitet. Det er godt dokumentert at fremmede makter som Russland og Kina har gjennomført og gjennomfører operasjoner og angrep over internett regelmessig.

D) Det foreligger ikke historie på at fremmede makter har forsøkt å infiltrere, sabotere eller utøve spionasje etater som har tilholdssted i Sola Rådhus

E) Det er ikke ny og pålitelig informasjon, som indikerer forberedelse av et angrep (forestående angrep).

Indikatorene A og C er til stede – Til tross for at det ikke foreligger informasjon direkte knyttet til intensjon og Sola rådhus vurderes trusselen som:

MODERAT

Trusselaktør:	**Person eller gruppe med intensjon om å utføre en kriminell handling**			
A) Tilstedeværelse	B) Intensjon	C) Kapasitet	D) Historie	E) Målvalg
x	**x**	**x**	**x**	**x**

Vurdering:

A) Det kan argumenteres for at aktører er til stede i nærmiljøet. Det kan være seg personer tilhørende sårbare grupper som benytter kommunens eller NAVs tjenestetilbud, eller har et hevnmotiv.

B) Videre kan det foreligge en intensjon, altså vilje og ønske, at aktører enten vil forhindre eller påvirke ansatte, publikum/brukere av tjenestetilbudet. Eller det foreligger en intensjon om å påvirke saksbehandling eller uttrykke misnøye.

C) Videre kan det argumenteres for at aktører har kapasitet og tilgang på nødvendige ressurser.

D) Det foreligger historikk på gjentatte angrep og drap på saksbehandlere innen barnevern og NAV. I rapporten Vold og trusler mot ansatte i NAV 2019 oppgis det at det har vært en nedgang i ansatte som er utsatt for trusler i møte med bruker med ca. 30 % i 2018.

E) Det er ikke ny og pålitelig informasjon, som indikerer forberedelse av et angrep (forestående angrep). Vi kan derimot ved å basere oss på historiske data anta at dette er noe som skjer raskt og spontant. Det er derfor svært sannsynlig at dette vil skje en gang i fremtiden.

Indikatorene A,B,C,D,E er til stede - På bakgrunn av indikatorene vurderes trusselen som:

SVÆRT HØY

Trusselaktør:	**Person eller gruppe med intensjon om å utføre en terrorhandling**			
A) Tilstedeværelse	B) Intensjon	C) Kapasitet	D) Historie	E) Målvalg
x	**-**	**x**	**-**	**-**

Vurdering:

A) Det kan argumenteres for at det eksisterer aktører til stede i regionen. Det er vanskelig å argumentere videre for tilstedeværelse annet enn at man kan anta de eksisterer. PST har derimot uttalt at medlemmer av høyreekstreme miljøer i hovedsak har tilhold på Østlandet og det er en betydelig overvekt av menn. Dette kan være med på å redusere grad av tilstedeværelse i Sola og i regionen, men det er viktig å ikke utelukke at majoriteten er spredd utover i landet og derfor kan ha tilhold der. PST sin analyse av høyreekstreme miljøer i Norge viser at over halvparten står utenfor arbeidslivet. Vi kan anta at arbeidsledige har en naturlig tilknytning til NAV sine tjenester og derav vil en radikalisert person eller gruppe kunne ha tilknytning til NAV sine tjenester lokalisert på Sola rådhus.

B) Videre kan det foreligge en intensjon, altså vilje eller ønske, fra aktører drevet av religion eller ideologi som vil forhindre demokratisk utførelse eller påvirke partipolitikk. Vi har ingen dokumentasjon som foreligger som støtter opp om at Sola Rådhus er et potensielt mål for en slik handling.

C) Videre kan det argumenteres for at aktører har kapasitet og tilgang på nødvendige ressurser. Terrorhandlinger er i tillegg vanskelige å forutse.

D) Det foreligger historikk over terrorhandlinger mot offentlige bygninger som er kategorisert som kritisk infrastruktur og mot demokratiet. Utført av personer med høyreekstreme holdninger. Eksempel på dette er 22. juli hvor det var angrep på regjeringskvartalet og Utøya. Eksemplet viser til handling der terror kan utføres av enkeltpersoner. Det foreligger derimot ingen historikk av lignende trusselaktør har gjort lignende handlinger mot Sola rådhus.

E) Det er ikke ny og pålitelig informasjon som indikerer forberedelse av et angrep (forestående angrep). Basert på trusselvurderingene fra PST og NSM kan det derimot ikke utelukkes at høyreekstreme personer eller grupper kan prøve å gjennomføre terrorhandlinger.

Indikatorene A,C er til stede – På bakgrunn av indikatorene over vurderes trusselen som:

MODERAT

Trusselaktør:	**Aksjonsgrupper**			
A) Tilstedeværelse	B) Intensjon	C) Kapasitet	D) Historie	E) Målvalg
x	**x**	**x**	**x**	**-**

Vurdering:

A) Det kan argumenteres for at aktører er til stede i nærmiljøet eller regionen. Hver tiende person i den norske befolkningen over 16 år har forsøkt å påvirke en sak gjennom innsats for et politisk parti, en organisasjon eller en aksjonsgruppe. Slike aksjonsgrupper finnes i nærmiljøet og går under betegnelsene folkeaksjoner eller folkeopprør.

B) Videre kan det argumenteres for at aktøren har kapasitet og tilgang på nødvendige ressurser. Det opprettes grupper på sosiale medier hvor meningsfeller samles raskt og det blir enklere å spre sitt budskap. Dette gjør at de får et stort nettverk og meningsfellene støtter opp med ulik grad av ressurser.

C) Videre kan det foreligge en intensjon, altså vilje og ønske, at aktøren enten forhindrer eller påvirker demokratiske prosesser som et mål for å oppnå medhold i sine politiske meninger. Det kan videre handle om å sabotere drift som en del av et større mål for å lage et poeng i favør for sin politiske sak.

Aksjonsgrupper samler aktører med ulik bakgrunn som enes om samme sak, som nevnt kan dette bety at aktørene har ulik grad av ressurser som kan benyttes og ulik grad av vilje og ønske for å benytte disse ressursene.

D) Det foreligger historikk på at aktører har forhindret demokratisk utførelse tidligere. I 2018 inntok rundt femti demonstranter fra aksjonsgruppen Nok-er-Nok bystyresalen i Stavanger kommune og kuppet bystyremøtet ved å nekte å forlate talestolen. Kuppet ble begrunnet med at de trengte en ny aksjonsform som var mer effektiv.

E) Det er ikke ny og pålitelig informasjon som indikerer forberedelse av et angrep (forestående angrep).

Indikatorene A,B,C,D er til stede – På bakgrunn av indikatorene over vurderes trusselen som:

Høy

Trusselaktør:	**Fremmede makter/Organiserte kriminelle**			
A) Tilstedeværelse	B) Intensjon	C) Kapasitet	D) Historie	E) Målvalg
x	**x**	**x**	**x**	**-**

Vurdering:

A) Det kan argumenteres for at det muligens finnes enkelte aktører til stede i regionen eller nasjonalt, som vil kunne ramme kommunens eller NAVs systemer, da hovedsakelig digitalt gjennom cyberangrep. NSM trakk særlig frem cyberangrep som ny trend i risikobildet for Norge fra årene 2016 og frem til nå, herunder at ressurskrevende saker fra kompliserte trusselaktørene økte i omfang og at aktørene angriper sårbare IKT-systemer i mindre virksomheter. Imidlertid er det ikke kjent at det er trusselaktører til stede som vil ramme Sola rådhus spesielt, men muligheten er til stede.

B) Det kan argumenteres for at det er aktører som har vilje og ønske om Cyber angrep/phishing for å få tilgang på informasjon i kommunens eller NAVs datasystemer.

C) Videre kan det argumenteres for at aktører som først bestemme seg for å gjennomføre et angrep vil ha kapasitet, samt tilgang på nødvendige ressurser.

D) Det er noe historikk på cyberangrep på kommuner og fylkeskommuner. I 2018 klarte en 13-åring å hacke seg inn på et datasystem, som ble brukt av kommunen. Personen varslet så om sikkerhetsbruddet. Det er også eksempler på phising-kampanjer mot kommuner, og PST etterforsket i 2019 cyberangrep på flere Fylkesmenn romjulen 2018. Bergen kommune har nylig vedtatt en bot på 3 millioner kroner etter at det var svikt i skoleappen Vigilo som gjorde at personopplysninger var tilgjengelig. E) Det er ikke ny og pålitelig informasjon som indikerer forberedelse av et angrep (forestående angrep). **Indikatorene A,B,C,D er til stede. På bakgrunn av indikatorene over vurderes trusselen som:**
HØY

Valg av scenarioer og scenariobeskrivelser

Med scenariobeskrivelsene er hensikten å belyse sårbarheter som er relevante for analysen. I scenariobeskrivelsene tar vi utgangspunkt i at alle inngår i trusselkategorien security og ser på måter trusselaktørene kan oppnå sine mål og skade de identifiserte verdiene. De ulike scenarioene vil avdekke ulike sårbarheter som alle tar med videre i analysen. Med bakgrunn i verdivurderingen og trusselvurderingen er følgende scenarioer valgt:

Scenario	Beskrivelse
1	Knivangrep mot en NAV-ansatt
2	Datainnbrudd
3	Forsøk på å sabotere en pågående politisk sak i kommunen
4	En person utfører et terroranslag mot rådhuset

Tabell 7 Valg av scenario

Scenariobeskrivelsene skal belyse følgende faktorer:

- Hendelsesforløp: Hva inntreffer, når inntreffer det, hvor inntreffer det, hvordan inntreffer det
- Kapasitet og intensjon til trusselaktøren(e)
- Hvordan rammes verdiene (f.eks. datainnbrudd, bilbombe, tyveri, m.m.).
- Andre verdier som indirekte rammes (f.eks. liv og helse, miljø, økonomi eller omdømme)
- Er hendelsen varslet i forkant (f.eks. fra terrororganisasjoner, etterretning og politiet).
- Tidspunktet for når trusselen rammer (f.eks. når på døgnet eller året, under en tilstelning eller lignende)
- Varigheten på hendelsen

Følgende scenario er på de neste sidene skissert for Sola rådhus:

Scenario:	Berørte verdier:	Trusselaktør:
Nr. 1	Liv og helse	Person med intensjon om kriminell handling
Scenariotittel:	Knivangrep mot en NAV-ansatt	
Scenario-beskrivelse:	En enkeltperson er fortvilet, da vedkommende finner seg i en vanskelig livssituasjon. Ut fra desperasjon vil vedkommende ha både intensjon og evne til skade en eller flere ansatte i NAV. En person (heretter kalt bruker) tar seg inn i NAVs lokaler i Sola rådhus med den hensikt å skade en saksbehandler hos NAV. Det har over en lengre periode vært en konflikt med brukeren og en navngitt ansatt på NAV. Brukeren bærer en kniv, som er skjult, og den aktuelle saksbehandler og brukeren oppholder seg alene på eget samtalerom. Den ansatte har ikke mottatt opplæring i rutiner for håndtering av samtaler med brukere som kan ha truende eller voldelig atferd, og blir i løpet av møtet muntlig og fysisk truet. Den ansatte er plassert nærmest døren til samtalerommet (døren går innover i rommet), da brukeren går til angrep med kniv. Den ansatte får et snitt i øvre del av venstre skulder. Hendelsen skjer like etter lunsj på et tidspunkt med stor aktivitet i området, og hendelsen blir raskt oppdaget av forbipasserende kollegaer. Kollegaene går imellom og får kontroll på situasjonen kort tid etter at hendelsen inntraff. Hendelsen blir umiddelbart varslet til politi. Politiet og Arbeidstilsynet starter etterforskning/granskning av hendelsen, og NAV igangsetter intern granskning.	

Scenario:	Berørte verdier:	Trusselaktør:
Nr. 2	Sensitiv informasjon	Fremmede makter/organiserte kriminelle
Scenariotittel:	Dataangrep mot kommunens IT-systemer	
Scenario-beskrivelse:	Et organisert nettverk som har spesialisert seg på cyberkriminalitet hacker seg inn i kommunens database. De har sendt en spear phishing-email med et vedlegg til et utvalg ansatte i kommunen. Det er nok at én ansatt åpner vedlegget for at den skadelige programvaren skal infiltrere datasystemene. En fredag ettermiddag åpner en eller flere ansatte mailen og det vedlagte infiserte dokumentet. Mens kommunens ansatte har helg og få ressurser er på jobb har hackerne benyttet anledningen til å infiltrere datasystemene. Målet er å hente ut sensitiv informasjon fra kommunens databaser og bruke infrastrukturen for å nå andre mål. Spear phishing-angrep benyttes for å innhente sensitiv informasjon som brukernavn, passord, kredittkortinformasjon eller finansiell informasjon. Ingen av kommunens ansatte som mottok mailen fikk noen mistanke om hva det faktisk var. Mailene kommer seg derfor forbi brannmuren og unngår sikringstiltakene i kommunens IT-systemer. Det tar lang tid før kommunens IT-systemer plukker opp at noe er galt og varsler om dette. Kommen igangsetter en større intern granskning og gjennomgang av rutinene. Det viser seg at kommunen har sårbare IKT-systemer og manglende tiltak for å kunne plukke opp tilsiktede uønskede hendelser som dette. Hendelsen krever en større etterforskning og PST vil derfor stå bak kartleggingen av dataangrepet. Omfanget og kostnaden er uklar.	

Scenario	Berørte verdier:	Trusselaktør:
Nr. 3	Materiell og bygning Operativt tjenestetilbud	Aksjonsgruppe
Scenariotittel:	Forsøk på å sabotere en pågående politisk sak i kommunen	
Scenario-beskrivelse:	En aktivistgruppe har over en periode varslet Sola rådhus sitt servicetorg at de vil aksjonere i forbindelse med en pågående politisk sak. Truslene har ikke blitt sett på som reelle. 10 aktivister klarer å ta seg ubemerket inn i Sola rådhus ved å utgi seg for å være vanlig publikum og besøkende. De har entret rådhuset via hoveddøren, og fulgt en nøye planlagt plan for videre bevegelser inn i bygget. Aktivistene har båret ID-kort tilnærmet like de som ansatte i rådhuset benytter og har ikke blitt stoppet av ansatte i bygget. Aktivistene har fått tilgang over plantegninger av bygget via enkelt søk på internett. Innsyn i rådmannen i Sola sin kalender og informasjon om arbeidstider, vaktskifte har aktivistene fått gjennom flere ulike henvendelser til servicetorg og andre medarbeidere fra Sola Rådhus På bakgrunn av dette klarer tre av aksjonistene å storme et planlagt avdelingsmøte ledet av rådmannen i Sola som en avledningsmanøver. De resterende 7 aksjonistene beveger seg systematisk inn i de ulike kontorene og ødelegger papirer som ligger fremme, pc utstyr og utfører hærverk i form av tagging med medbrakte spraybokser. Før politiet rekker å ankomme rådhuset har aktivistene klart å forlate rådhuset.	

Scenario	Berørte verdier:	Trusselaktør:
Nr. 4	Liv og helse Materiell og bygning Operativt tjenestetilbud	Person eller gruppe med intensjon om å utføre en terrorhandling
Scenariotittel:	En person utfører et terroranslag mot rådhuset	
Scenario-beskrivelse:	Det er et stort arrangement på rådhuset på dagtid med innbyggere, ansatte og folkevalgte fra hele regionen som er på besøk. Rådhusets selskapslokaler er fylt med mennesker, parkeringsplassen er full av biler. En person tilknyttet et høyreekstremt terrornettverk ankommer rådhuset etter alle andre, h*n har en ryggsekk med seg som inneholder en bombe. H*n går langs bygningen og kaster sekken fra seg på utsiden inntil veggen mot selskapslokalet og går vekk for å få rådhuset på avstand. Deretter ringer h*n et mobilnummer som gjør at bomben aktiveres og går av. Det blir omfattende tap av liv og mange får alvorlige skader. Det blir store skader på bygning og materiell. Kommunens kriseledelse var alle til stede på arrangementet og er nå i episenteret av angrepet. Det operative tjenestetilbudet får en lang nedetid og kommuneledelsen er satt ut av drift. Personen hadde tidligere på dagen postet høyreekstreme meningen knyttet til anledningen for arrangementet på sosiale medier. Dessverre var ikke dette plukket opp av de riktige kanalene i forkant.	

Sårbarhetsvurdering

I vurderingen ses det på om det er mulig for en trusselaktør å gjennomføre en uønsket handling uten å bli stoppet. Vil eksisterende sikringstiltak kunne forhindre eller påvirke de beskrevne scenarioene som vi illustrerte tidligere i analysen? Her ser vi nærmere på hvordan eksisterende tiltak, eller mangel på tiltak, kan påvirke hendelsene skissert i de forskjellige scenarioene.

Følgende er sårbarhetsvurderingene for de ovennevnte fire scenarioene:

Scenario 1		**Knivangrep mot en NAV-ansatt**						
Teknologiske tiltak			**Organisatoriske tiltak**			**Menneskelige tiltak**		
Fysisk sikring	*Elektronisk sikring*	*Logisk sikring*	*Administrasjon og ledelse*	*Analyse*	*Verifikasjon*	*Biologiske tiltak*	*Kognitive tiltak*	*Sosiale tiltak*
M	**IR**	**IR**	**M**	**M**	**IT**	**X**	**X**	**X**
Nøkkel: M = Mangelfull. X = Til stede. IR = Ikke relevant IV= Ikke vurdert IT = Ikke tilgjengelig informasjon								

Vurdering: Verdien i dette scenarioet er liv og helse. Verdien vurderes som svært høy med bakgrunn i skadeomfang.

Fysisk sikring: NAV, som statlig etat, har ansvar for å innføre ytterligere sikringstiltak på sine kontorer. NAV i samarbeid med KS har utarbeidet minimumskrav til fysisk sikring av NAV-kontor. Disse inkluderer at adgangspartiet er utformet slik at de ansatte og brukerne får en sikker ankomst til kontorene. Hoveddøren skal kunne låses manuelt fra innsiden. Indre områder for de ansatte skal være låst. For publikumsmottak gjelder at det skal være ryddig og oversiktlig, og blindsoner skal om mulig ikke være til stede. I dette området skal det være alarmeringsmuligheter slik at man kan påkalle hjelp. I tillegg skal det være rømningsveier her. Det skal være mulig å foreta tilfredsstillende evakuering av områdene. Løse gjenstander skal begrenses, og utformingen av inventar og ledninger skal være slik at de de ikke kan kastes rundt, eventuelt være festet. For samtale og møterom gjelder at det skal være ryddig og oversiktlig, herunder gjelder at løse gjenstander skal unngås, ledninger og inventar skal enten være fastmontert eller utformet på en slik måte at de ikke kan benyttes som våpen, innredningen skal kunne utgjøre en barriere mellom saksbehandler og bruker. Døren skal ikke kunne låses fra innsiden. I tillegg er det krav til alarmeringsmuligheter for å tilkalle hjelp, egen rømningsvei skal være tilgjengelig og det skal være innsyn inn i rommene. Indre områder skal fortrinnsvis ikke brukes til brukeroppfølging, og tiltak i disse områdene beskrives ikke nærmere her.

Personalinngangen, der dette er en egen inngang, skal være låst og kun benyttes av personale med id. Samtalerommene er samlet langs en kommunikasjonsåre, som gjør at disse rommene er lett tilgjengelig for alle ansatte og publikum, og er plassert i et område der det er stor sannsynlighet for at det er andre folk til stede ved behov for hjelp. Møterom og kontorlokaler har ikke dører med lås og innredningen skal lage en fysisk barriere mellom bruker og saksbehandler.

Administrasjon og ledelse: Analysen avdekker at det er manglende opplæring av ansatte, noe som gjør de ansatte sårbare for slike angrep.

Analyse: Det er ikke kjent at det tidligere er gjennomført sikringsrisikoanalyse for tilsvarende eller lignende scenario. Imidlertid er dette å anta er ivaretatt med referanse til standardkrav til årlig risikovurdering gitt i Minimumsstandard med krav til fysisk utforming og sikring av NAV-kontorer. Vi vet at NAV fører statistikk over hendelser mellom brukere og ansatte.

Verifikasjon: Vi har ikke informasjon om det er utført øvelser på lignende scenario.

Biologiske forhold: Det legges til grunn at hensyn til arbeidsforhold, hvile, fysisk tilstand og stresstoleranse med mer er regulert.

Kognitive tiltak: Det legges til grunn at den ansatte har en normal situasjons- og sikkerhetsforståelse med tanke på håndtering av slike situasjoner. Scenario tilsier at den ansatte ikke følger rutinene ved å la brukeren være alene i samtalerommet. NAV har utarbeidet en egen nettside for ansatte hvor rutiner, prosesser, tiltak etc. kommuniserer ut og er tilgjengelig til enhver tid.

Sosiale: Det legges til grunn at ansatte er profesjonelle, har en forståelse av viktigheten av sikker jobbatferd og sikkerhetsmessig forberedelse til slike typer møter, og at det er høy grad av konformitet blant ansatte.

På bakgrunn av dette er analysens vurdering: Det er mangel på opplæring og gode rutiner.

Vurderingen av sårbarhet: Sårbarheten vurderes som **moderat.**

Scenario 2		Dataangrep mot kommunens IT-systemer						
Teknologiske tiltak			**Organisatoriske tiltak**			**Menneskelige tiltak**		
Fysisk sikring	*Elektronisk sikring*	*Logisk sikring*	*Administrasjon og ledelse*	*Analyse*	*Verifikasjon*	*Biologiske tiltak*	*Kognitive tiltak*	*Sosiale tiltak*
IR	**IR**	**X**	**M**	**M**	**IT**	**IR**	**M**	**M**
Nøkkel: M = Mangelfull. X = Til stede. IR = Ikke relevant IV= Ikke vurdert IT = Ikke tilgjengelig informasjon								

Vurdering: Verdien i dette scenarioet er sensitiv informasjon. Verdien vurderes som svært høy med bakgrunn i skadeomfang.

Logisk sikring: Avbruddsfri strømforsyning hindrer at strømmen uteblir i lengre perioder noe som sørger for mindre sårbare systemer. Det fremkommer av dokumentasjon at kommunens IKT-avdeling jobber kontinuerlig med vedlikehold og forsterkning av infrastruktur. Man kan derfor anta at det føres jevnlig kontroll og oppdateringer av systemer. Det er anskaffet programvare for robotteknologi som skal gjøre det mulig å automatisere og robotisere oppgaver, dette setter større krav til opplæring i evne til å håndtere nye systemer. Derimot oppdager og varsler robotteknologien automatisk om feil og avvik. Vi antar at brannmurer og virusprogram integrert i epost-systemet er til stede, men epostene har sluppet igjennom disse, de er derfor ikke sikre nok. Vi har ikke informasjon om kommunen har sikkerhetsovervåkningssystemer (IDS).

Administrasjon og ledelse: Personopplysningsloven setter føringer for oppfølging. IKT-avdelingen til kommunen har tilholdssted på rådhuset og dermed nærhet til systemene. Kommunen har eget personvernombud (PVO) som håndterer avvik, men kommunen selv påpeker at PVO må involveres tidligere i prosesser og prosjekter for å ha en mer proaktiv rolle. Kommunen har vedtatt en digital strategi.

Analyse: Det er mangel på risikoanalyser som tar for seg kommunens IT-systemer etter at kommunen fikk nytt rådhus, ei heller er det tilgjengelig informasjon om analyser av slike scenario.

Verifikasjon: Vi har ikke informasjon om det er utført øvelser på lignende scenario.

Kognitive tiltak: Det er gjennomført kurs i informasjonssikkerhet og personvern. Vi antar likevel at det med nye teknologiske løsninger vil være krevende å sørge for at alle ansatte får nødvendig opplæring i håndtering av disse. Det er store digitaliseringstiltak og vi kan anta at i takt med dette øker behovet for klare rutiner og prosesser. Nye systemer åpner opp for menneskelige feil ved mangel på opplæring og oppfølgning.

Sosiale tiltak: Det legges til grunn at ansatte ikke har vært årvåkne, at det er mangel på forståelse av datasikkerhet for å sikre en trygg arbeidshverdag. Dette er viktig for å sikre høy grad av konformitet blant ansatte.

På bakgrunn av dette er analysens vurdering: At det er teknologiske tiltak som logisk sikring til stede, men det antas at det er mangel på sosiale tiltak som sikrer reell evne og bevissthet hos de ansatte om hvordan være bevisst over og håndtere sikringstiltakene. Eposten har sluppet igjennom brannmuren.

Vurderingen av sårbarhet vurderes som: Sårbarheten vurderes som **moderat.**

Scenario 3		**Forsøk på å sabotere en pågående politisk sak i kommunen**						
Teknologiske tiltak			**Organisatoriske tiltak**			**Menneskelige tiltak**		
Fysisk sikring	*Elektronisk sikring*	*Logisk sikring*	*Administrasjon og ledelse*	*Analyse*	*Verifikasjon*	*Biologiske tiltak*	*Kognitive tiltak*	*Sosiale tiltak*
M	**IV**	**IR**	**M**	**IT**	**IT**	**X**	**IV**	**X**
Nøkkel: M = Mangelfull. X = Til stede. IR = Ikke relevant IV= Ikke vurdert IT = Ikke tilgjengelig informasjon								

Vurdering: Verdiene i dette scenarioet er operativt tjenestetilbud samt materiell og bygning. Verdien operativt tjenestetilbud vurderes som høy, mens materiell og bygning vurderes som moderat med bakgrunn i skadeomfang. Totalt settes summen av verdi til høy da operativt tjenestetilbud veier tyngre i denne sammenhengen.

Fysisk sikring: Når aktivistene først var innenfor skallet er det lett å ta seg videre. Det er kodelås på møterommene, men det er uvisst om rommene låses automatisk når de er i bruk.

Elektronisk sikring: I dette tilfellet er elektronisk sikring ikke vurdert.

Administrasjon og ledelse: Informasjon om møtekalender og deltagelse er lett å hente ut, og rutiner og prosesser om rådhuset er tilgjengelig.

Analyse: Vi har ikke informasjon om det foreligger analyser av lignende scenario.

Verifikasjon: Vi har ikke informasjon om det er utført øvelser på lignende scenario.

Biologiske forhold: Det legges til grunn at hensyn til arbeidsforhold, hvile, fysisk tilstand og stresstoleranse mm er regulert.

Sosiale: Det legges til grunn at ansatte er profesjonelle, har en forståelse av viktigheten av sikker jobbatferd og sikkerhetsmessig forberedelse til slike typer møter, og at det er høy grad av konformitet blant ansatte.

På bakgrunn av dette er analysens vurdering: Funn tilsier at det er mangel på fysisk sikring og elektronisk sikring som hindrer uautorisert adgang. Beskrivelser av rutiner og prosesser til tilgjengelig, men det er mangel på risikoanalyser som angår objektet. Vi kan derfor anta at det er mangel på sosiale tiltak for å sikre reell evne hos de ansatte til å benytte de sikringstiltakene og prosessene som er tilgjengelige ved et slikt scenario.

Vurderingen av sårbarhet vurderes som: Sårbarheten vurderes som **høy** basert på

Scenario 4		**En person utfører et terroranslag mot rådhuset**						
Teknologiske tiltak			**Organisatoriske tiltak**			**Menneskelige tiltak**		
Fysisk sikring	*Elektronisk sikring*	*Logisk sikring*	*Administrasjon og ledelse*	*Analyse*	*Verifikasjon*	*Biologiske tiltak*	*Kognitive tiltak*	*Sosiale tiltak*
M	**X**	**IR**	**M**	**M**	**IT**	**IV**	**IV**	**X**
Nøkkel: M = Mangelfull. X = Til stede. IR = Ikke relevant IV= Ikke vurdert IT = Ikke tilgjengelig informasjon								

Vurdering: Verdiene i dette scenarioet er liv og helse, materiell og bygning samt operativt tjenestetilbud. Liv og helse vurderes som svært høy, operativt tjenestetilbud som høy og materiell og bygning vurderes som moderat med bakgrunn i skadeomfang.

Fysisk sikring: Kriminalitetsforebyggende tiltak utenfor rådhuset er oversiktlige og godt belyste adkomstforhold, møteplasser, uteoppholdsarealer og gårdsrom. Dette synes å være mest effektivt på kveldstid da det på dagtid vil være normalt at personer beveger seg i dette området. De ulike funksjonene er plassert slik at det er mulighet for sosial kontroll av rådhusparken og gang- og sykkelveger, samt bygningen innvendig og utvendig. På grunn av at det var mange mennesker i bygget lå fokuset på de som oppholdt seg inne, dermed er det ingen fysiske sikringstiltak til stede i uteområdet som kan forhindre dette angrepet.

Elektronisk sikring: Uteområdet er overvåket med CCTV. Imidlertid anses dette sikringstiltaket som reaktivt i denne sammenhengen, og sikringstiltaket vil ikke forhindre et angrep av denne typen.

Administrasjon og ledelse: Det er ikke kjent om det er utarbeidet beredskapsplan for lignende scenarioer.

Analyse: Vi har ikke informasjon om det foreligger analyser av lignende scenario.

Verifikasjon: Vi har ikke informasjon om det er utført øvelser på lignende scenario.

Sosiale tiltak: Det legges til grunn at ansatte er profesjonell, har en forståelse av viktigheten av sikker jobbatferd og sikkerhetsmessig forberedelse til slike typer møter, og at det er høy grad av konformitet blant ansatte.

På bakgrunn av dette er analysens vurdering: Basert på manglende fysisk sikring av verdiene, det er derimot elektroniske sikringstiltak til stede, selv om disse anses som reaktive. Det er grunn til å tro at det mangler organisatoriske og menneskelige tiltak for å håndtere slike scenario mot rådhuset.

Vurderingen av sårbarhet vurderes som: Sårbarheten vurderes som **svært høy.**

Forslag til sikringstiltak

Basert på avdekkede sårbarheter og det totale risikobilde fra analysen anbefales ulike tiltak. Risikobilde presenteres på ny i tabellene nedenfor, gitt at anbefalte tiltak settes inn. Hvilken strategi som benyttes for hver risiko, og hvorvidt tiltakene blir implementert eller ikke, blir opp til beslutningstageren.

Scenario Nr 1	**Knivangrep mot en NAV-ansatt**
Teknologisk sikring	Det anbefales at det utredes et behov for ytterligere fysiske tiltak som kan forhindre angrep.
Organisatorisk sikring	Innføre rutine slik at ansatt alltid rapporters til leder dersom det er konflikt med en av brukerne. Innføre at det alltid er minst to saksbehandlere til stede i saker som oppleves som spesielt krevende.
Menneskelig sikring	Det bør innføres obligatorisk opplæring i håndtering av fysisk angrep fra brukere og hvordan dette kan forebygges.
Vurdering av risiko etter tiltak	Lav

Scenario Nr 2	**Dataangrep mot kommunens IT-systemer**
Teknologisk sikring	Siden vi ikke har funnet informasjon om hvilke fysiske sikringstiltak som er til stede, ønsker vi å anbefale at det gjøres en vurdering på hvorvidt de fysiske sikringstiltakene til stede er tilstrekkelige for å hindre uautorisert tilgang. Videre anbefaler vi at det utredes behov for anskaffelse av sikkerhetsovervåkningssystemer, hvis dette ikke er allerede på plass.
Organisatorisk sikring	Det anbefales at det utarbeides analyser for angrep mot IT-systemene både fysisk og logisk. Med nye digitaliseringstiltak i kommunen og økt behov for bevissthet anbefaler vi kommunen å utarbeide gode rutiner og prosesser for korrekt håndtering av disse. Innføring av tiltak vil kunne redusere sårbarheten ytterligere, men trusselen vil fortsatt være til stede.
Menneskelig sikring	Det er nødvendig å kontinuerlig arbeide for at kommunens ansatte til enhver tid utviser nettvett. Økt bevissthet oppnås gjennom målrettede kurs og informasjonskampanjer.
Vurdering av risiko etter tiltak	Moderat

Scenario Nr 3	**Forsøk på å sabotere en pågående politisk sak i kommunen**
Teknologisk sikring	Det bør utredes et behov for videre fysiske sikringstiltak for å skille publikumsområder fra kontorlokalene.
Organisatorisk sikring	Det må utarbeides analyser som vurderer objektsikkerheten og adgangskontroll. Det må etablerers rutiner og retningslinjer som gjør de ansatte i stand til å kunne utøve god sikkerhetsmessig utøvelse ved mottak av besøk.
Menneskelig sikring	Det er nødvendig å kontinuerlig arbeide for at kommunens ansatte til enhver tid har reel evne til å følge rutiner og prosesser. Dette kan oppnås gjennom kurs og/eller opplæring.
Vurdering av risiko etter tiltak	Lav

Scenario Nr 4	**En person utfører et terroranslag mot rådhuset**
Teknologisk sikring	Det anbefales at det gjøres en analyse som ser inn på aktuelle mulige fysiske tiltak i uteområdet.
Organisatorisk sikring	Innføre vakthold utenfor bygningen ved store arrangementer, for å være diskret kan det være sivilt vakthold. Ved større tilstedeværelse inne og utenfor rådhusets lokaler ved større arrangementer er det sannsynlig at det kan avverge et potensielt terroranslag. Et slikt tiltak kan derfor anses som svært effektivt for å forhindre et scenario som foreslått, og dermed redusere risikoen. Inkludere trusselvurderinger i fremtidige analyser.

Menneskelig sikring	Fokus på sikker jobbadferd. Ledertrening for å bistå ansatte til å takle stressede situasjoner. Fokus på tilstrekkelig balanse mellom jobb og privatliv og å unngå belastende merarbeid utover normal arbeidstid. Fokus på tilstrekkelig balanse mellom hver enkelt ansatte motivasjons.
Vurdering av risiko etter tiltak	Moderat

Vedlegg 4. Vurderingsskalaer for VTS-analysen

Verdivurdering:

Verdi:	Beskrivelse:
Svært høy	Tap eller reduksjon av verdi *har umiddelbare og svært alvorlige konsekvenser*
Høy	Tap eller reduksjon *har store konsekvenser*
Moderat	Tap eller reduksjon av verdi *kan ha* store konsekvenser
Lav	Tap eller reduksjon av verdi *har* små konsekvenser

Trusselvurdering:

Nivå	Beskrivelse	**Grad av sannsynlighet**	Beskrivelse
Svært høy	Indikatorene a, b, c, d og e er til stede	Meget sannsynlig	Det er meget god grunn til å forvente
Høy	Indikatorene a, b, c og d eller e er til stede	Sannsynlig	Det er grunn til å forvente
Moderat	Indikatorene a, b og c eller d er til stede	Mulig	Det er like sannsynlig som usannsynlig
Lav	Indikatorene a og b er til stede	Lite sannsynlig	Det er liten grunn til å forvente
Ubetydelig/Ikke relevant	Indikatorene a eller b er til stede	Svært lite sannsynlig	Det er svært liten grunn til å forvente

Indikatorer for trusselvurdering:

Indikator	Beskrivelse
A) Tilstedeværelse	Aktøren er til stede, antas å være til stede, eller kan forflytte seg til området eller regionen, eller på annen måte nå verdiene.
B) Kapasitet	Tilegnet, antatt eller demonstrert evne til å utføre handlingene som kan ramme virksomhetens verdier.
C) Intensjon	Det eksisterer, eller kan antas at det eksisterer, en vilje og/eller ønske til handling om å ramme virksomhetens verdier.

D) Historikk	Det eksisterer påviselig aktivitet over tid.
E) Målvalg	Det eksisterer ny og pålitelig informasjon som indikerer forberedelsen av et nært forestående angrep.

Sårbarhetsvurdering:

Nivå	Beskrivelse
Svært høy	Det eksisterer ingen sikringstiltak som beskytter verdiene og/eller sikringstiltakene er svært mangelfulle
Høy	Det finnes få eller ingen sikringstiltak som beskytter verdiene og/eller sikringstiltakene er mangelfulle
Moderat	Det eksisterer sikringstiltak som beskytter verdiene, men de er mangelfulle
Lav	Det finnes flere og gode overlappende sikringstiltak som beskytter verdiene
Ubetydelig/Ikke relevant	Det er ikke behov for sikringstiltak

Vedlegg 5. Grovanalyse med sløyfediagram

Bakgrunn

I dette kapitlet vil prosjektgruppen vurdere sannsynligheten og konsekvensen av identifiserte sikringsrisikoer knyttet til rådhuset og mulige konsekvenser av disse. For å systematisere og visualisere dataene vil sløyfediagram/bow-tie og grovanalyseskjema bli brukt. Da den delen av prosjektet som omhandler VTS-analyse tar for seg verdier, trusler og sårbarhet, vil disse elementene ikke bli vurdert i dette kapitlet. Oppgaven har som mål å undersøke om to forskjellige risikomodeller kan supplere hverandre, derfor er det valgt en tilnærming hvor sikringsrisikoelementene er komplimenterende og ikke overlappende. Tilnærmingen til sikringsrisiko med fokus på vurdering av sannsynlighet og konsekvens i denne delen av oppgaven, tar utgangspunkt i et realistisk syn på risikostyring hvor utgangspunktet er at risiko kan håndteres.

Undergruppen i prosjektet som skal gjennomføre analysen av sannsynlighet og konsekvens, har en tverrfaglig yrkesbakgrunn fra Kriminalomsorgen, Helsevesenet, Bane NOR og Forsvaret. Kompetansen til gruppemedlemmene strekker seg fra sikring av bygg og infrastruktur, IKT-trusler, kriminalitet, psykiatri, terror, etterretning og sabotasje. Gruppemedlemmene mener denne kombinasjonen av kompetanse vil redusere usikkerhets-momentet i analysen, da gruppen har relevant innsikt i de aktuelle problemstillingene. Sannsynlighetsvurderingene i kapitlet er også basert på teamets kompetanse og ikke frekvensen av hendelser. Det nye rådhuset i Sola skal bestå i mange år fremover. Selv om truslene i grovanalysen er valgt ut fra PST sin trusselvurdering for 2020, er risiko er et element som er i konstant endring. Prosjektgruppen har derfor vurdert trender og tatt med mulige fremtidige trusler og scenarier i analysen. Spesifikk kunnskap om sikringsobjektet og sikringsrisikoforhold knyttet til Sola Rådhus er hentet gjennom systembeskrivelsen, som er beskrevet tidligere i dette dokumentet.

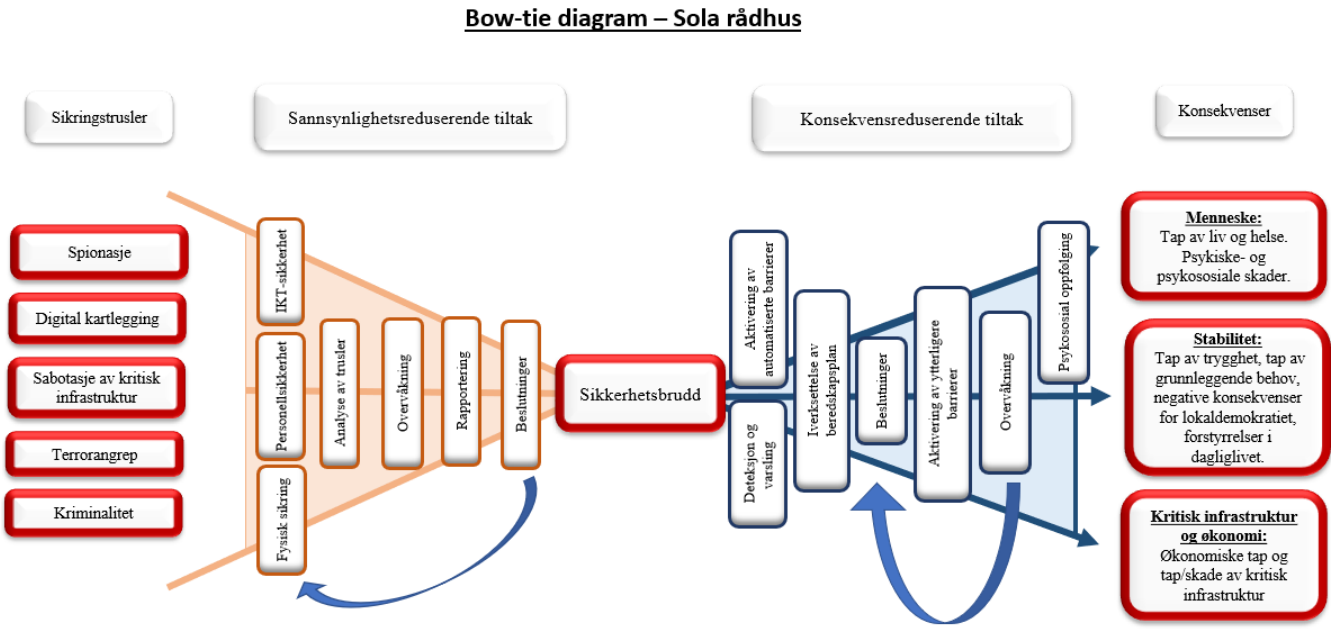
I PST sin trusselvurdering for 2020 fremheves det at de mest alvorlige truslene mot Norge er (PST, 2020):

- spionasje mot regjeringen, Stortinget og Forsvaret
- digital kartlegging og sabotasje av kritisk infrastruktur
- terrorangrep utført av enkeltpersoner motivert av høyreekstrem eller ekstrem islamistisk ideologi

I tillegg har vi identifisert flere trusler som kan være relevante mot et offentlig bygg som Sola rådhus, og kategorisert disse under samlebegrepet kriminalitet.

Vurdering av relevante sikringsrisikoer knyttet til Sola rådhus

Prosjektgruppen har valgt å bruke sløyfediagram som hjelpemiddel for å sette de identifiserte elementene inn i en kontekst, og for å visualisere hva analysen skal inneholde. Sløyfediagrammet i figur 6 illustrerer hvilke sikringstrusler, sannsynlighetsreduserende tiltak, konsekvensreduserende tiltak, og konsekvenser som vi har identifisert for Sola rådhus. Videre i risikovurderingsskjema for grovanalysen vil disse identifiserte sikringstruslene relateres til tilhørende tiltak og konsekvenser.



Figur 5 Bow-tie diagram for Sola rådhus

Sikringstrusler

Utgangspunktet for modellen starter med de definerte sikringstruslene som står oppført helt til venstre i diagrammet. På bakgrunn av PST sin trusselvurdering og prosjektgruppens egne vurderinger, er følgende sikringstrusler vurdert som mest relevant:

- Spionasje: PST skriver at utenlandske etterretningstjenester i 2020 vil rette sin aktivitet mot blant annet norske myndigheter, næringsliv, forsvar og beredskap, og norske forskningsmiljøer (PST, 2020). Sola kommune har viktig infrastruktur knyttet

til olje- og gassindustrien gjennom offshore-basene i Risavika, og mange bedrifter knyttet til oljenæringen holder til i kommunen. Flere av disse bedriftene er knyttet til forskning og utvikling, og kan av den grunn være av interesse for utenlandske etterretningsaktører. Oljenæringen forvalter også store naturressurser som er av betydning for andre staters energiforsyning og næringen er derfor utsatt. Flyplassen som et viktig knutepunkt for infrastrukturen på Nord-Jæren og helikopterbase for transport av personell til å fra Nordsjøen, er annen infrastruktur som kan være av interesse for etterretningstjenester. I flere land bistår etterretningstjenestene eget næringsliv, og det kan derfor være vanskelig å skille statlig etterretning fra industrispionasje. Saker som omhandler petroleumsnæringen og viktig infrastruktur i kommunen, kan bli administrativt og politisk behandlet i kommunen. Av denne grunn mener prosjektgruppen at Sola kommune kan være utsatt for spionasje.

- Digital kartlegging og sabotasje: For å få tak i informasjon bruker aktører innen fremmede makters statlige etterretning, og aktører innen industrispionasje, digital kartlegging for å skaffe seg urettmessig tilgang til datanettverk. I Sola rådhus kan datanettverket være av interesse i forbindelse med etterretningsinnsamling. Hvis aktørene ønsker å påvirke politiske beslutninger kan tilgang til datanettverk gjøre inntrengere i stand til å sabotere eller manipulere data.
- Terrorangrep: PST har definert det som sannsynlig at denne type hendelser kan ramme Norge i 2020. Sola rådhus kan neppe regnes for å være et potensielt mål med høy symbolverdi for internasjonal terrorisme, men det kan være andre intensjoner som ligger bak ønske om å gjennomføre terroraksjoner. Motivet kan for eksempel være hevn mot lokale myndigheter, slik som vi så under terroraksjonen i Oklahoma City i 1995.
- Kriminalitet: Selv om kriminalitet ikke er tatt med i PST sin liste over de mest alvorlige truslene i 2020, er gruppens vurdering at kriminalitet vil utgjøre en av de mest sannsynlige sikringstruslene rettet mot Sola rådhus.

Nærmere beskrivelse og analyse av de identifiserte sikringstruslene vil inngå i grovanalysen.

Sannsynlighetsreduserende tiltak

Gruppen har identifisert disse sannsynlighetsreduserende tiltakene i forbindelse med sannsynlige sikringsbrudd i Sola Rådhus:

- Fysisk sikring: Fysiske adgangsregulerende tiltak som dører, kortlesere, kodelåser, personellsluser, fysiske kjøretøysperringer, bommer, garasjeporter og vakthold.
- IKT-sikkerhet: IKT-infrastruktur, hardware og software løsninger, overvåkning av datatrafikk, opplæring av personell.
- Personellsikkerhet: Opplæring i sikring, akkreditering og individuelle tiltak.
- Analyse av trusler: I planfasen av byggeprosessen for nytt rådhus i Sola vil det bli gjennomført en sikringsrisikoanalyse (Ref. NS 5831:2014 Sikringsrisikostyring og NS 5832:2014 Krav til sikringsrisikoanalyse). I driftsfasen vil informasjon som samles inn gjennom virksomhetens overvåkningssystemer bli analysert, bearbeidet og rapportert. Innsamlet informasjon vil bli satt i sammenheng med sikkerhetsrelatert informasjon fra norske myndigheter.
- Overvåkning: Teknisk overvåkning med kamera (video eller TV). Automatisk eller manuell overvåkning. Fysisk overvåkning av vektere eller annet personell med sikkerhetsfunksjon.
- Rapportering: Data fra overvåkning rapporteres til ansvarlig for aktuelt område.
- Beslutninger: Analyse og vurdering av rapporter gis til beslutningstakere, som beslutter videre handling og tiltak.

Konsekvensreduserende tiltak

Gruppen har identifisert disse konsekvensreduserende tiltakene i forbindelse med sannsynlige sikringsbrudd i Sola Rådhus:

- Deteksjon og varsling: De tekniske overvåkningssystemene detekterer og varsler om sikringsbrudd. I tillegg vil mennesker med operasjonelle vakt- og sikringsfunksjoner kunne detektere sikringsbrudd via egen overvåkning eller mottak av varsel fra publikum. Mottakere av varsel kan være private eller offentlige beredskapsorganisasjoner som f.eks. alarmsentral, politi, NorCERT (Norwegian Computer Emergency Responce Team).

- Aktivering av automatiske barrierer: Bruk av automatiske bommer, låser, dører, porter etc.
- Iverksettelse av beredskapsplanen: Iverksettelse av tiltak i henhold til beredskapsplanen. Varsling - håndtering - normalisering.
- Beslutninger: Ut ifra situasjonsbilde og vurdering av potensiale vil beredskapsledelsen beslutte iverksettelse av konsekvensreduserende tiltak.
- Aktivering av ytterligere konsekvensreduserende barrierer, for å stanse sikkerhetsbruddet og starte normalisering.
- Overvåkning: Observere om sikkerhetsbruddet er stanset, eller om det må tas nye beslutninger og evt. Iverksettes ytterligere tiltak.

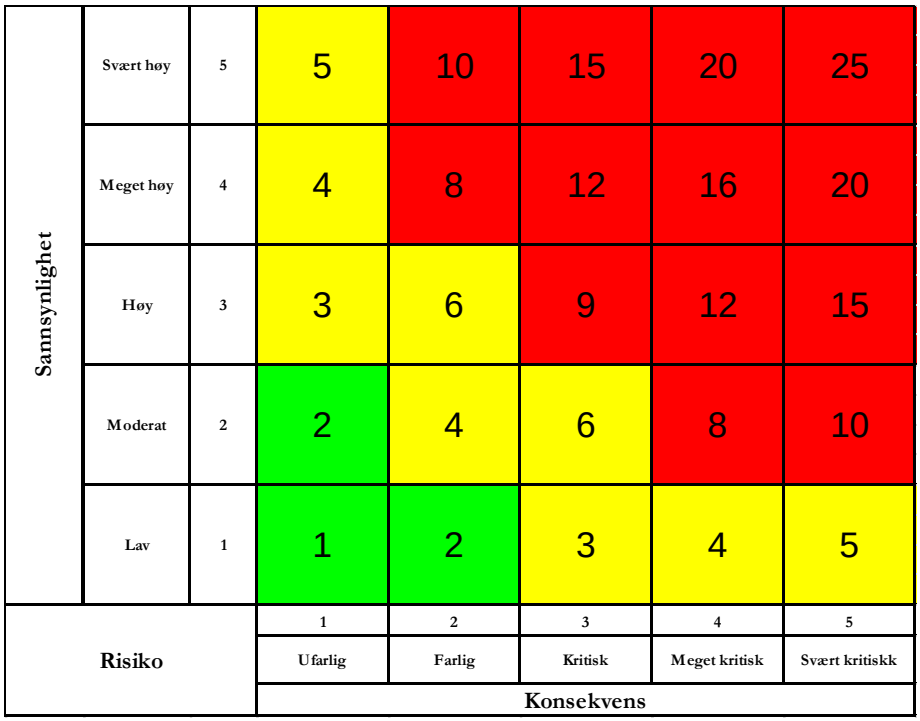
Konsekvenser

Sikringsbrudd innen spionasje, digital kartlegging og sabotasje, terrorangrep og kriminalitet knyttet til Sola rådhus vil ha ulike konsekvenser. Følgende hovedgrupper av konsekvenser er identifisert:

- Liv, helse, dødsfall og skader som direkte følge av sikkerhetsbrudd.
- Stabilitet: grunnleggende behov, forstyrrelser i dagliglivet, negative konsekvenser for lokaldemokratiet.
- Negative konsekvenser for kritisk infrastruktur.
- Materielle verdier: Økonomiske tap og tap av infrastruktur.

Grovanalyse av sikringstrusler, sannsynlighetsreduserende- og konsekvensreduserende tiltak knyttet til nye Sola rådhus

Gruppen har valgt å bruke grovanalyseskjema som metode for vurdering av sannsynligheter og konsekvenser. Forsvarsbygg (FB) har utviklet en risikomatrise som arbeidsgruppen vurderer å passe til risikovurderingene i dette kapitlet (Busmundrud, Maal, Kiran, & Endregard, 2015). Følgende matrise utarbeidet av FB vil bli brukt videre i dette kapitlet:



Figur 6 Risikomatrise. Hentet fra Forsvarsbygg (Busmundrud, Maal, Kiran, & Endregard, 2015)

Følgende konsekvensvurderinger er lagt til grunn i matrisen:

Betegnelse	**Driftsforstyrrelser/skade**
1 UFARLIG	a) Ingen nedetid. Få eller små endringer i forhold til operativ evne b) Kompromittering av informasjon UGRADET c) Ingen personskader d) Økonomiske konsekvenser opptil 100 000 kr
2 FARLIG	a) Nedetid < 1 døgn. Viktig funksjon kan ikke opprettholdes, eller ekstraordinære tiltak må iverksettes for å håndtere situasjonen b) Kompromittering av informasjon BEGRENSET c) Få mennesker blir skadet, mindre personskader d) Økonomiske konsekvenser opptil 100 000 – 1 000 000 kr
3 KRITISK	a) Nedetid 1 døgn til 1 uke. Flere viktige funksjoner kan ikke opprettholdes, eller omfattende ekstraordinære tiltak må iverksettes for å håndtere situasjonen. b) Kompromittering av informasjon KONFIDENSIELT c) Få mennesker blir skadet, mindre personskader

	d) Økonomiske konsekvenser opptil 1 000 000 – 50 000 000 kr
4 MEGET KRISTISK	a) Nedetid mer enn 1 uke. Vital funksjon kan ikke opprettholdes b) Kompromittering av informasjon HEMMELIG c) Død/alvorlig masseskade > 5 personer d) Økonomiske konsekvenser over 50 000 000 kr
5 KATASTROFALT	a) Nedetid mer enn 1 år. Vital funksjon kan ikke opprettholdes b) Kompromittering av informasjon STRENGT HEMMELIG c) Massedød d) Økonomiske konsekvenser over 100 000 000 kr

Tabell 8 konsekvensvurdering. Hentet fra Forsvarsbygg (Busmundrud, Maal, Kiran, & Endregard, 2015)

Følgende sannsynlighetsvurderinger er lagt til grunn i matrisen:

Betegnelse	**Kriterier for sannsynligheten**
1 Lav	a) Grad av aktive sikringstiltak b) Grad av passive siktingstiltak c) De ansattes kompetanse innen sikring d) Beslutningstakere og fagpersoner innen risikostyring/beredskap sin kunnskap om sikringstrusler og evne/myndighet til å iverksette dimensjonerende tiltak. e) Beslutningstakere og fagpersoner innen risikostyring/beredskap sin tilgang til relevant etterretningsinformasjon og råd fra statlige organ.
2 Moderat	
3 Høy	
4 Meget høy	
5 Svært høy	

Tabell 9 Sannsynlighetsvurdering. Hentet fra Forsvarsbygg (Busmundrud, Maal, Kiran, & Endregard, 2015)

Vedlegg 6. Risikovurderingsskjema

Risikovurderingsskjema for risikoanalyse Sola rådhus

Ansvarlig for prosjektet:	Prosjektgruppe Regjeringskvartalet
Ansvarlig for gjennomføring:	Prosjektgruppen
Dato:	22.05.2020

SAM 510

Uønsket hendelse	Årsak	Sannsynlighetsreduserende barriere	Konsekvensreduserende barriere	Konsekvens	S	K	R
Etterretning - Spionasje og digital kartlegging	Datainnbrudd / Innhente data	Sikkerhetssystemer innen IKT, opplæring av ansatte/forbedre kunnskap om informasjonssikkerhet, bedre sikkerhetskulturen, adgangskontroll, vurdering av ansatte opp mot utroskap/ innside-jobb, bevisstgjøring innen bruk av mobiltelefon og avlytting, avlytningssikre møterom, skjerme innsikt igjennom vinduer.	Krise- og beredskapsplanverk	Tap av kritisk informasjon/ omdømme	Høy	Kritisk	9
Etterretning - Spionasje og digital kartlegging	Angrep mot IKT infrastuktur som en del av hybrid operasjon	God IKT-sikring avgjørende for å minimere risikoen. opplæring av ansatte/forbedre kunnskap om informasjonssikkerhet, bedre sikkerhetskulturen, adgangskontroll, bevisstgjøring innen bruk av mobiltelefon og avlytting, avlytningssikre møterom, skjerme innsikt igjennom vinduer. Strøm, datalinjer, nødaggregat, UPS, redundante linjer, datalagring.	Krise- og beredskapsplanverk	Tap eller skade av IKT-infrastruktur eller informasjon	Høy	Kritisk	9
Etterretning - Spionasje og digital kartlegging	Påvirke politiske saker	Sikkerhetssystemer innen IKT, opplæring av ansatte/forbedre kunnskap om informasjonssikkerhet, bedre sikkerhetskulturen, adgangskontroll, vurdering av ansatte opp mot utroskap/ innside-jobb, bevisstgjøring innen bruk av mobiltelefon og avlytting, avlytningssikre møterom, skjerme innsikt igjennom vinduer.	Krise- og beredskapsplanverk	Svekket demokrati / tap av omdømme	Lav	Kritisk	3
Etterretning - Spionasje og digital kartlegging	Utro tjener/ innside-jobb	Bakgrunnssjekk opp mot politregisteret og økonomisk situasjon. Eventuell sikkerhetsklarering av ansatte.	Krise- og beredskapsplanverk	Tap av kritisk informasjon/ omdømme/ svekket demokrati	Lav	Kritisk	3
Kriminalitet	Bevisste og ubevisste voldshandlinger mot ansatte i rådhuset	Opplæring og trening av ansatte i slike situasjoner. Sikkerhetspersonell, alarm, kodelåser, inndeling i soner med adgangskontroll.	Oppfølging gjennom: Debrifieng, defjusing, Kollegastøtte, BHT, medarbiedersamtale, etc.	Psykisk og/ eller fysisk skade på personell	Svært høy	Kritisk	15
Kriminalitet	Ansatt tatt som gissel	Opplæring og trening av ansatte i slike situasjoner.	Krise- og beredskapsplanverk, debrifieng, defjusing, Kollegastøtte, BHT, medarbiedersamtale, etc	Skade/ død på personell.	Lav	Meget kritisk	4
Kriminalitet	Trusler mot ansatte psykisk/fysisk. Sosiale forskjeller	Opplæring og trening av ansatte i slike situasjoner.	Oppfølging gjennom: Debrifieng, defjusing, Kollegastøtte, BHT, medarbiedersamtale, etc	Psykisk og/ eller fysisk skade på ansatte	Svært høy	Kritisk	15

Kriminalitet	Cyberangrep mot ansatte sine dokumenter. Ønske om penger, informasjon eller sverte rådhusets ry/-e.	Sikkerhetssystemer innen IKT, opplæring av ansatte gjennom Nasjonalt cybersikkerhetssenter (NSM), adgangskontroll, Opplæring innen informasjonssikkerhet.	Krise- og beredskapsplanverk	Tap av kritisk informasjon/ omdømme	Moderat	Meget kritisk	**8**
Sabotasje av kritisk infrastruktur	Ødelegge data	Sikkerhetssystemer innen IKT, opplæring av ansatte gjennom Nasjonalt cybersikkerhetssenter (NSM), adgangskontroll, Opplæring innen informasjonssikkerhet, vurdering av ansatte opp mot utroskap/ innside-jobb.	Krise- og beredskapsplanverk	Tap av kritisk informasjon/ omdømme	Høy	Kritisk	**9**
Sabotasje av kritisk infrastruktur	Hindre kommunen å iverksette planer/ ta besluttninger.	Adgangskontroll for ansatte og besøkende, begrenset antall personer i møtesalene. Øke barrierene/ sikringen mellom publikum og møtedeltagere i møtesalene. Opprettholde en god adgangskontroll. Begrenset antall publikum under møtene. Øke sikkerheten ved kjent probelmatisk tematikk.	Krise- og beredskapsplanverk	Hindre demokratiet i å ta valg og avgjørelser. Skade på materielle verdier	Høy	Meget kritisk	**12**
Terrorangrep	Politiske mål for å skape endringer. Kan gjennomføres gjennom ulike virkemidler som skyting, bomber, knivstikking, gisseltaking.	Dialog med PST for oppdatert informasjon vedrørende endring i trusselbilde for politiske mål. Adgangskontroll. Inndeling av huset i soner. Kjøretøyssperrer. Kameraovervåkning.	Krise- og beredskapsplanverk	Skade/ død på personell. Skade på materielle verdier.	Lav	Svært kritisk	**5**

Vedlegg 7. Informasjon om Sola rådhus

Nedenfor listes opp egenskapene ved organiseringen og utformingen ved bygget (Longva arkitekter, 2015):

- *"Trapp/heis og alle publikumsfunksjoner er plassert lett tilgjengelig langs den sentrale kommunikasjonsåren.*
- *Servicetorg/publikumsmottak er godt synlig – vis a vis hovedinngang.*
- *Bystyresalen ligger i direkte tilknytning til foajéen, sentralt på plan 1.*
- *Store glassflater i både vegg mot foaje og i foajeens fasade eksponerer bystyresalen mot Rådhusplassen.*
- *Kantinen er foreslått sentralt i komplekset – i "mellombygget" på plan 0. […] Kantinen har mulig direkte adkomst fra adkomst fra nord. Dette gjør at kantinen enkelt kan stenges fra resten av rådhuset for ulike arrangementer.*
- *Felles "møteroms-pool" er foreslått sentralt på plan 1.*
- *Konferanseavdeling er foreslått ved kantinen i plan 0.*
- *Bystyresalen, møterom på plan 1 og konferanseavdelingen på plan 0 har alle nærhet til hverandre, og er plassert langs kommunikasjonsåren. De kan benyttes sammen ved store arrangementer.*
- *Adkomsten mot nord på plan 0 vil kunne benyttes som ansatte inngang, med nærhet til sykkelparkering og garderober.*
- *Mot vest vil det være en serviceadkomst samt en sekundær publikumsadkomst og skjermet adkomst for publikum til oppvekstenhet.*
- *Alle publikumsfunksjoner og møterom er organisert langs kommunikasjonsåren langs den nordvendte fasaden. Slik blir det differensiert mellom arealer med tilgang for publikum og rene kontorarbeidsplasser. En slik skjerming av kontorarbeidsplassene er viktig i den daglige driften. Alle delene vil ha god kontakt.*
- *I utgangspunktet vil begge bygningsvolumene være generelle og kunne innredes fleksibelt til ulik bruk.*
- *Den nye "administrasjonsblokken" vil ha større sammenhengende etasjeflater enn eksisterende fløy D – og vil være meget godt tilrettelagt for generelle kontorarbeidsplasser.*
- *En generøs lysgård ned til plan 2 vil gi meget gode dagslysforhold, og lysgården er i direkte tilknytning til pauseareal for ansatte."*

Det fremkommer av plantegningene til det nye Sola rådhus at det i underetasjen av fløy A er samlet teknisk rom, serverrom, UPS/Avbruddsfri strømforsyning, arkiv og lager for IKT. UPS/Avbruddsfri strømforsyning hindrer at strømmen uteblir i lengre perioder noe som sørger for at systemer er mindre sårbare. Fra Sola kommunes årsrapport for 2019 fremkommer det at kommunens IKT-avdeling jobber kontinuerlig med vedlikehold og forsterkning av infrastruktur. Det er anskaffet programvare for robotteknologi, som skal gjøre det mulig å automatisere og robotisere oppgaver. Denne teknologien oppdager og varsler automatisk om feil og avvik (Sola kommune, 2020b).