Handelshøgskolen Innlandet - Fakultet for økonomi og samfunnsvitenskap

Bjørn Melandsø Kjelsaas

Masteroppgave

Modeller for risikoanalyse i Norge

En organisasjonsteoretisk studie av sikkerhets- og beredskapsorganisasjoners bruk av risiko- og sårbarhetsanalyser eller sikringsrisikoanalyser. Hva er bakgrunnen for disse modellene og hvilke faktorer kan forklare valget?

An organizational view on the choice between the risk- and vulnerability analysis vs. security threat analysis models within Norwegian security- and emergency preparedness environments.

Master i offentlig ledelse og styring (MPA)

2020

Samtykker til tilgjengeliggjøring i digitalt arkiv Brage JA ☒ NEI ☐

Innhold

Norsk sammendrag

Denne studien baserer seg på problemstillingen; "Hva forklarer at vi har to risikomodeller i Norge og hva er bakgrunnen for at sikkerhets- og beredskapsmiljøene så langt ikke har klart å samle seg om en felles og omforent modell for risikoanalyse?"

Problemstillingen hentyder til de to risikomodellene som har størst utstrekning og aktualitet innenfor sikkerhets- og beredskapsmiljøene. Den ene er risiko- og sårbarhetsanalysen (ROS), som tar utgangspunkt i de to faktorene *sannsynlighet* og *konsekvens* for å beskrive risikoen. Den andre er sikringsrisikoanalysen som tar utgangspunkt i de tre faktorene *verdi*, *trussel* og *sårbarhet* (VTS) for å beskrive risikoen. Basert på innsamlingen av primærdata fra miljøene er funnene suksessivt analysert i lys av et knippe organisasjonsteoretiske perspektiver.

Det ble påvist distinkte forskjeller mellom ROS- og VTS-modell på hver enkelt undersøkelse. Funnene tyder på at valget av ROS-analyse kan forklares ut fra i teorier om instrumentalisme og tvungen isomorfisme, det institusjonelle kulturperspektivet og stiavhengighet. Funnene tyder videre på at valget av VTS kan forklares som et rasjonelt og kunnskapsbasert valg hos organisasjoner som har ressurser til å ta et selvstendig valg (handlefrihet). I tillegg fremstår VTS-modellen som et godt eksempel på myteperspektivet fra ny-institusjonell teori. Begge modellene kan forklares ut fra rasjonelle valg-teorier i form av optimal eller begrenset rasjonalitet. Det er videre gjort kvalitative observasjoner som identifiserer svakheter ved begge disse modellene.

Årsaken til at sikkerhets- og beredskapsmiljøene ikke har klart å samle seg om en felles og omforent risikomodell ser ut til å basere seg på kulturelle forskjeller, ulik forståelse av hva sikkerhet er for noe, ulike oppfatninger om hvordan trusselen skal forstås, ulikt teoretisk startpunkt for hver av modellene og forskjellige forutsetninger hos aktørene. Til tross for forskjellene ser vi at det er en rekke fellestrekk som gjenspeiler seg. En god risikoanalyse bygger på en strukturert tilnærming med et verdifokus, et tilstrekkelig datagrunnlag, kompetente analytikere og ledelsesforankring. Analysene bør innbefatte både teknisk/lokal kunnskap og overblikk, og de bør bunne ut i transparente, etterprøvbare vurderinger. Uavhengig av metodevalg må risikobildet legges frem for beslutningstaker på en overbevisende måte, med en reflektert beskrivelse av usikkerhetsgraden og validitet.

Abstract

This study explains why we utilize two different risk models in Norway, and for what reasons the security and emergency preparedness environments so far have failed to gather upon a common and unified model for risk analysis.

The problem refers to the risk- and vulnerability analysis model (ROS), based on *probability* and *consequence*, and the security threat analysis model founded on the factors *value*, *threat* and *vulnerability* (VTS). The findings were analyzed in the view of selected organizational theoretical perspectives.

Each of three separate reviews identified differences between the ROS and VTS models. Findings suggest that the choice of ROS can be explained on the basis of theories of instrumentalism and forced isomorphism, the institutional cultural perspective and path dependency. The findings further suggest that the choice of VTS can be explained as a rational and knowledge-based choice among organizations with sufficient resources to make their independent choice (freedom of action). Additionally, the VTS-model exemplifies the myth perspective from neo-institutional theory. Both models can be explained by rational choice theories in terms of optimal or limited rationality.

In addition, further observations identified weaknesses and the need for improvements on both of these models.

The reason why the security and preparedness environments have failed to gather together on a common and unified risk model seems to be caused by cultural differences, different understandings of safety and security, different perceptions of how the threat is to be understood, different theoretical starting points and different characteristics of the actors.

Despite the distinction, we see a number of qualitative similarities. A proper risk analysis should rely on a structured approach with a focus on the values (assets), a satisfactory information base, competent analysts and management anchoring. The process should include both technical and local expertise as well as a strategic overview and culminate in transparent and verifiable assessments. Regardless of the model chosen, the risk picture should be handed over to the decision maker in a convincing matter, including truthful descriptions of the degree of uncertainty.

Forord

Etter en årrekke innenfor offentlig sikkerhet og beredskap har jeg spesielt bitt meg merke i et par tilbakevendende tema som kommer opp i faglige diskusjoner hos profesjonsutøvere. Det ene er diskusjonen om sikkerhetsbegrepet, nærmere bestemt om distinksjonen mellom utilsiktede *hendelser* og tilsiktede *handlinger*. Det andre er debatten om hva som er den beste måten å analysere risiko på. Jeg mener at det er på tide å legge denne ballen død...

Jeg ser tilbake på inspirerende forelesninger sammen med mer eller mindre likesinnede. Mest på Rena, men også gjennom studiesamlingene i Karlstad og på Schæffergården utenfor København. Det sosiale samspillet på kullet vårt har vært unikt, jeg minnes at flere av oss fant tonen allerede fra første middagen på Kjellerkroken i august 2017. Noen av mine medstudenter har betydd mer for meg enn andre, både på samlinger, i forbindelse med innleveringer og ikke minst i innspurten på denne oppgaven. Dere vet selv hvem dere er.

Jeg ville aldri greid å realisere en erfaringsbasert ledelsesmaster kombinert med full jobb uten en kunnskapsorientert arbeidsgiver som Departementenes sikkerhets- og serviceorganisasjon. Jeg takker til mine kolleger og seksjonssjef Stian Sørensen som har gitt meg fleksibilitet og forståelse i hverdagen, kanskje spesielt gjennom innspurten de siste ukene.

Takk til Handelshøgskolen Innlandet for muligheten, og veileder Pernille Rieker som har loset meg gjennom struktur og format på det vitenskapelige arbeidet. Videre vil jeg rette en kjempestor takk til alle dere som hjalp meg med å bygge et godt tallmateriale, så vel som kvalitative refleksjoner omkring risikoanalysen ved å støtte opp om spørreundersøkelsen i januar. Fra fagmiljøene vil jeg spesielt honorere Morten Bremer Mærli og Tore Drtina som begge bidro med innsiktsfulle bidrag i full gjennomsiktighet, fra ulike faglige ståsted. Alle som er nevnt over har hjulpet meg å virkeliggjøre studiens fulle potensial.

Aller mest vil jeg takke min kjære Brita og mine to sønner som har holdt ut med en far som i ukesvis har trukket seg tilbake på hjemmekontoret for å studere og skrive. Dere betyr alt.

Oslo, 2. mars 2020

Bjørn Melandsø Kjelsaas

1. Innledning

1.1 Introduksjon til tema

Risikoanalyse handler om å gjennomføre en systematisk prosess for å få visshet og deretter fremstille et beslutningsgrunnlag for eventuelle tiltak mot sikkerhetstruende forhold. I norske sikkerhets- og beredskapsmiljøer er det hovedsakelig to ulike modeller som har fått særlig anvendelse. Den ene er risiko- og sårbarhetsanalysen (ROS), den andre er sikringsrisikoanalysen (VTS). Begge disse modellene har til hensikt å forklare hva slags og hvor mye risiko en står overfor, men modellene har forskjeller av både teoretisk, institusjonell og kulturell karakter. Det er få personer som arbeider med risiko i utgangspunktet og "miljøene", om vi i hele tatt kan bruke et sånt utrykk er fragmenterte[1]. Spørsmålet er om det ikke ville vært samfunnsøkonomisk lønnsomt å samle sikkerhets- og beredskapsfolk omkring en felles analysemodell.

Det krever både tid, penger og øvrige ressurser å etablere, vedlikeholde og ikke minst utvikle kompetansen på flere risikomodeller overfor en spredt og fragmentert målgruppe. Målsetningen med studien har vært å fremskaffe kunnskap om hva som er bestemmende for valget mellom de to analysemodellene og hva som skiller de fra hverandre, slik at det blir enklere å orientere seg i landskapet og velge riktig "verktøy" til riktig jobb. Som en del av forklaringen blir det nødvendig med en beskrivelse av modellenes kontekst i lys av gjeldende regelverk og etablert praksis, i tillegg til de organisasjonsteoretiske perspektivene som legges til grunn for analysen. Hva er bakgrunnen for at man har to slike modeller for risikoanalyse, og hvilke faktorer er bestemmende når man velger å benytte den ene fremfor den andre? [2]

[1] Studien fokuserer på sikkerhet og beredskapsmiljøer innenfor stat, kommune og private virksomheter på sektor- og organisasjonsnivå ned til objekt- eller entitetsnivå. "Miljø" må i denne sammenhengen forstås som en sosial konstruksjon da det typisk gjelder enkeltpersoner i vidt forskjellige organisasjoner, sjeldent et homogent miljø som sådan. Se også punkt 3.1.

[2] Det finnes mange måter å analysere risiko på, men mitt arbeid er avgrenset til disse to modellene.

1.2 Historisk kontekst

I Norge har både industrien og offentlige organer vært preget av en sterk sikkerhetskultur gjennom flere tiår. Mye av sikkerhetskulturen oppsto på 1980-tallet som blant annet var preget av Alexander L. Kielland-ulykken i 1980 (Solbakken og Dahle 2019) og Tsjernobyl-ulykken i 1986 (Salbu 2019). Ulykkene satte fokus på *safety*-risiko[3], enten den kom som en følge av tekniske svakheter med tap av menneskeliv innenfor et bestemt område, eller om vi i tillegg til tap av mange liv skulle oppleve en internasjonal miljøkatastrofe med enormt ødeleggende konsekvenser. Foruten de overnevnte ulykkene nådde den kalde krigen sitt høyde- og vendepunkt i samme perioden. Men til tross for den sikkerhetspolitiske situasjonen og det rystende drapet på statsminister Olof Palme i vårt naboland i 1986, var det lite fokus på politisk vold eller andre former for *security*-risiko[4] i samfunnsdebatten.

Basert på den tydelige helse, miljø- og sikkerhetskulturen (HMS) ble risikoarbeidet gradvis og i økende grad systematisert og profesjonalisert, slik at ROS-analysen som vi kjenner i dag har tradisjoner med røtter så dype at det kan være vanskelig å finne startpunktet. Men grunnlaget for diskusjonen omkring ROS- eller VTS-analyse i Norge ser ut til å være knyttet til distinksjonen mellom *safety* og *security*.

Etter terrorangrepene mot Regjeringskvartalet og Utøya fikk security-debatten et spillerom, og risikopersepsjonen i samfunnet ble satt under lupen. Det var både pårørende til de mange ofrene, sikringsmiljøene og ikke minst 22. juli-kommisjonens rapport (Gjørv-kommisjonen) som fremmet mye av kritikken (NOU 2012: 4). Foruten systemsvakheter hos forskjellige offentlige instanser, gikk diskusjonen videre på mulige trusler som beslutningstakerne eller allmenheten ikke hadde kunnskaper eller persepsjon til å ta inn over seg. Faresignaler blir sjelden tatt på alvor dersom de blir oppfattet som urealistiske eller usannsynlige av en majoritet. Eksemplene kan være mange, men jeg vil holde meg til 22. juli. Sikringsmiljøer vurderte Regjeringskvartalet for å være et aktuelt mål for terrorbomber også før 22. juli, men hverken Oslo Kommune eller majoriteten av innbyggerne kunne fatte og begripe at slike handlinger kunne materialisere seg i vårt lille land. I ettertiden er det mange som beskriver

[3] Helse, miljø og sikkerhetsarbeid knyttet til utilsiktede uønskede hendelser.

[4] Sikringsarbeid som skal identifisere og helst forebygge tilsiktede (villede) uønskede handlinger.

slike hendelser som "sorte svaner[5]", det vil si at det har skjedd noe utenkelig som ikke kunne forutses (Taleb, 2010). Selve bombescenariet mot Regjeringskvartalet fantes det imidlertid risikovurderinger på, og de ansvarlige var bekymret for at sikringsarbeidet tok alt for lang tid (Andersen, 2006).

1.3 Problemstilling og hypoteser

Hvorfor kan eller vil ikke organisasjoner benytte seg av samme risikometodikk dersom det finnes en modell som i prinsippet kan brukes på alt? Med utgangspunkt i modellene med sine underliggende forskjeller blir mitt hovedspørsmål som følger:

> Hva forklarer at vi har to risikomodeller i Norge og hva er bakgrunnen for at sikkerhets- og beredskapsmiljøene så langt ikke har klart å samle seg om en felles og omforent modell for risikoanalyse?

La oss starte med en kort forklaring på hva som skiller disse to modellene.

Risiko- og sårbarhetsanalysen (ROS) er en to-faktormodell hvor de definerte farescenariene analyseres ut fra samsvaret mellom *sannsynligheten* for at noe vil skje og *konsekvensen* dersom dette skjer. Ut fra analysen kommer man opp med en risikoverdi som eksempelvis kan angis med farger, tallverdier eller nivåer, slik som lav, middel, høy, eller grønn, gul og rød. ROS-modellen er velkjent både i og utenfor sikkerhetsmiljøene. Samme modell blir også brukt innenfor en rekke forskjellige bransjer, organisasjoner og fagområder, slik som forsikring, finans, virksomhetsstyring og mye mer. ROS-modellen kan ifølge sin norske standard brukes for å analysere risiko knyttet til både uønskede *utilsiktede* hendelser (safety) og *tilsiktede, villede* handlinger (security), men kritiseres for at den har vært mindre egnet til å håndtere lavfrekvente hendelser/handlinger som sjelden eller aldri har forekommet tidligere.

Sikringsrisikoanalysen (VTS) er en tre-faktormodell hvor de aktuelle farescenariene analyseres ut fra samsvaret mellom *verdien*, *trusselen* og *sårbarheten.* Til tross for at begge modeller har en felles hensikt i det å analysere risikoen, er VTS-analysen ut fra beskrivelsen mer komplisert da analyseprosessen tar for seg en syklus som blant annet omfatter verdivurdering, fastsetting av sikringsmål, trusselvurdering, scenariovalg,

[5] "Alle svaner er hvite", med referanse til Karl Poppers skepsis til å fatte standpunkt basert på induksjon.

sårbarhetsvurdering, valg av sikringstiltak og vurdering av usikkerhet. I tillegg er VTS-modellen dedikert for analyse av *tilsiktede* (security) handlinger. Sammenlignet med ROS-analysens enkelhet fremstår VTS-analysen med både større kompleksitet og begrenset bruksnytte. Men en grundig ROS-analyse bør vel også innbefatte en verdivurdering, sikringsmål, trusselvurdering ut fra noen scenariovalg, sårbarhetsvurdering og kommunikasjon av usikkerhetsfaktorer? Forskjellene mellom modellene er slett ikke sort/hvitt og jeg vil gjennom denne oppgaven se nærmere på både likheter og distinkte forskjeller mellom de to, samt antyde noen tanker om kommende utvikling.

Hovedhypotesen i oppgaven er at *safety*-orienterte[6] samfunnssikkerhets- og beredskapsorganisasjoner benytter seg av ROS-modellen, samtidig som *security*-orienterte[7] aktører benytter VTS-modellen. Antagelsen baserer seg på at de premissgivende direktoratene i offentlig sektor gjennom lover, forskrifter og veiledere gir motstridende signaler med forskjellige regler som de pliktige må forholde seg til. Jeg ser derfor på ytre rammefaktorer og organisasjonsteoretiske forklaringer som *instrumentalisme* og *tvungen isomorfisme*. Direktoratet for samfunnssikkerhet- og beredskap (DSB) er fagmyndighet for blant annet sivil beredskap og kommunesektoren, hvor ROS-analyse er foretrukken modell for både tilsiktede og utilsiktede uønskede hendelser. Jeg vil foreløpig kategorisere "DSB-skolen" og kommunesektoren som *safety*-orienterte aktører. Nasjonal sikkerhetsmyndighet (NSM) er på sin side voktere av sikkerhetsloven som pålegger eiere av skjermingsverdige objekter og annen kritisk infrastruktur å analysere risiko og sette inn mottiltak for å beskytte verdiene mot *tilsiktede* handlinger. Jeg anser dermed "NSM-skolen" for å være *security*-orienterte aktører. Veiledningsmateriellet knyttet til gammel lov om forebyggende sikkerhetstjeneste med sine forskrifter favoriserte VTS-modellen, men etter at ny lov om nasjonal sikkerhet trådte i kraft i 2019 ble bildet litt mer uklart (kapittel 4). Jeg har likevel valgt å beholde hypotesen for å gå dypere inn og se hvor vi står og hvor veien går videre.

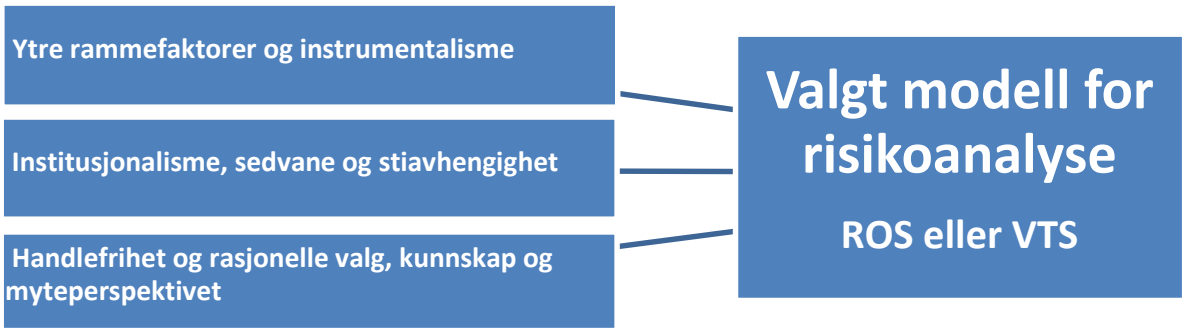
Foruten hoved hypotesen åpner jeg for en organisasjonsteoretisk forklaring hvor jeg vil undersøke om det er noen sammenheng mellom *institusjonalisme, stiavhengighet* og

[6]Med "safety-orientert" tenker jeg på organisasjoner som primært arbeider med sikkerhet- og beredskapsspørsmål knyttet til utilsiktede, uønskede hendelser, slik som uhell, materiellsvikt, ulykker, naturkatastrofer og HMS.

[7]Med "security-orientert" menes organisasjoner som i hovedsak arbeider med sikkerhet- og beredskap knyttet til tilsiktede/villede handlinger, eksempelvis terror, sabotasje, spionasje og kriminalitet. Det er ikke nødvendigvis noe sort/hvitt skille mellom slike organisasjoner, mange aktører beskjeftiger seg trolig med begge deler.

institusjonell isomorfisme hos aktørene. Isomorfisme innebærer at organisasjoner standardiseres og blir mer og mer lik hverandre, enten endringene skyldes tvunget, mimetisk (etteraping) eller normativ isomorfisme. Til sist vil jeg undersøke om aktørene har tilstrekkelig med ressurser og kompetanse til å gjøre et selvstendig, rasjonelt og kunnskapsbasert valg ut fra egen normativ vurdering. Dersom organisasjonene har tilstrekkelig med ressurser og handlefrihet ser jeg samtidig etter tegn på både normativ og mimetisk isomorfisme og ikke minst myteperspektivet fra ny-institusjonell teori.

For å komme fram til et vitenskapelig fundert svar på hovedspørsmålet vil analysen ta utgangspunkt i ulike former for organisasjonsteori og statsvitenskap, hvor hvert funn vurderes i lys av sikkerhetsteori, gjeldende lovverk, tidligere forskning og annen sekundærlitteratur. Valgt modell for risikoanalyse (ROS eller VTS) er oppgavens avhengige variabel, og jeg ser nærmere på hvilke uavhengige faktorer (variabler) som kan bidra til å forklare ulike valg.



Figur 1. Analysemodell

Ut fra denne analysemodellen kan vi utlede tre følgende hypoteser som ikke nødvendigvis er gjensidig utelukkende forklaringer på valg av risikomodell.

H_1 Overordnet myndighet eller ytre sektorkrav avgjør valg av analysemodell. Eksempelvis ved at samfunnssikkerhets- og beredskapsorganisasjoner underlagt DSBs myndighetsområde og regelverk benytter ROS metodikk. Samfunnssikkerhets- og beredskapsorganisasjoner underlagt NSMs myndighetsområde og regelverk benytter VTS metodikk. Denne hypotesen samsvarer med "top-down" policy, tvungen isomorfisme og begrenset rasjonalitet.

H_2 Valg av analysemodell skyldes sedvane eller andre institusjonelle forhold i organisasjonen, eksempelvis lokalkultur, stiavhengighet og "tykk" institusjonalisme ("sånn har vi alltid gjort det her"). Organisasjonen er fornøyd med etablert løsning og ønsker ingen endring. Hypotesen samsvarer med kulturperspektivet, normativ isomorfisme og begrenset rasjonalitet.

H_3 Aktørene har tilstrekkelig kompetanse, kapasitet og handlefrihet til å fatte selvstendige beslutninger basert på rasjonelle valg. De velger fritt mellom ROS, VTS eller andre modeller ut fra kunnskap, egen vurdering, egeninteresse og andre subjektive forhold. Hypotesen kan samsvare med myteperspektivet så vel som normativ og mimetisk isomorfisme.

Etter undersøkelsen av disse hypotesene vil jeg med utgangspunkt i datamaterialet fremstille noen *kvalitative observasjoner* som kjennetegner en god risikoanalyse, uavhengig av valgt modell. Til sist kan jeg presentere noen ideer om veien videre og forslag til videre forskning.

1.4 Oppgavestruktur

Oppgaven består av i alt seks hovedkapitler.

Kapittel 2 fremstiller det teoretiske grunnlaget for analysen hvor jeg spesielt legger vekt på instrumentalisme og kulturperspektivet fra ny-institusjonell teori, rasjonelle valg og de tre formene for isomorfisme.

Kapittel 3 presenterer metodevalg for datainnsamling og analyse. Jeg har valgt å triangulere mellom kvantitativ og kvalitativ metode i lys av teoriene og bakgrunnsinformasjonen, hvor en spørreundersøkelse danner grunnlaget for påfølgende intervjuer.

Kapittel 4 utgjør dokumentanalysen som oppsummerer bakgrunn for ROS og VTS slik de fremstår i dagens kontekst, sammen med et teoretisk grunnlag for disse modellene så langt dette er mulig. Her gjengis også komprimerte sammendrag av to norske risikostandarder og tidligere relevant forskning. Siden de fleste sikkerhets- og beredskapsorganisasjoner er underlagt sektorlovgivning presenteres et utdrag fra lover og forskrifter som direkte berører problemstillingen.

Kapittel 5 utgjør analysedelen som svarer ut de uavhengige variablene og hypotesene utledet fra problemstillingen i lys av teorivalget, samt kvalitative observasjoner.

Kapittel 6 utgjør oppsummerer hovedfunn og videre drøfting, konklusjon og forslag til videre forskning.

2. Teoretisk rammeverk

Bakgrunn for organisasjonsteorien

Klassisk organisasjonsteori baserer seg på en systematisk tilnærming til hvordan foretak skulle administreres og ledes. På begynnelsen av det tjuende århundret var Frederic Taylor sentral i diskusjonen om effektivisering av produksjonsbedrifter ut fra et ingeniørperspektiv. Taylor separerte intellektuelle oppgaver (brainwork) fra manuelle oppgaver på verkstedgulvet for å oppnå både rasjonalisering og spesialisering. Taylor ble kritisert for å undervurdere menneskelige faktorer som motivasjon og belønning for å holde produksjonen gående med tungt og "hjernedødt" arbeid i bytte mot middelmådig lønn. Taylors "Scientific Management" blir likevel fortsatt hyppig referert og regnes som en forløper til samtidens bedriftsøkonomi og organisasjonsteori (Eriksson-Zetterquist, Kalling, Styhre og Woll, 2014, s. 48).

Innen offentlig sektor er det spesielt Max Webers beskrivelse av det rasjonelle byråkratiet som har bidratt til å påvirke vårt syn på offentlige organisasjoner. Dette handlet blant annet om embetsverkets lojalitet til samfunnsoppgaven ut fra et instrumentelt perspektiv, ved at byråkratiet er underlagt styring fra politiske myndigheter. Mye av Webers tankesett dreide seg videre om likebehandling ovenfor innbyggere på tilsvarende saker, standardisering av repeterende arbeidsoppgaver og spesialisering av kompetanse knyttet til kompliserte oppgaver. På innsiden var byråkratiet veldig regelstyrt, men systemet viste å motivere den lojale tjenestemannen ved å legge til rette for opprykksmuligheter i et internt hierarki, basert på prestasjoner eller ansiennitet (Eriksson-Zetterquist et. al. S. 67-77).

Det ny-institusjonelle organisasjonsperspektivet utviklet seg fra 1970-tallet, med vekt på at organisasjoner påvirkes av egne normer, fagtradisjoner og verdier slik at de ikke kan styres eller forandres like lett som det antydes under det instrumentelle perspektivet. Christensen, Egeberg, Lægreid, Roness og Røvik forklarer organisasjonsperspektivet med utgangspunkt i et instrumentelt perspektiv, et institusjonelt kulturperspektiv og et institusjonelt myte/moteperspektiv (2017). I en utvidelse av det instrumentelle perspektivet har jeg inkludert Michael Hills Public policyprosess fra statsvitenskapen og tvungen isomorfisme, siden de tre perspektivene gir samsvarende effekt for de organisasjoner som berøres av min analyse.

I løpet av 1990-årene ble studiet av organisasjoner og byråkrati aktualisert på nytt gjennom post-byråkratiske organisasjonsformer og ny-institusjonell teori, for eksempel ved å se på prosjektorganisasjonen. Jonas Söderlund (2007) beskriver prosjektet som organisasjonsform i

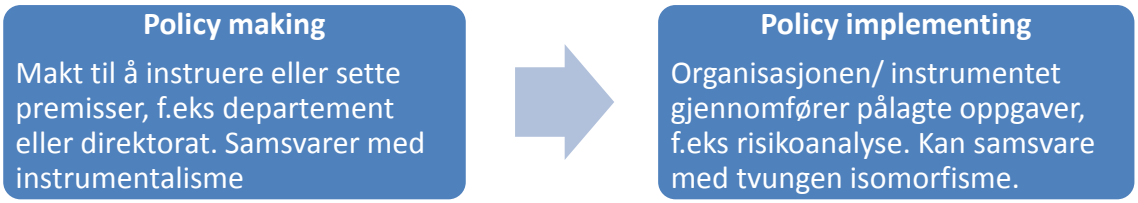
sin bok, basert på røttene fra det klassiske byggeprosjektet og frem til dagens mangfoldige og til dels sterkt institusjonaliserte organisasjoner som etableres, leverer og deretter termineres.

I de følgende delene av teorikapittelet presenteres perspektiver som ligger direkte til grunn for analysen, jamfør problemstillingen og uavhengige variabler/hypoteser.

2.1 Ytre rammefaktorer og instrumentalisme

Det instrumentelle perspektivet tar utgangspunkt i at organisasjonen lojalt utfører oppgaver på samfunnets vegne. Organisasjonen kan oppfattes som et redskap eller et instrument som blir brukt for å oppnå visse mål (Christensen et al. 2017, s. 34). Det instrumentelle perspektivet samsvarer samtidig godt med top-down perspektivet i Michael Hills "Public Policy prosess", som fastslår at organisasjonen plikter å utføre de vedtak som følger av styringsrelasjon fra overordnet nivå, herunder lover og forskrifter. Implementering forstås som en operasjonell handling for å realisere de gitte beslutningene, enten det dreier seg om kjerneoppgaver (for eksempel levere offentlige tjenester til innbyggerne) eller sekundæroppgaver (eksempelvis gjennomføre pålagte risikoanalyser). Pressman og Wildavsky la følgende definisjon til grunn; Implementering er å utføre, oppnå, oppfylle, produsere eller fullføre en policy, noe som er blitt vedtatt. Verbet "implementere" er en konsekvens av "policy" (Hill, 2014, s. 206-207).

For å underbygge samsvaret mellom det instrumentelle perspektivet og policyprosessen har jeg satt som premiss at den som har vedtatt policyen har direkte eller indirekte makt ovenfor de som skal fullbyrde vedtaket. En slik hierarkisk styringsrelasjon beskrives av Høyer, Kasa og Tranøy (2016, s. 55-57). Styringsrelasjon kan for eksempel dreie seg om eierdepartements makt til å vedta politikk eller oppgaver som underliggende organ (eksempelvis direktorat, sektor eller kommune) plikter å oppfylle gjennom styringen. På samme måte kan styringsrelasjonen beskrive et premissgivende direktorats makt til å instruere eller påvirke aktiviteter hos underliggende organisasjoner innen sin sektor. Sett i sammenheng med øvrige ny-institusjonelle fenomen er også *prosjektet* et typisk utrykk for implementering, ved at en prosjekteier (policymaker) delegerer ansvaret for gjennomføring av oppgavene innenfor en gitt tidsramme, budsjett og beskrevne kvalitetskrav (Andersen, 2005). Med overføring til dagens situasjon samsvarer styringsrelasjonen for eksempel med departementenes årlige tildelingsbrev til sine underliggende direktorater, etater eller fylker/kommuner.



Figur 2. Sammenhengen mellom policyprosessen, det instrumentelle og tvungen isomorfisme.

Som det fremgår av figuren setter jeg videre tvungen *isomorfisme* i sammenheng med det instrumentelle perspektivet og policyprosessen. Dette henger blant annet sammen med at Lov om kommunal beredskapsplikt eksplisitt pålegger kommunene å gjennomføre helhetlige risiko- og sårbarhetsanalyser (ROS). Kommunens handlefrihet til å eventuelt velge en annen tilnærming til risikoanalyse er i lys av policyprosessen svært begrenset. Men pålegget om at kommunene skal gjennomføre ROS kan også forstås som et hensiktsmessig standardiseringstiltak som skal forhindre at 356 forskjellige kommuner (antallet pr. 2020) løser den samme oppgaven på like mange måter. Når lovteksten pålegger kommunene å analysere risiko ut fra ROS samsvarer et slikt krav og standardisering med definisjonen på tvungen isomorfisme. Dette uansett hvorvidt standardiseringen gjøres av praktiske årsaker eller fordi lovgiver anser ROS-modellen for å være normativt best egnet for analyse i kommunesektoren (se ellers punkt 4.4).

2.2 Institusjonalisme og stiavhengighet, kulturperspektivet

Det institusjonelle perspektivet åpner for at organisasjoner påvirkes av indre og egne normer, fagtradisjoner og verdier slik at de ikke kan styres eller forandres like enkelt som det antydes under det instrumentelle perspektivet. Det institusjonelle perspektivet kan deles inn i organisasjonskultur og myte/moteperspektivet.

Kulturperspektivet baserer seg på at organisasjoner formes og utvikles av stadige prosesser mellom menneskene i organisasjonen, eller tilsvarende mellom organisasjoner som samarbeider. At organisasjonen er "institusjonalisert" viser til at de leverer sine tjenester tilnærmet likt, uavhengig av tid og rom. "Alle" i organisasjonen vet hvilket ansvar og plikter som skal utføres, både ved normaldrift og i krisesituasjoner. Et eksempel ser vi på sykehuset. Alle på institusjonen vet hvilke ulike roller som legen, kirurgen, sykepleieren, ambulansearbeideren og renholdsarbeideren skal fylle i de ulike situasjonene, nettopp fordi oppgavene er instituert og tillært ved sosialisering, opplæring, rutinefastsetting og repetering.

Ved at oppgavene kan utføres på automatikk er organisasjonen institusjonalisert og mye kan gjøres på vane. Et utrykk som blir brukt på veldig innarbeidede organisasjoner er "tykk" institusjonalisme. Organisasjonen blir nærmest et "levende" vesen, hvor verdiene, normene og handlingsmønsteret sitter i "veggene", uavhengig av hvem som fratrer eller blir ny-ansatt. En fersk leder som kommer til en slik organisasjon med et instrumentelt utgangspunkt vil møte på utfordringer ved å innføre selv de enkleste forandringer, fordi gamle vaner er vonde og vende. Jeg undersøker om institusjonalisert sedvane med løsninger eller holdninger innarbeidet over tid fører til at andre måter å gjøre risikoanalyse på ikke blir vurdert så lenge gamle måten fungerer bra for de som bruker den. En slik tilnærming kan også samsvare med begrenset rasjonalitet og satisfisering.

Stiavhengighet. En organisasjon som på et tidligere tidspunkt brukte ressurser på et veivalg har ikke all verdens overskudd til å tenke over saken på nytt og vurdere alternative handlemåter hver gang en alternativ mulighet viser seg gjeldende. Det kan også tenkes at det forrige veivalget var godt gjennomtenkt, og at organisasjonen ikke prioriterer samme beslutningsprosess på nytt. Stiavhengighet kan selvfølgelig forklares mer bokstavelig. Dersom du har valgt *en* bestemt sti i skogen og befinner deg godt ut i løypa, så vil du neppe gå tilbake til startpunktet for å bytte til en annen sti. For å sitere March og Simon (1993, s. 17): "Ours is a path-dependent world in which small steps are easily escalated into irreversible, or nearly irreversible, commitments".

Selv små skritt i en bestemt retning gjør det vanskelig å endre kursen. Jeg vil undersøke om også stiavhengighet kan forklare organisasjoners valg av modell for risikoanalyse og ser fenomenet i sammenheng med både institusjonell sedvane og begrenset rasjonalitet.

2.3 Det institusjonelle myteperspektivet

Et nøkkelresonnement for myte/moteperspektivet er at organisasjoner befinner seg i institusjonelle omgivelser under påvirkning av sosialt skapte normer. Gjennom slike prosesser blir organisasjoner mer like hverandre, i alle fall på overflaten. De sosialt skapte normene kalles myter. Mytene kan være brede og innrettet for mange typer organisasjoner, eller smale, ved at de representerer presise oppskrifter rettet inn mot spesifikke deler av organisasjonen eller en avgrenset gruppe virksomheter. Myter spres raskt gjennom imitasjon og de kan tas inn i organisasjoner også uten at de nedfelles i organisatorisk praksis. Sosiologen Talcott Parson

var en av de første som så at organisasjoner ikke bare var effektivitetsorienterte, de søker også legitimitet fra omgivelsene ved å leve opp til modernitetsnormer som kontinuerlig framskritt, fornyelse og rasjonalitet. Myteperspektivet viser dermed hvordan organisasjoner forsøker å styrke sin legitimitet eller posisjon ved å skape et inntrykk av at de gjør innovative forandringer, basert på aktørenes virkelighetsoppfattelse om hva som er meningsfullt.

> En myte er altså en legitimert oppskrift på hvordan man bør utforme utsnitt eller deler av en organisasjon. Det er en oppskrift som gjerne begeistrer eller vekker oppmerksomhet, og som har en forbilledlig status for flere organisasjoner…. Rasjonaliserte myter har to viktige kjennetegn. For det første presenteres de gjerne som svært effektive redskaper som organisasjoner kan bruke for effektiv måloppnåelse. At myten er rasjonalisert innebærer at det ved hjelp av vitenskapslignende argumentasjon er skapt en overbevisning om at den er et effektivt virkemiddel for å oppnå bestemte organisatoriske mål. (Christensen et al. 2017, s. 76-77).

Kjell Arne Røvik utdyper fenomenet i sin avhandling om reformer: "Siden mytene er tidsriktige fremstår de gjerne som moter, noe "alle" skal ha inntil de går av moten" (Moren, 2011, s. 52). I videre forstand ser vi at institusjonaliserte myter i prinsippet kan representere alt fra tunge offentlige reformbølger som "New Public Management" og ned til avgrensede oppskrifter, som det populære effektiviseringsverktøyet "Lean". Jeg vil undersøke om myteperspektivet bidrar til å forklare valgt modell for risikoanalyse i Norge. Her er det spesielt interessant å se på VTS-analysen som kom friskt på banen i 2014, med 22. juli (2011) og Gjørv-rapporten (2012) som bakteppe.

2.4 Rasjonalitet, kunnskap og handlefrihet

Essensen av rasjonelt valg innebærer at når aktørene står ovenfor flere forskjellige måter å gjøre ting på, vil de vanligvis velge de løsningene som trolig gir best mulig utfall. Forutsetningen er at individene besitter rasjonell kapasitet, tid og emosjonell objektivitet til å velge en løsning som samsvarer med ønsket sluttilstand (Marsh og Stoker, 2002, s. 65-69). Teorien bygger dermed på antagelsen om at menneskene kan kalkulere seg fram til et optimalt utbytte og fatte beslutninger deretter. Simon skiller mellom rasjonelle og ikke-rasjonelle beslutninger hvor sistnevnte innebærer at det ikke tas hensyn til relevant informasjon. Videre skiller han mellom objektive- og subjektive rasjonelle beslutninger, fordi en beslutning alltid vil være farget av hvem som tar den. Dermed finnes det ikke perfekte beslutninger siden dette

innebærer optimal kunnskap om alle forutsetningene som påvirker den. Beslutningen kan dermed bli tilfredsstillende (*saticfying*), (Eriksson-Zetterquist et. al 2015, s. 119).

Begrepet formålsrasjonalitet skiller mellom *fullstendig* og *begrenset* rasjonalitet. Fullstendig rasjonalitet er gjeldende i de situasjoner hvor gruppen eller organisasjonen har full oversikt over all relevant informasjon, og dermed er i stand til å fatte optimale beslutninger. Studier viser imidlertid at spesielt komplekse organisasjoner sjelden har oversikt over alle innfallsvinkler og fakta når beslutningen tas. Siden informasjonsgrunnlaget har mangler eller målene kan være ufullstendig, blir det rasjonelt å bruke beslutningsregler basert på *satisfisering*. Enkelt forklart vil organisasjonen fatte beslutninger som er gode nok til å oppnå hensikten, gitt tilgjengelig informasjon og tid til rådighet. Beslutninger basert på begrenset rasjonalitet har samtidig preg av konsekvenslogikk (Christensen et al. 2017, s. 37). Begge deler handler om å ta best mulig beslutning ut fra de rådende omstendigheter. Jeg vil undersøke i hvilken grad rasjonelle valg kan forklare organisasjoners valg av ROS- eller VTS-modell.

Handlefrihet

Cyert og March ser på organisasjoner som informasjonsbearbeidende og beslutningstakende systemer (ibid, s. 120). Det innebærer i praksis at organisasjonene bearbeider tilgjengelig informasjon og tar rasjonelle beslutninger basert på optimal eller begrenset rasjonalitet. Valget vil basere seg på et informasjonsgrunnlag, men beslutningen om å gjennomføre et rasjonelt valg forutsetter at organisasjonen har tilstrekkelig frihet til å kunne velge og til å gjennomføre det som de selv ønsker (handlefrihet). Ledelseslitteraturen forutsetter at det er en positiv sammenheng mellom handlingsrom (autonomi) og innflytelse (makt), (Espedal og Kvitastein 2012). Graden av handlefrihet avhenger følgelig av de avklaringer som er gjort i styringsdialogen mellom nivåene, jamfør policyprosessen. Resultatene fra innsamlede data indikerer at organisasjoner som har tatt selvstendige valg av risikomodell (ROS eller VTS) innehar relativt stor grad av handlefrihet.

2.5 Isomorfisme

Grupper eller organisasjoner tilpasser seg omgivelsene i en vekselvirkning mellom seg selv og omgivelsene. Dette skaper tilpasninger slik at organisasjonene blir mer og mer like hverandre. Jo sterkere kobling mellom organisasjonen og omgivelsene, desto større grad av isomorfisme (DiMaggio og Powell, 1983).

Institusjonell isomorfisme fører til at organisasjoner i større grad overlever og blir framgangsrike. Blant annet styrkes samhandlingen gjennom utvikling av et felles vokabular og metodikk. Et eksempel på dette er om en bestemt tekniker skal inn hos en annen virksomhet for å gjøre en bestemt type arbeid. Dette innebærer ikke nødvendigvis at man vet eksakt hva som vil skje, men ut fra et felles vokabular får man en forklaring på aktiviteten som skal gjøres. Isomorfisme har ikke noen direkte sammenheng med effektivisering, men organisasjonene oppnår i praksis gode effektivitetseffekter ved at de blir mer kompatible og snakker samme språk. Institusjonell isomorfisme kan også innebære at organisasjonen legger en form for standard til grunn for en bestemt type arbeidsprosess, for eksempel fra The International Organization for Standardization (ISO) eller Norsk standard (NS). Jeg ser spesifikt på både NS 5814 (norsk ROS-standard) og NS 5832 (norsk VTS standard) som del av studien.

Tvungen isomorfisme utvikles først og fremst gjennom politisk påvirkning ved at sterke organisasjoner pålegger svakere organisasjoner innenfor det samme feltet å tilpasse seg gitte formelle og uformelle krav. Et eksempel kan være når staten krever at en bedrift skal tilpasse seg en ny teknikk eller metode for å nå bestemte mål, for eksempel formatet for innlevering av offentlige anbud (Digitaliseringsdirektoratet, 2020). Dersom en virksomhet skal tas i betraktning som tilbyder i et offentlig anbud må prosedyren gjennomføres nøyaktig på den måten som staten har bestemt. Jeg har i min studie likestilt tvungen isomorfisme med det instrumentelle perspektivet og public policy prosessen (top-down), siden utfallet har samme konsekvens for de som blir styrt på valg av analysemodell av en ytre premissgiver med sterkere maktposisjon enn egen organisasjon.

Imiterende (mimetisk) isomorfisme oppstår gjennom usikkerhet eller mangel på ressurser til å utrede seg fram til den beste løsningen. I stedet for å finne opp "kruttet" på nytt kan man likeså godt etterligne øvrige fremgangsrike organisasjoner som allerede har gått opp samme løypa. På denne måten tror man selv at man blir like framgangsrik som "inspiratoren" og vinner en viss legitimitet i feltet. Den organisasjonen som virker som modell for "imitatoren", er ikke alltid klar over dette selv.

Normativ isomorfisme utvikles først og fremst gjennom profesjonalisering av bransjene, for eksempel ved at de ansetter folk med en standardisert utdanningsbakgrunn eller tilfører en omfattende og uniform grunnopplæring ved tiltreden, (Eriksson-Zetterquist et al. 2014, s. 254-255). Også her ser jeg paralleller til NS standardene for ROS/VTS-analyse respektivt.

2.6 Oppsummering, teorivalg

Analysen vil dermed basere seg på følgende teoretiske perspektiver:
- Ny-institusjonell teori i form av instrumentalisme, institusjonalisme og myteperspektivet.
- Tvungen, normativ eller mimetisk isomorfisme.
- Rasjonelle valg-teorier, kunnskap (informasjon) og handlefrihet.

Teoriperspektivene er valgt fordi jeg ønsker å forklare hvilke faktorer som kan være bestemmende for valg av henholdsvis ROS eller VTS for risikoanalyse. Det er sjelden bare en forklaring på hvert fenomen, følgelig er det en fordel å basere seg på et bredt teorirepertoar. Det ligger dermed flere alternative forklaringsperspektiv til grunn for hver hypotese.

H_1-hypotesen antar at det er ytre rammefaktorer som styrer valget av analysemodell. Analysen gjøres i lys av instrumentalisme, tvungen isomorfisme og begrenset rasjonalitet.

H_2-hypotesen antar at valget av analysemodell skyldes sedvane eller andre institusjonelle forhold. Analysen gjøres i lys av institusjonalisme og stiavhengighet fra kulturperspektivet, samt normativ isomorfisme og begrenset rasjonalitet.

H_3-hypotesen antar at valget av analysemodell kan forklares som et rasjonelt valg basert på kunnskap (informasjon) og handlefrihet, sett i lys av rasjonelle valg-teorier, det institusjonelle myteperspektivet og normativ og mimetisk isomorfisme.

3. Metode

I dette kapittelet vil jeg gjøre rede for forskningsdesign og metodevalg, samt begrunne de valg som er gjort. Studien har en kvalitativ hovedtilnærming men inkluderer et kvantitativt tilsnitt som øker breddeperspektivet. Studien baserer seg på triangulering av forskjellige metoder. Analysen (kapittel 5.) bygger på en kombinasjon av sekundær- og primærkilder, hvor de sistnevnte er basert på både kvantitativ- og kvalitativ datainnsamling.

3.1 Forskningsdesign og metodevalg

Innenfor samfunnsvitenskapene er det vanlig å skille mellom kvantitative og kvalitative forskningsmetoder. De metodiske tilnærmingene har ulike tradisjoner og anerkjennelse i forskningsmiljøene. I dag er det imidlertid en utbredt oppfatning om at samfunnsforskere ser på valg av metode ut fra hensiktsmessighet (Ringdal, 2000, s. 107). Formålet med denne studien er å nå frem til "sikkerhets- og beredskapsmiljøene i Norge". Gruppen er ikke homogen, men tvert imot sterkt fragmentert og lite definerbar. Noen jobber i staten som består av dusinvis av departementer, direktorater og underliggende etater. Andre jobber i kommunene, men her finnes det hundrevis av forskjellige, spredt over hele landet. I tillegg så har vi et utallige private næringer fordelt på smått og stort, hvor noen av de i større eller mindre grad analyserer sin egen risiko etter langt på vei de samme standardene. Fordelingen av aktuelle profesjonsutøvere, både organisasjonsmessig og geografisk er total. Samtidig er det også stor forskjell på kulturene, både mellom stat, kommune og privat, men også innad i disse gruppene. Er egentlig beredskapskoordinatoren i Engerdal en del av det samme kulturfellesskap som beredskapskoordinatoren i Bergen? Og er en statsansatt sikkerhetsrådgiver i et tilfeldig direktorat en del av samme "risikomiljø" som en tilsvarende sikkerhetsrådgiver i en helt annen etat? Neppe. Begrepet "miljø" er i all hovedsak en sosial konstruksjon.

Erling Andersen forklarer at virkeligheten, eller kunnskapene om virkeligheten blir konstruert av betrakteren, som er preget av sin bakgrunn. "Sosial" i denne betydning kan for eksempel romme utdanning og erfaringer. Man anlegger et perspektiv for å kunne forstå. I henhold til den sosiale konstruktivismen innebærer dette at man skaper virkeligheten. "Perspektivet blir altså ikke bare forklarende, men også skapende" (Andersen, 2005, s. 10).

"Sikkerhets- og beredskapsmiljøene i Norge" er dermed en sosial konstruksjon og ingen konsistent gruppe. Hvem som inngår i perspektivet avhenger av øyet som ser. For å legge på ytterligere en dimensjon til kan vi samtidig trekke frem begrepet *policynettverk*, som beskriver hvordan uformelle mekanismer for ideskaping kan eksistere ved siden av formelle institusjoner som et parallelt rammeverk (Marsh og Stoker, 2002, s. 99). Med andre ord kan et policynettverk bestå av personer som kan tenkes å ha lignende kompetanse, tankesett og holdninger omkring risikoanalyse, selv om disse befinner seg i forskjellige organisasjoner. For eksempel basert på at de muligens kan ha lignende utdannings- eller erfaringsbakgrunn.

3.2 Triangulering

En kombinasjon av kvalitative og kvantitative data i et flermetode-design kalles for *triangulering*. Det kan for eksempel skje ved at feltarbeid blir brukt som en forundersøkelse før en kvantitativ hovedundersøkelse (Ringdal 2001, s. 115). For å se nærmere på min problemstilling trianguleres jeg mellom flere ulike metoder, men på en litt annen måte enn i eksempelet over. Jeg valgte å bruke surveydesign med nettverksrekruttering etter *snøballmetoden*, etterfulgt av semi-strukturerte dybdeintervjuer. Snøballmetoden beskriver en utvalgsmetodikk hvor et antall "førstekontakter" fanger opp ballen og ruller den videre, slik at forskeren får tips om stadig nye informanter. I følge Vassenden og Andrews er metoden utbredt i "studier av sosiale nettverk, i studier med ukjent univers, og i studier hvor det ellers er vanskelig å rekruttere tilstrekkelige utvalg før studien starter" (Tjora, 2012, s. 151). I og med at populasjonen jeg søker å nå frem til består av geografisk spredte enkeltpersoner i forskjellige organisasjoner innenfor det norske "universet" kan vi i dagens samfunn benytte sosiale medier og annen digital kommunikasjon.

Risikoanalyse kan oppfattes som et ganske lukket, men samtidig tverrfaglig område som er teoretisk komplekst og samtidig praktisk og konkret orientert. Det kan være krevende å nå frem til personer som faktisk inngår i målgruppen. Jeg valgte dermed å innlede datainnsamlingen med et dokumentstudium, spisset mot problemstillingen og den påfølgende innsamling av primærdata. Spørreundersøkelsen kunne designes deretter.

3.2.1 Dokumentstudier

Dokumentstudier er en vanlig måte å generere kvalitative data på. Dette innebærer at vi "i hovedsak bruker dokumenter som er produsert for andre formål enn forskning" (Tjora, 2112, s. 162). Det er typisk for dokumentstudier å bruke de som bakgrunnsdata, men noen velger også å gjøre rene dokumentstudier. Dokumentene kan være *casespesifikke*, *generelle*, fra *medier* eller de kan være *forskningsdokumenter*. Det vesentlige poenget er at de gir oss informasjon om det saksforholdet som skal belyses, ofte med tanke på spesifikke lesere, og satt inn i en kontekst (Tjora 2012, s. 163).

Dokumentstudier betraktes som *ikke-påtrengende metoder* og er velegnet til å redusere belastningen på deltakerne. For min del handlet dette om respekt ovenfor de ressursene som var villige til å bli med og dele av sin kunnskap. Uten grunnlag i dokumentstudiene ville det blitt vanskelig å utforme spørreundersøkelsen eller intervjuguiden med overveide og fagspissede spørsmål og formuleringer. Interessen for å delta kunne blitt tilsvarende dårligere.

For å berede grunnen for innsamlingen av primærdata innledet jeg forskningsprosessen med å se nærmere på selektert litteratur og annen bakgrunnsinformasjon med relevans for å opplyse problemstillingen. Denne delen utgjør dermed et skreddersydd og ikke minst tidsaktuelt grunnlag for den påfølgende analysen i kapittel 5. Dokumentstudien gjengis i kapittel 4.

3.2.2 Spørreundersøkelse

Survey-design er det mest brukte design innenfor samfunnsvitenskapene (Ringdal 2001, s. 257). Min intensjon var å samle synspunkter fra mennesker i sikkerhets- og beredskapsmiljøene for å finne ut hvorfor de benytter de ulike modellene. Ved å bruke spørreskjema treffer jeg langt flere representanter for miljøene enn hva som ville vært tilfellet utelukkende med intervju eller andre kvalitative metoder. Samtidig ville jeg nå ambisjonen om full metodetriangulering, noe som styrker både bredden og dybden i studien.

Etter å ha vurdert kommersielle innsamlingsverktøy falt valget på Nettskjema som disponeres av Høgskolen i Innlandet etter avtale med Universitetet i Oslo. Dette fordi Nettskjema ansees som det sikreste verktøyet. Anonymiteten på min undersøkelse ble tydeliggjort i innledningsteksten, og senere repetert i en egen tekstboks hvor respondenten måtte ta et aktivt valg om å avgi elektronisk samtykke for å delta i undersøkelsen, uten at personopplysninger

oppgis eller lagres. Til tross for at hensikten utelukkende var samling av anonyme data som ikke er søknadspliktig til Norsk senter for forskningsdata (NSD), sikret jeg likevel at forskningen overholdt krav knyttet til Personvernforordningen (GDPR), (NSD, 2020).

Menneskene i målgruppen har det til felles at de utfører eller kjenner til risikoanalyse ved bruk av ROS eller VTS-modellen. For å treffe populasjonen best mulig valgte jeg å lansere undersøkelsen gjennom spesifikke grupper på sosiale medier, samt annen digital kommunikasjon. Målsetningen var nettverksrekruttering gjennom *snøballmetoden*. Jeg designet dermed et "åpent" spørreskjema som i prinsippet hvem som helst kunne klikke seg inn på og sende inn. For å innsnevre til aktuelle personer som faktisk har kunnskapene kommuniserte jeg tydelig hvem som inngår målgruppen, med avgrensninger. Videre ble det brukt et språk med fagterminologi, slik at øvrige publikum i mindre grad ville føle seg kallet til å svare.

Spørreundersøkelsen ble lansert den 6.1.2020 med en tilpasset motivasjonstekst i følgende fora:

- Facebook-gruppen "*Beredskapsledelse*", 469 medlemmer
- Facebook-gruppen "*Samfunnssikkerhetsfaglig forum*", 2154 medlemmer
- Facebook-gruppen "*Næringslivets sikkerhetsråd*", 2185 medlemmer
- Facebook-gruppen "*MPA 13*" fra Høgskolen i Innlandet, 45 medlemmer hvor anslagsvis 15 av disse har kjennskap til risikoanalyse
- LinkedIn-gruppen "*Security Norway – Sikring i Norge*", 228 medlemmer
- Åpen kunngjøring på personlig LinkedIn profil med 285 forbindelser, hvor anslagsvis 50 individer kan tenkes å ha kjennskap til risikoanalyse
- E-post til et trettitalls rådgivere og ledere som kan tenkes å ha kjennskap til risikoanalyse i egen organisasjon.
- Epost, SMS eller chat-melding til et tjuetalls selekterte enkeltpersoner i eget nettverk.

Undersøkelsen har dermed teoretisk nådd 5151 mulige respondenter i målgruppen som i bestefall vil rekruttere nye deltakere. Siden det kan være til dels stor overlapp av personer som befinner seg i flere av de samme gruppene og videre at veldig mange skroller uinteressert forbi en melding når den dukker opp, anslår jeg at kunngjøringen nådde ut til maksimalt 3000 potensielle respondenter, kanskje færre. Fra disse har det kommet inn 138 fullførte besvarelser, som utgjør en teoretisk svarprosent på 4,6%. Av hensyn til avgrensninger på prosjektet har jeg ikke foretatt T-test, khikvadrattest eller signifikanstest for å undersøke korrelasjon mellom

utvalg og populasjon (Johannesen 2008, s. 129). Tatt i betraktning at målgruppen er en sosial konstruksjon bestående av ukjent antall enkeltindivider, og videre at spørreundersøkelsens relativt sett har gitt en god deltagelse vil jeg anslå at representativiteten er meget god. Da undersøkelsen pågikk observerte jeg at den prosentvise svarfordelingen holdt seg forholdsvis stabilt allerede fra dag 2 hvor den hadde svar fra 40 respondenter. Fra om lag 100 respondenter og opp til avslutningen med 138 fullførte besvarelser den 20.1.2020, var det kun marginale bevegelser på prosentvis fordeling. Undersøkelsen kunne dermed trolig blitt betraktet som representativ for denne populasjonen, også med en lavere svarprosent. Kvantitative rådata er i alle tilfeller digitalt lagret, slik at signifikansnivået er etterprøvbart.

Hvordan kan vi så vite at respondentene faktisk tilhører sikkerhets- og beredskapsmiljøene, og hvordan identifisere "spam" eller useriøse besvarelser? Undersøkelsens Del I dreide seg utelukkende om fagspesifikk terminologi, og siden det også her kan være delte meninger la jeg opp til flere mulige svaralternativer på noen av spørsmålene, slik at mer enn ett svar kunne betraktes som korrekt.[8] Som en "kontroll" på respondentenes kunnskapsnivå ville jeg vurdere i hvilken grad de kunne skille på endel begrep som typisk diskuteres i miljøene, hvor de faglige definisjonene ikke nødvendigvis er godt kjent i befolkningen for øvrig. Disse begrepene var:

"sikkerhet" vs "beredskap"
"safety" vs "security"
"risiko" vs "trussel".

Sikkerhetsdefinisjonen er i seg selv utfordrende og distinksjonen mellom safety og security er flertydig, også i norsk faglitteratur (se kapittel 4). Jeg endte likevel opp med 91.9 % "korrekte" svar på spørsmål 4 om definisjon på "security". På spørsmål 5 om definisjon på "beredskap" fikk jeg 100% "korrekt" besvarelse. Til sist var det 94,9 prosent av de spurte som oppga at begrepene "risiko" og "trussel" hadde forskjellig betydning. Antall "feilbesvarelser", om vi kan bruke et sånt utrykk var dermed lavere enn 10 %. Jeg fastslår dermed at deltakerne i all hovedsak var personer med god kjennskap til fagområdet. Betraktingen bekreftes av et stort antall innsiktsfulle replikker i de åpne kommentarfeltene, samt den erfaring og utdanningsnivå

[8] "Fasitsvarene" angitt til spørreundersøkelsens del I er basert på definisjoner hentet fra NOU 2006:6, Store Norske Leksikon og Sikringshåndboka (2017).

som respondentene oppga på demografidelen. Gjennomsnitts-respondenten har oppgitt mer enn 20 års erfaring i faget og utdanning på mastergrads-nivå.

Datagrunnlaget som reelt sett inngår i analysen baserer seg på undersøkelsens del II (ROS) og del III (VTS), i tillegg til de kvalitative observasjonene som er hentet fra del IV. Basert på disse resultatene fikk jeg et veldig godt utgangspunkt for intervjuene og påfølgende analyse.

Tilbakemeldingene jeg mottok underveis og etter spørreundersøkelsen tyder på at det har vært stor interesse for studien i miljøene. Av hensyn til transparens, etterprøvbarhet og eventuelt videre forskning er resultatene fra spørreundersøkelsen kunngjort i sin helhet sammen med studien (Vedlegg I). Kvantitativt datagrunnlag kan utleveres etter forespørsel.

3.2.3 Semi-strukturerte intervju med nøkkelinformanter

> If you want to know how people understand their world and their lives, why not talk to them?

Sitatet introduserer boken Interviews av Kvale og Brinkmann som vektlegger samtalen som grunnleggende for menneskelig interaksjon (2009, s. 102). I en studie med en spisset problemstilling er det utelukkende fagsterke ressurspersoner fra sikkerhets- og beredskapsmiljøene som har noe å bidra med for å opplyse problemstillingen. Å gjennomføre intervjuer med nøkkelinformanter er også typisk for slike studier (Fangen, 2010, s. 188). Informantene som deltok hadde begge vært synlige i fagmiljøene gjennom mange år og ble spesielt valgt på grunnlag av fremragende kompetanse på risikoanalyse. Siden spørreundersøkelsen allerede hadde gitt verdifulle data var det mulig å redusere antallet til to personer med ekspertkompetanse på henholdsvis ROS og VTS.

Som et bidrag til å styrke etterprøvbarheten samtykket begge informantene til å stå fram med navn og publisering av intervjureferatene sammen med studien (Vedlegg II og Vedlegg III). Denne delen av prosjektet var dermed meldepliktig til NSD. Som en del av godkjenningen formulerte jeg på forhånd et informasjonsskriv i lys av personvernlovgivningen, sammen med samtykkeerklæringen som var basert på NSD sitt malverk (Vedlegg IV). NSD vurderte prosjektet som godkjent den 17.1.20, slik at intervjuene kunne iverksettes påfølgende uke (Vedlegg V). Samtykkene ble underskrevet av informant ved intervjuets oppstart.

Intervjuprosessen tok utgangspunkt i Kvaale og Brinkmanns syvtrinnsprosess (2009, s. 123-141). Siden intervjuene ble gjennomført i etterkant av spørreundersøkelsen var det mulig å

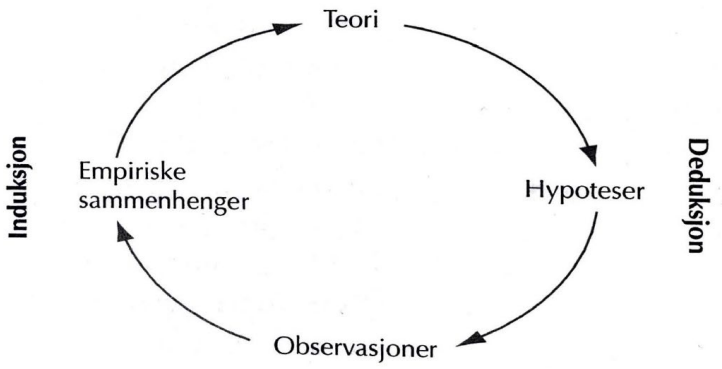
finjustere intervjuguiden i lys av resultatene, for å fange opp supplementær informasjon med økt dybdeperspektiv. For å tydeliggjøre at intervjuene bygget videre undersøkelsen i en triangulert studie delte jeg resultatene fra spørreundersøkelsen (uten fritekstkommentarer) med informantene forut for møtet, sammen med en intervjuguide på 10 spørsmål.

Intervjuene tok utgangspunkt i semi-strukturert metode med mulighet for dialog og refleksjon, også litt på siden av spørsmålene. Begge intervju ble gjennomført ved personlig møte på informantens respektive arenaer. Det ene intervjuet ble etter avtale notert direkte inn på en dokumentkladd fra PC, med påfølgende e-postoppfølging av teoretiske figurer som inngikk i intervjuet. Det andre intervjuet ble gjennomført med båndopptaker, etterfulgt av transkripsjon. Samtlige direktesitat og begge intervjureferat ble individuelt kommunisert og godkjent. Av hensyn til personvernforordningen og NSD-avtalen om å begrense omfanget av personopplysninger til navn og posisjon ble lydopptaket permanent slettet på det tidspunktet respondent hadde godkjent sitt intervjureferat.

3.3 Hypotetisk deduktiv metode og operasjonalisering

Kristen Ringdal beskriver vitenskapelig kunnskap som generelle utsagn eller teorier som er generalisert fra empiriske observasjoner. Dette innebærer at kunnskapen bygger på induksjonsprinsippet, eller slutninger fra observerte regelmessigheter til generelle teorier eller lovmessigheter (indiksjon). Å begrunne vitenskap bare på induksjon er imidlertid problematisk, siden slutningen kan være feil (Ringdal 2000, s. 57).

Ut fra Karl Poppers vitenskapssyn er *falsifiserbarhet* nøkkelen til vitenskapelig prøving og feiling. Vitenskapen vokser etter hvert som teorier forkastes og nye, bedre teorier formuleres. En grunnleggende forutsetning er dermed at teoriene formuleres slik at de *kan* forkastes, det vil si at de er falsifiserbare. Induksjonsprinsippet kan dermed aldri bevise eller verifisere lovmessigheter. (ibid, s. 58). Med utgangpunkt i Poppers vitenskapsteori starter forskningsprosessen ovenfra med en slags teori som avledes til hypoteser som i neste omgang kan testes ved hjelp av observasjoner (deduksjon). Ut fra observasjonene vil vi forsøke å bygge ny kunnskap basert på empiriske sammenhenger, som igjen kan utlede til ny teori. I Ringdals bok utgjør den hypotetisk-deduktive metoden en felles ramme for all vitenskap, hvor induksjon og deduksjon inngår i en sirkulær prosess.



Figur 3. Vitenskapssirkelen (Ringdal, 2000, s. 68).

Med utgangspunkt i vitenskapssirkelen fra Ringdals bok har jeg bygget opp analysen slik at hver delanalyse tar utgangspunkt i analysemodellen i innledningen (kapittel 1). Fra analysemodellens uavhengige variabler med teorigrunnlag er det utledet hypoteser og disse vil være startpunktet for undersøkelsen av observasjoner fra primærdataene (deduksjon).

Konseptuell generalisering innebærer at vi fremstiller funn som ikke bare representerer den avgrensede empirien (observasjonen) men at de samtidig kan representere modeller, begreper eller lovmessigheter. For å sikre relevans utover egne primærdata benyttes tidligere forskning og teorier som støtter opp om en større gyldighet og generaliserbarhet (Tjora, 2012, s. 215).

Jeg har ikke tillatt meg å dra generaliserte slutninger basert på datagrunnlaget. Jeg sier heller at hypotesene enten blir styrket eller svekket gjennom analysen. Alle relevante observasjoner gjennomgår en systematisk prosess hvor vi med utgangspunkt i hypotesen utledet fra analysemodellen begynner med funn fra spørreundersøkelsen, etterfulgt av bekreftende eller avkreftende funn fra de to intervjuene (deduksjon). Dersom minst 2 av disse tre separate datakildene er gjensidig bekreftende går jeg videre til sekundærdataene i dokumentstudien. Om jeg fortsatt finner bekreftelse anser jeg teorien for å være styrket gjennom falsifiserbar induksjon. Om jeg derimot mangler grunnlag i datamaterialet sier jeg heller at hypotesen er svekket. Se figur under.

Figur 4. Arbeidsprosess for analyseprosessen

Hver av de tre hypotesene som er utledet fra problemstillingen deles opp i henholdsvis analyse av ROS-modell og VTS-modell. Disse del-analysene utgjør, sammen med de kvalitative observasjonene (Kapittel 5.4) grunnlaget for drøftingen og konklusjonen i kapittel 6. Funnene presenteres fortløpende.

3.4 Metodekritikk og etiske vurderinger

Siden jeg har arbeidet innenfor det samme fagområdet som jeg selv forsker på gjennom mange år var det først fristende å skrive en ren sikkerhetsmaster, noe som jeg fram til november 2019 var i ferd med å gjøre. Risikoen for at jeg selv skulle bli alt for subjektiv og forutinntatt var overhengende. Muligheten for at noen "biaser" fortsatt spiller inn er trolig til stede, men i langt mindre grad. Etter at jeg totalt snudde om teorigrunnlaget til å i stedet studere tematikken i lys av organisasjonsteori og statsvitenskap falt bitene bedre på plass og jeg følte selv at jeg oppnådde en mye sunnere avstand til analyseobjektet. I interaksjon med fagmiljøer og informanter var jeg konsekvent på at jeg skrev på en ledelsesmaster som tok utgangspunkt i organisasjonsteori, slik at de ikke skulle oppfatte meg i rollen som sikkerhets- og beredskapsmann fra et bestemt miljø. På teorisiden utvidet jeg gradvis grunnlaget til å inkludere flere samsvarende perspektiv fra ulike startpunkt innenfor hver av de uavhengige variablene. Det tror jeg har bidratt til å styrke oppgaven.

Jeg kunne valgt en ren kvalitativ tilnærming, men siden debatten om ROS og VTS periodevis har vært preget av polarisering vil det kvantitative tilsnittet bidra til å styrke validiteten. Undersøkelsen gav så gode data av både kvantitativ og kvalitativ karakter at jeg betraktet den som en suksess. Det dannet igjen grunnlaget for full metodetriangulering.

Spørreskjemaet kunne med fordel blitt utvidet til ren kvantitativ forskning ved bruk av krysstabeller og regresjonsanalyser i analyseverktøyet SPSS. Nettskjema har dessverre ikke noe grensesnitt som gjør det mulig med effektiv konvertering av dataene, som jeg hadde ønsket. Av hensyn til avgrensninger på oppgavens format og omfang valgte jeg derfor bort muligheten. I stedet for å lete etter direkte sammenhenger basert på et marginalt samsvar, som kvantitative forskere har en tendens til å gjøre valgte jeg i stedet å se etter klare sammenhenger basert på rent flertall, det vi si 50 prosent eller høyere.

Diskusjonen om valg av analysemodell og ikke minst safety/security har pågått i mange år, og etter min oppfatning finnes det både etablerte sannheter og paradigmepregede holdninger hos noen dyktige fagfolk ute i miljøene.

> Troen på et paradigme blant tilhengerne, kan sammenlignes med religiøs eller politisk tro. Dette er en enorm kontrast til Poppers kontinuerlige tvil på en teoris riktighet, (Ringdal, 2000, s. 61).

Jeg innforstått med at noen profesjonsutøvere i beste mening vil kunne kritisere deler av litteraturvalget, observasjonene, drøftingen og konklusjonen. Dette er jeg åpen for. Jeg har fra mitt utgangspunkt forsøkt å presentere et mest mulig balansert faglig grunnlag med en 50-50 prosents representasjon, både i dokumentstudien, gjennom spørsmålene i spørreundersøkelsen og ved valget av informanter. En objektiv tilnærming er, så langt der er menneskelig mulig lagt til grunn for analysen. Der hvor mine vurderinger måtte overskygges av subjektiv forforståelse så er primærdataene like transparente som dokumentstudiene. Hvor jeg eventuelt feiler kan både observasjoner og betraktninger etterprøves og falsifiseres av andre.

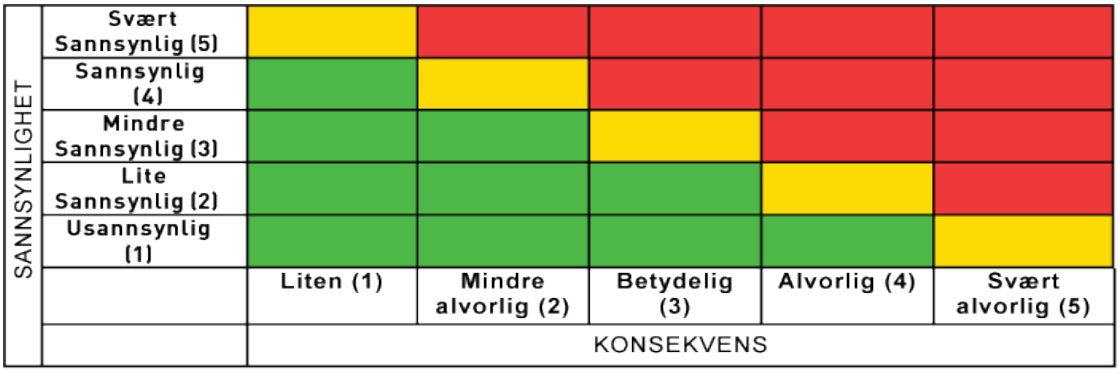
4. Dokumentstudium: Grunnlag og kontekst

Kapittelet gjengir noen hovedtrekk som skisserer hva som karakteriserer ROS- og VTS-modellene, og deres teoretiske grunnlag, så langt det er mulig. I tillegg gjengis et utdrag fra de norske risikostandardene, betraktninger fra tidligere forskning og kort beskrivelse av lover og forskrifter som har påvirkning på aktørenes valg av risikomodell.

4.1 ROS-modellen

Med utgangspunkt i faktorene *sannsynlighet* og *konsekvens* benyttes risiko- og sårbarhetsanalysen av en rekke offentlige og private virksomheter. ROS-modellen bygger på lange tradisjoner og har en bred anvendelse i samfunnet, og en sterk akademisk forankring (Aven 2015). Metodikken blir blant annet henvist til i flere av DSBs veiledere (DSB 2014, DSB 2018), som igjen er tuftet på aktuelle lover og forskrifter (se eller punkt 2.4.1).

En klar fordel med ROS er at analysen kan være relativt enkel å gjennomføres uten spesialisert kompetanse. Samtidig er det pedagogisk enkelt å illustrere resultatene av analysen i en matrise overfor beslutningstaker. Figuren under viser hvordan matrisen kan brukes for å vise samsvaret mellom sannsynlighet og konsekvens sammen med grønn, gul og rød visualisering. Risiko som ligger oppe på rødt betraktes som uakseptabel risiko som må håndteres. Gult illustrerer et middels nivå som man må ha fokus på og grønt illustrerer et lavt risikonivå.



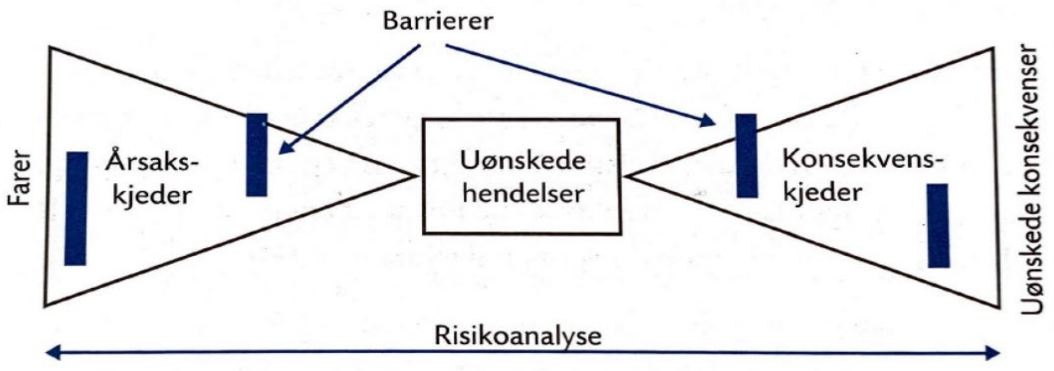
Figur 5. Eksempel på risikomatrise for ROS, hentet fra Norsk offentlig utredning (NOU 2012: 4).

Det er mye faglitteratur innen generell samfunnssikkerhet- og beredskap som peker i retning av ROS som en foretrukken og langt på vei enerådende modell for risikoanalyser. Basert på fire fagbøker som refereres under neste punkt konstaterer jeg at litteraturen som støtter ROS-

modellen i hovedsak har en trygghet-/safety-orientert tilnærming til sikkerhet og risiko. Denne slutningen kan sikkert kritiseres av noen, men lar seg forsvare ut fra sikring/security-litteraturen som legges frem under punkt 2.2.1, gjeldende oppfatninger om ROS-modellen sett fra security-miljøene (Barane 2014) og egne primærdata som fremstilles i analysen. ROS-metodikk kan like fremt anvendes for å analysere tilsiktede security hendelser, men er ikke nødvendigvis best egnet til formålet slik modellen fremstår i dag.

4.1.1 Teori som støtter opp om ROS-modellen

I følge Antonsen, Heldal og Kvalheim har menneskene til all tid forholdt seg til ulike former for fare, enten de er forårsaket forskjellige naturkrefter eller av ytre fiender. Sikkerhet kan i dette perspektivet ses i relasjon til en eller annen form for negativ hendelse og forstås som en tilstand hvor det er lav sannsynlighet for at en negativ hendelse med alvorlige konsekvenser skal inntreffe. "Når risikoen er lav, er sikkerheten høy". Videre forklares risikoanalyse som en systematisk metode for å gi svar på tre sentrale spørsmål; "Hva kan gå galt? Hva er sannsynligheten for at det går galt? Hva blir konsekvensen dersom det går galt? (2017, s. 24-25). Den norske ROS-standarden (NS 5814) blir nevnt som aktuell risikostandard. Videre viser de til et sløyfediagram som fremstiller årsaksfaktorer til en uønsket hendelse (handling) og konsekvenser, eventuelt inkludert respons- og beredskapstiltak. Samtidig illustreres barrierer eller tiltak som kan bidra til å forebygge at hendelsen utløses, eller redusere konsekvensen dersom den har inntruffet. Sløyfediagrammet er også egnet for å illustrere uønskede tilsiktede handlinger.



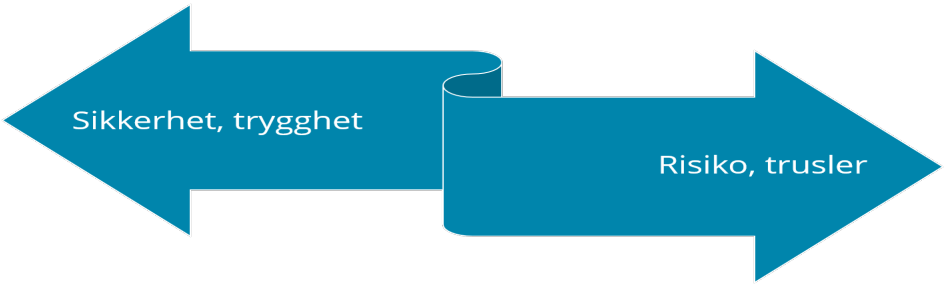
Figur 6. "Bowtie-modellen" (Antonsen, Heldal og Kvalheim 2017, s. 242).

Ivar Konrad Lunde forklarer *risikostyring* som et systematisk forsøk på å påvirke fremtidsutviklingen gjennom tiltak og aktiviteter som gjøres for å styre risiko. Usikkerheten

som ligger inn i fremtiden blir omtalt som risiko, forstått som en kombinasjon av mulige konsekvenser og tilhørende usikkerhet. Usikkerhetsbegrepet operasjonaliseres til et utrykk for hvor sannsynlig det er at en identifisert hendelse inntreffer. Det presiseres dermed at det alltid foreligger usikkerhet knyttet til sannsynlighetsbeskrivelsen. Når vi likevel velger å benytte en sannsynlighetsbeskrivelse kan risiko forstås som sammenhengen mellom sannsynlighet for at en hendelse inntreffer, og konsekvensen hendelsen kan føre til dersom den inntreffer. Risikohåndtering innebærer dermed å sette i verk tiltak som enten reduserer sannsynligheten eller konsekvensen, basert på risikoanalyser. Dette kan gjøres med utgangspunkt i en risikomatrise som samsvarer med ROS-modellen (2016, s. 25-30).

Gangdal og Angeltveit beskriver risiko- og sårbarhetsanalyse på tilsvarende måte; "Hva kan skje? Hvor sannsynlig er det? Hvilke følger/konsekvenser kan hendelsen få? Hva kan vi gjøre for å forebygge at det uønskede likevel skjer? Hvordan kan vi redusere omfanget om det uønskede likevel skjer?" (2018, s. 147). Også disse henviser til norsk ROS-standard (NS 5814) for virksomheter som ikke har en egen bransjespesifikk standard.

Fra internasjonal litteratur har jeg kikket på Ulrich Becks "Risk Society", som første gang ble utgitt i 1986. Han skriver ut fra det internasjonale perspektivet som preger en modernistisk tidsalder med farer og risiko, blant annet knyttet til forurensning eller andre menneskeskapte miljøutfordringer. Becks bok representerer dermed samfunnssikkerhet i global forstand og han forklarer forholdet mellom risiko og trygghet på denne måten; "Not so the risk society. Its normative counter-project, which is its basis and motive force, is safety"…. The utopia of the risk society is that everyone should be spared from poisoning" (Beck, 2013, s. 49). Når det kommer til det å beregne risikoen henviser Beck til frekvensbasert sannsynlighet så fremt det finnes tilstrekkelige data eller teknisk klarhet (ibid, s. 28). I likhet med Antonsen, Heldal og Kvalheim oppfatter altså Beck sikkerhet (trygghet) som en motsetning til risiko, noe som kan illustreres enkelt med en skillelinjemodell.



Figur 7. Skillelinjemodell, sikkerhet vs risiko.

4.1.2 Norsk ROS-standard

Siden lang historikk, faglitteratur og regelverk peker mot ROS-modellen finnes det en standardisert metodikk som benevnes som NS 5814:2008. Gjeldende versjon ble utarbeidet av Standard Norges komité SN/K 239 *Risiko,* som revisjon av en tidligere standard fra 1991. I forbindelse med den nye versjonen (2008) ble standarden utvidet til å omfatte risikoevaluering. Standarden er orientert mot å hindre eller forebygge uønskede hendelser, og beskriver hvordan risikovurderinger passer inn i en bredere sammenheng som beslutningsstøtte for tiltak eller løsningsvalg. Selve risikobegrepet beskrives som "et utrykk for kombinasjonen av sannsynligheten og konsekvensen av en uønsket hendelse" (Standard Norge 2008, s. 5). Standarden kan utgjøre et av flere metodiske verktøy for alle typer risikovurdering med unntak av økonomisk risiko som følge av forretningsmessige disposisjoner[9]. På en rekke områder er det utarbeidet egne standarder. NS 5814:2008 er dermed primært rettet mot organisasjoner som ikke har en bransje- eller sektorspesifikk modell.

To kategorier av beslutninger knyttet til risiko er aktuelle: Den ene er beslutninger på overordnet nivå hvor vurdering av risiko er del av en større beslutningsprosess. Sikkerhetskrav veies i slike tilfeller ofte opp mot andre krav, for eksempel funksjonalitet og økonomi (kost/nytte). Den andre er beslutninger om løsningsvalg, slik som risikoreduserende tiltak ved en bestemt løsning eller valg mellom ulike alternativer.

Risikovurderingene har også en sentral funksjon i forbindelse med andre styringsprosesser, som etablering av tekniske, organisatoriske og operative sikringstiltak (ibid, s. 2). I 2008 ble standarden i motsetning til den forrige utvidet til å innbefatte sikring (security). Inkorporeringen av sikring gjenspeiles i definisjonen av *fare* under punkt 2.2, hvor fare framstilles som "Handling eller forhold som kan føre til en uønsket hendelse… Handlingen eller forholdet kan både være både tilsiktet (sikring/"security") og utilsiktet (sikkerhet/"safety"), (Standard Norge, 2008, s. 5).

[9] Årsaken til at komitéen har satt en slik spesifikk begrensning på en generell risikomodell er for meg ukjent.

4.2 VTS-modellen

Sikringsmiljøene (security) har de senere årene fokusert på sikringsrisikoanalyser og en tre-faktormodell som tar utgangspunkt i forholdet mellom en *verdi*, *trusselen* mot denne og *sårbarheten*. Den (i norsk sammenheng) nye modellen ble introdusert på et tidspunkt som ga den mer eller mindre "drahjelp" av 22. juli. Den nye modellen ble arbeidet fram som en respons på ROS-modellens svakheter knyttet til *sannsynlighet* ved lavfrekvente hendelser og ikke minst vurderingen av *usikkerhet*. Standarden ble etablert for å ivareta det som er særegent for risiko relatert til tilsiktede uønskede handlinger, og er dermed ment som en alternativ metode, ikke som en erstatning til andre standarder med samme formål (Standard Norge, 2014, s. 2). Mange i sikringsmiljøene oppfatter VTS som den foretrukne modellen for å vurdere risiko fra tilsiktede (villede) handlinger (Barane, 2014, NSM, 2016). VTS innebærer imidlertid en mer komplisert analyseprosess enn ROS og bør derfor gjennomføres av et spesialisert analysemiljø med tilstrekkelige ressurser. Hovedfaktorene som inngår i modellen kan kort beskrives som:

Verdi – hvilke verdier eller funksjoner må beskyttes, og hvor attraktive er våre verdier for andre? Hva er verdiens entitetens tålegrense / resiliens, og hvilken rest-risiko er akseptabel?

Trussel – hvilke aktører kan true våre interesser, hva er deres kapasitet, motivasjon og fremgangsmåte? Hva er det med våre verdier som kan tiltrekke et angrep fra dem?

Sårbarhet – hvilke eksisterende forebyggende mottiltak finnes, og hva er våre gjenværende svakheter? Hvilke svakheter kan trusselaktørene utnytte?

Risikohåndtering på VTS-modell kan for eksempel gjøres gjennom *verdireduksjon*, *trusselreduksjon* eller *sårbarhetsreduksjon* (Mærli, 2012). VTS-faktorene illustreres i modellen under.

Figur 8. VTS-trekanten (NSM 2016).

Sikringsrisikoanalysen innebærer en større syklus av aktiviteter. Stegene verdivurdering, fastsettelse av sikringsmål, trusselvurdering, scenariovalg, sårbarhetsvurdering og risikovurdering oppsummerer selve sikringsrisikovurderingen, slik det fremkommer av figur 5.

Figur 9. Eksempel på VTS syklusen (Næringslivets sikkerhetsråd (NSR), 2017).

4.2.1 Teori som støtter opp om VTS-modellen

I motsetning til ROS-modellen som tar utgangspunkt i generell samfunnssikkerhet og safety-tradisjonen, så har VTS-modellen et fundament som bygger på kriminologi og sikkerhetsteori.

Rutineaktivitetsteorien. Kriminologene Felson og Cohen utviklet perspektivet *crime opportunity theories* som en utvidelse av rammeverket for *rational choice* teori. Teorien tar utgangspunkt i at mennesker, herunder kriminelle, spioner og terrorister er rasjonelle aktører som velger seg rasjonelle mål som gir best mulig gevinst til lavest mulig innsats og risiko. Rammeverket bygger på forskning knyttet til kriminelle situasjoner i perioden 1947-1974 i USA. Basert på funnene publiserte de i 1979 *The routine activity approach.* Med rasjonelle valg og kriminologi som utgangspunkt har teorien etter hvert blitt omfavnet av sikringsmiljøer som planlegger og gjennomfører tiltak mot tilsiktede hendelser. Roy Stranden oppsummerte essensen av rutineaktivitetsteorien i sin bok:

> En kriminell handling oppstår når et passende mål og en potensiell lovbryter møtes på et passende sted og tidspunkt, og hvor det er et fravær av en kapabel beskytter. (2019, s. 34).

Alle elementene må være tilstede i tid og rom. Dersom et av elementene mangler vil det ikke skje en kriminell handling der og da. Om verdien eller målet for handlingen fjernes, eller situasjonen ikke lengre er passende, eller om verdien er tilstrekkelig beskyttet, vil det ikke skje et vellykket angrep. Et passende mål kan være for eksempel en person, en gjenstand, informasjon eller en organisasjon. Målet kan være dynamisk ved å endre sin karakter, slik at det øker eller reduserer sin attraktivitet ovenfor den mulige lovovertrederen (trusselen). En potensiell lovbryter kan være alt fra en profesjonell kriminell, til en betrodd kollega eller annen nærstående som utnytter en mulighet som byr seg, ut fra ordtaket "leilighet skaper tyv". Hva som utgjør en kapabel forsvarer er tilsvarende situasjonsbestemt. Det teoretiske rammeverket inkluderer alt fra nasjonale sikkerhetsstyrker, ned til en tilfeldig ansatt eller forbipasserende. I "lette" situasjoner kan det for være tilstrekkelig med synlighet ovenfor aktøren, som "nabokona i vinduet". Dersom trusselen både har sterk intensjon og nok kapasitet kan det kreve betydelig innsats å få stanset vedkommende, langt utover hva en politimann kan håndtere.

Rutineaktivitetsteorien er like enkel som den er robust, fleksibel og universell. Utfordringen ligger i å tolke de ulike faktorene, deretter velge og tilpasse eventuelle tiltak (Stranden 2019, s. 34-36).

APT-teorien. I 1997 utviklet Giovanni Manunta en universell teori om sikkerhet mot tilsiktede uønskede handlinger (security). Manunta videreutviklet rutineaktivitetsteorien til et verktøy som skal kunne anvendes på alle situasjoner hvor en aktør kan eller vil kunne skade våre verdier. Han skiller distinkt mellom sikkerhet mot tilsiktede uønskede handlinger (*security*) og annen sikkerhet (*safety*). Tanken er at operativ sikkerhet utgjør en funksjon av samspillet mellom en *verdi* (Asset), en *beskytter* (Protector) og en *trusselaktør* (Threat) i den gitte situasjonen (Si), (Manunta, 1997).

Security = (A, P, T) Si.

I likhet med rutineaktivitetsteorien må alle tre faktorene, verdi, trusselaktør og beskytter være tilstede for at en sikringskontekst skal kunne eksistere. Uten noe av verdi er det ikke noe å beskytte, uten trusselaktør har det ingen hensikt å beskytte verdien, og uten en beskytter er det ingen som jobber for å redusere sårbarhet, og det er følgelig ingen sikringskontekst. Det er selvfølgelig mulig å bruke penger på sikkerhet også om noen av faktorene over mangler, men da er det andre mål med sikringen som ønskes oppnådd (Stranden, 2019, s. 37).

Med utgangspunkt i rutineaktivitetsaktiviteten og APT-teorien oppsummeres det teoretiske grunnlaget for VTS-modellen i figuren under.

Rutineaktivitetsteorien Utgangspunkt i Rational choice teori og kriminologi (1979).	Et passende mål	En potensiell lovbryter	Fravær av en kapabel beskytter (der og da i situasjonen).
APT teori (i en sikringskontekst) Utgangspunkt i security-teori (1997)	Verdi (asset)	Trusselaktør (threat)	Beskytter (protector)
Sikringsrisikoanalysen Norsk utgangspunkt i standard 5832:2014 (2014).	Verdi	Trussel	Sårbarhet (i hvilken grad er verdien beskyttet)?

Figur 10. Grunnlag for VTS-modellen

4.2.2 Norsk VTS-standard

Den norske VTS-standarden (NS 5832:2014) bygger på tre-faktormetodikk som har vært i bruk innenfor noen sikringsmiljøer også før 2014, selv om metodikken tidligere ikke var nedfelt i noe standardformat. Standarden ble dermed utarbeidet som del av en ny standardserie av komiteen SN/K 296, og utgjør et supplement til ROS for organisasjoner som arbeider spesielt med beskyttelse mot tilsiktede handlinger. Standarden ivaretar det som er særegent for risiko relatert til tilsiktede uønskede handlinger, men kan også anvendes for å analysere risiko relatert til andre uønskede hendelser. Metodikken er mer komplisert enn ROS og passer best for organisasjoner som har tilgang på ressurser og likesinnede. Metodikken baserer seg på kvalitative metoder, men statistisk materiale som sier noe om repetisjonsfrekvens på hendelser eller skadeomfang kan brukes som et supplement. VTS ble på daværende tidspunkt lansert som en standard uten sannsynlighetsfaktor.

Hoveddelen i analysen er sikringsrisikovurdering – vurdering av strategi – vurdering av tiltak.

- Selve sikringsrisikovurderingen baserer seg på faktorene verdivurdering, fastsetting av sikringsmål, trusselvurdering, vurdering og valg av scenarioer, sårbarhetsvurdering og vurdering av ren risiko.
- Vurdering av strategi omfatter identifisering og vurdering av strategi, ren risiko (vs. evt mulighet for gevinst) og valg av strategi (i lys av eventuell gevinstrealisering).
- Vurderingen av tiltak baserer seg på; Identifisering og vurdering av tiltak ift ren risiko (vs eventuelt gevinstrealisering), revurdering av sikringsmål og valg av tiltak.

Basert på selve prosessene som beskrevet gjenstår implementering, verifisering og tilpasning av de aktuelle sikringstiltakene (Standard Norge, 2014, s. 3).

Fram til nåværende tidspunkt (januar 2020) oppfattes VTS-modellen som gjeldende standard og et de facto krav for "statssikkerhetssektoren"[10]eller øvrige virksomheter underlagt sikkerhetsloven. Etter at ny sikkerhetslov trådde i kraft fra 2019 står saken litt mer åpnet, og det blir spennende å se hvordan VTS-modellen påvirkes av dette i fremtiden. Endringene i sikkerhetsloven oppsummeres under punkt 4.4.2.

[10] Med "statssikkerhetssektoren" tenker jeg på organisasjoner som typisk er underlagt sikkerhetslovens bestemmelser og/eller har i oppdrag å beskytte samfunnsinstitusjoner eller kritisk infrastruktur mot tilsiktede, villede handlinger. Begrepet kan innbefatte deler av næringslivet (f. eks leverandørmarkedet av sensitivt utstyr eller eiere av skjermingsverdige objekt).

4.3 Tidligere relevant forskning

4.3.1 Forskningsrapport viste til svakheter ved begge modellene

Forsvarets forskningsinstitutts (FFI) rapport "Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger" (2015/00923) gjengir FFI sine vurderinger av forskjellige tilnærminger til risikovurdering på vegne av Forsvarsbygg. Deres bestilling tok utgangspunkt i de to norske standardene (NS 5814 og NS 5832). Rapporten har dermed belyst mange sider av det temaet som jeg arbeider med. Når det gjelder VTS påpekte de svakheter ved det teoretiske grunnlaget for NS 5832, så vel som mangelen på en eksplisitt sannsynlighetsfaktor. I rapporten heves det likevel at sannsynlighet inngår som en implisitt faktor gjennom den mulighetsvurderingen som gjøres gjeldende ved vurdering av trussel, sårbarhet og scenariovalg (Busmundrud, Maal, Kiran og Endregard, 2015, s. 36). Rapporten belyste også svakheter ved ROS-modellen, ved at risikomatrisen kan overforenkle og gi inntrykk av større presisjon enn det er grunnlag for, altså underkommunikasjon av *usikkerhet* (ibid, s. 70). Det fremgår av rapporten at modellene har flere likhetstrekk, og det påpekes at kompetansen på analysegruppen er av langt større betydning enn valg av metode (ibid, s. 55). Hovedfunnene oppsummeres slik:

> Det er ingen omforent beste fremgangsmåte internasjonalt eller nasjonalt for risikovurderinger for tilsiktede uønskede handlinger. Vitenskapelige artikler og intervjuer støtter opp om denne konklusjonen. Selv om det ikke eksisterer en beste fremgangsmåte, går følgende kjennetegn igjen i en god tilnærming: den (i) er strukturert, (ii) har en arbeidsgruppe med bred kompetanse, (iii) kartlegger kunnskapsstyrken, (iv) er basert på systemforståelse og er konkret, (v) har et helhetlig perspektiv, (vi) kommuniserer risiko og usikkerhet samt (vii) er gjennomsiktig, sporbar og etterprøvbar. (Busmundrud et. al. 2015, s. 3).

4.3.2 Modellene har likhetstrekk men er for kompliserte

Stein Sletten skrev i 2018 masteroppgaven "Oppdragsrelatert risikovurdering i politiet: Hvilken metodikk egner seg best?" Sletten diskuterer de samme modellene i lys av innsatslederrollen i politiet. En utfordring for politiet er at beslutningen om bruk av metodikk ikke alltid skiller mellom planlagte og akutte oppdrag. Det som kjennetegner innsatslederen er at vedkommende både skal være i stand til å gjøre strukturerte og grundige vurderinger som del av et analyseteam for oppdrag et stykke frem i tid, og samtidig være i stand til å håndtere

tidskritiske pågående hendelser med mange ukjente faktorer, hvor erfaring og intuitiv beslutninger har større betydning. Så fremt samme metodikk brukes vil erfaringen fra de strukturerte vurderingene gi god nytteverdi til kortsiktige oppdrag, og vice versa.

> Hvis man vurderer etter en trefaktormodell med satt verdi og kjent trussel, så gjenstår bare scenario og sårbarhetsvurdering. Dette er likt tofaktormodell når man ikke fokuserer på bruk av sannsynlighet, men hovedsakelig identifiserer farer og scenario mot konsekvens. Det kan argumenteres for at for kortsiktige politioppdrag vil modellene dermed ofte oppfattes som like. (Sletten, 2018, s. 74).

I følge Sletten har modellene dermed vesentlige likhetstrekk, men må forenkles for å kunne gi bruksnytte til akuttsituasjonen.

4.4 Aktuelle lover og forskrifter

Samtlige kommuner og sivilforsvaret er underlagt lov om kommunal beredskapsplikt. Videre finnes det en rekke statlige eller andre aktører som er underlagt lov om nasjonal sikkerhet. Siden sektorlovgivningen er med på å regulere organisasjoners valg av risikomodell (ROS eller VTS) er det i lys av H_1-hypotesen nødvendig å se nærmere på utvalgte deler av disse.

4.4.1 Lov om kommunal beredskapsplikt med forskrift

Formålet med sivilbeskyttelsesloven (2010) er blant annet å beskytte liv og helse, miljø, materielle verdier og kritisk infrastruktur ved uønskede hendelser. Lovens §14 forplikter kommunene til å utarbeide helhetlige ROS-analyser som utgangspunkt for kommunens beredskapsplanverk (SBL § 14 2010). Lovteksten er helt eksplisitt på at kommunene plikter å kartlegge hvilke uønskede hendelser som kan inntreffe, hva sannsynligheten er for at de inntreffer, og hvordan de i så fall påvirker kommunen (konsekvens). Resultatet av dette arbeidet skal vurderes og sammenstilles i en helhetlig risiko- og sårbarhetsanalyse som videre legges til grunn for kommunens arbeid med blant annet samfunnssikkerhet og beredskap (sivilbeskyttelsesloven, 2010, § 14).

Forskrift om kommunal beredskap (2011)
Hverken Sivilbeskyttelsesloven eller forskriften spesifiserer *hvordan* ROS-analysene skal utføres og hvilke ressurser som skal settes inn i arbeidet. Derimot tydeliggjøres det en hel rekke krav som skal inngå i analysen, som i neste omgang skal forankres i kommunestyret. Ut fra dette regelverket er det dermed lovpålagt for kommuner å legge helhetlige ROS-analyser til grunn for arbeidet med samfunnssikkerhet og beredskap. Kravet til bruk av ROS oppfattes som et absolutt krav. Kommunens handlefrihet er følgelig svært begrenset, men et mulighetsvindu åpner seg under nest siste avsnitt av § 2: "Kommunen skal påse at relevante offentlige og private aktører inviteres med i arbeidet med utarbeidelse av risiko- og sårbarhetsanalysen" (forskrift om kommunal beredskapsplikt, 2011).

Involvering av eksterne utenfor kommunen vil kunne styrke analysen og åpne for bredere diskusjon omkring risiko og metodebruk. I siste ledd av § 2 åpnes det et annet lite mulighetsvindu for øvrige analyser eller involvering av andre aktører: Der det avdekkes behov for videre detaljer skal kommunen foreta ytterligere analyser eller oppfordre andre relevante

aktører til å gjennomføre disse. Kommunen skal stimulere relevante aktører til å iverksette forebyggende og skadebegrensende tiltak (forskrift om kommunal beredskapsplikt, 2011). Dersom kommunen selv vurderer et behov for ytterligere analyser så *skal* det gjennomføres. Dette leddet åpner dermed for bruk av VTS eller annen metodikk for å imøtekomme et slikt krav.

4.4.2 Lov om nasjonal sikkerhet m/ forskrift

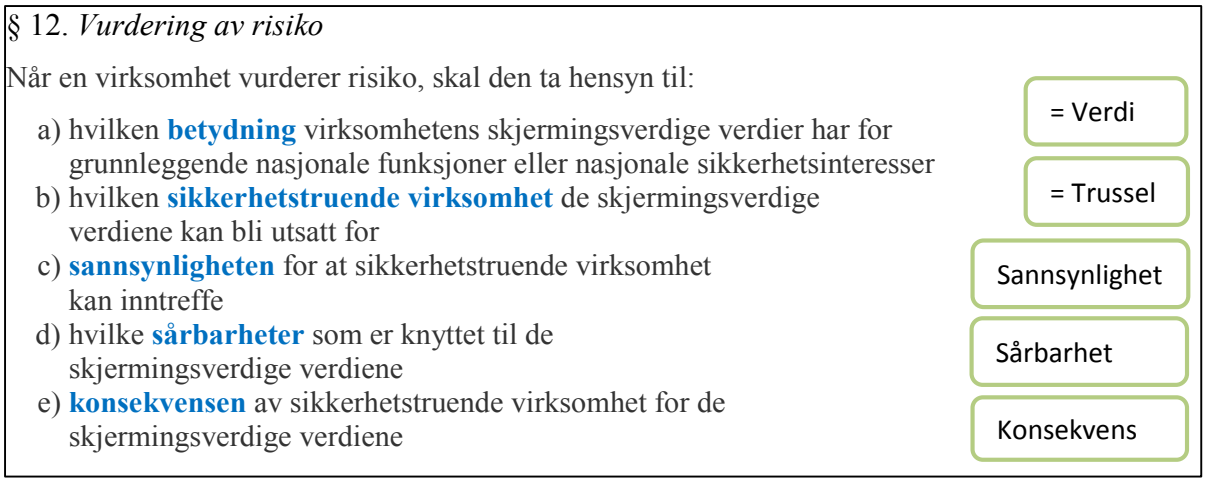
Sikkerhetsloven (pr. 1.1.19) bidrar blant annet til å

- Trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
- Forebygge, avdekke og motvirke sikkerhetstruende virksomhet
- At sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Loven gjelder for statlige, fylkeskommunale og kommunale organer, samt underleverandører i forbindelse med sikkerhetsgraderte anskaffelser. Loven kan også gjøres gjeldende ovenfor private aktører som rår over informasjon, systemer, objekter eller infrastruktur smed avgjørende betydning for grunnleggende nasjonale funksjoner (sikkl, 2019, § 1-3). Departementene har selv ansvar for det forebyggende sikkerhetsarbeidet innenfor sine respektive ansvarsområder/sektorer (sikkl, 2019, § 2-1). I § 4-2 settes det krav om regelmessig vurdering av risikoen som et grunnlag for iverksetting av forebyggende sikkerhetstiltak. Men noe krav til hvilke faktorer som skal inngå i risikoanalysen står ikke i selve sikkerhetsloven, men i forskriften som trådte i kraft på samme tidspunkt.

Virksomhetssikkerhetsforskriften

Forskrift om virksomheters arbeid med forebyggende sikkerhet spesifiserer endel krav som skal oppfylles ved vurdering av risikoen. Figur 7 siterer tekst fra § 12, påført mine uthevninger og markeringer.



Figur 11. Virksomhetssikkerhetsforskriftens § 12 med uthevinger og markeringer

Forskriften fastslår dermed hva som skal inngå i vurderingen for virksomheter underlagt sikkerhetsloven, men ingen spesifikke krav til metodikk. Dette utgjør i realiteten en endring fra tolkningen av tidligere praksis, hvor veiledningsmateriellet til NSM pekte mot VTS-modellen (NSM, 2015, NSM, 2016). Faktorene som nå skal oppfylles er reelt sett de samme som fremkommer av begge modeller sammenlagt. Ingen av dagens eksisterende standarder vil dermed ivareta sikkerhetslovens krav fullt ut. Analysemetodikken har som en konsekvens vært i en endrings- og utviklingsfase siden 2019, og en modifikasjon av enten ROS- eller VTS modellen vil tvinge seg frem. En løsning kan være å fusjonere to- og tre-faktormodellene til en samlet fem-faktor modell, uten at dette nødvendigvis blir beste løsning. Det kom interessant nok frem av begge intervjuene at en arbeidsgruppe arbeider med utforming av en ny, felles analysemodell i 2020.

5. Analyse: Hva forklarer valget av ROS eller VTS?

Analysekapittelet består først og fremt av tre delanalyser som tar for seg ROS og VTS, basert på de uavhengige variablene og hypotesene, som presentert innledningsvis. Hvert underkapittel i denne delen baserer seg på funn som belyser validiteten til en hypotese ut fra en hypotetisk-deduktiv metode (punkt 3.3). Funnene presenteres og fremstilles i lys av teoriene fortløpende, med delkonklusjoner som fastslår hvorvidt hypotesen vurderes som styrket eller svekket.

Til sist består analysen også av et underpunkt (5.4) som presenterer kvalitative observasjoner som kjennetegner begge modellene, både ROS og VTS.

5.1 Ytre rammefaktorer og instrumentalisme

En av hypotesene er antagelsen om at det ikke er organisasjonen selv, men et overordnet nivå eller en ytre sektormyndighet som avgjør valg av analysemodell (ROS eller VTS). Denne hypotesen bygger, som tidligere vist på teorier om instrumentalisme, tvungen isomorfisme og begrenset rasjonalitet i lys av policyprosessen (top-down). Jeg vil her analysere validitetene til hypotesen ut fra det datagrunnlaget jeg har samlet inn.

5.1.1 Ytre rammevilkår, instrumentalisme i valg av ROS

Basert på spørreundersøkelsen og begge intervjuene er det mye som tyder på at det er overordnet myndighet eller ytre sektorkrav som avgjør valget av ROS-modell.

Figur 12. H_1-hypotesen mot spørreskjema, instrumentalisme

Resultatene fra spørreundersøkelsen viser fire spørsmål eller påstander som berører denne hypotesen. Tre av disse bekreftet antagelsen om at det er et overordnet nivå, ytre sektor eller et lovkrav som avgjør at disse organisasjonene skal bruke ROS-modell. Spørsmål 13 bekrefter ikke kravet i lys av det instrumentelle perspektivet. Spørsmål 12 skiller ikke mellom styringskrav fra overordnet eller lovkrav, men som vi ser av svaralternativene som er gjengitt på spørsmål 16 er prosentsatsen nærmest sammenfallende med spørsmål 12. Dette styrker antagelsen om at valget om å bruke ROS-modell skyldes ytre krav (Vedlegg I).

Intervjuet med ROS-informant bekreftet at observasjonen stemmer dersom en snakker om kommuner eller andre organisasjoner som er underlagt DSB som sektormyndighet:

> Når det gjelder kommunene så oppleves det som et sektorkrav at to-faktor skal brukes. Lov om kommunal beredskapsplikt peker den retningen, det er et lovkrav og det skal de være compliant med. (Vedlegg III).

Intervjuet med VTS-informant gir et mer generelt svar på samme spørsmål:

> Etatstyrere/premissgivere har ikke alltid kunnskap nok om fenomenet. Derfor blir underliggende organer styrt på metodevalg som kan være basert på feil premisser. Sedvane, instituert tenkning, osv hos etatstyrer som smitter nedover (Vedlegg II).

I kommentaren fra VTS-informanten ligger det tilsynelatende en kritikk av etatsstyrere som instruerer undergitte på metodevalg dersom de har svakheter knyttet til egne kunnskaper. Siden uttalelsen er såpass generell kan den ikke etterprøves nærmere, men jeg beholder kommentaren fordi den representerer en ganske utbredt oppfatning ute i miljøene. Tilsvarende synspunkt kom til syne flere steder i spørreundersøkelsen. Her følger et lite utvalg fritekstkommentarer som støtter dette synet:

> Etatstyrer krever det.
> Krav fra PBL[11]
> For å ha gjort det som overordnet ledelse forventer og for å ha ryggen fri dersom noe skal skje.
> Nivået over bestemmer
> Mest for å tilfredsstille lovkrav
> Dett bestemmer fagmyndighetene
> Enkelt, lovpålagt i offentlig sektor.
> Ukjent med alternativer eller pålagt gjennom rapporteringskrav.
> Pålegg om å gjøre slik analyse i f.eks. kommuner. Andre velger det kanskje fordi det er den modellen de kjenner til, kopierer kommuner og andre som bruker ROS. (Vedlegg I).

Hypotesen støttes også av sekundærdata, blant annet fordi ROS-modell blir henvist til i flere av DSB's veiledningsmateriell for kommuner, sivilforsvar og andre samfunns- eller beredskapsaktører som DSB er premissgiver for. Det veier likevel tyngst at ROS er et eksplisitt lovkrav for organisasjoner som er underlagt sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt.

Som vist i teorikapittelet er denne hypotesen utledet av ulike teorier og funnene viser at det er ulike forklaringer som samsvarer med disse og alle er med på å styrke antagelsen om at ytre rammefaktorer er av betydning. For det første er funnet gjort i tråd med klassisk organisasjonsteori, representert ved Webers byråkratiteori som støtter ideen om embetsverkets lojalitet til samfunnsoppgaven. Dette ved at organisasjonene er instrumentelt styrt av de politiske myndigheter, videre at byråkratiet innad er underlagt regelstyring, som de lojalt

[11] Plan og bygningsloven.

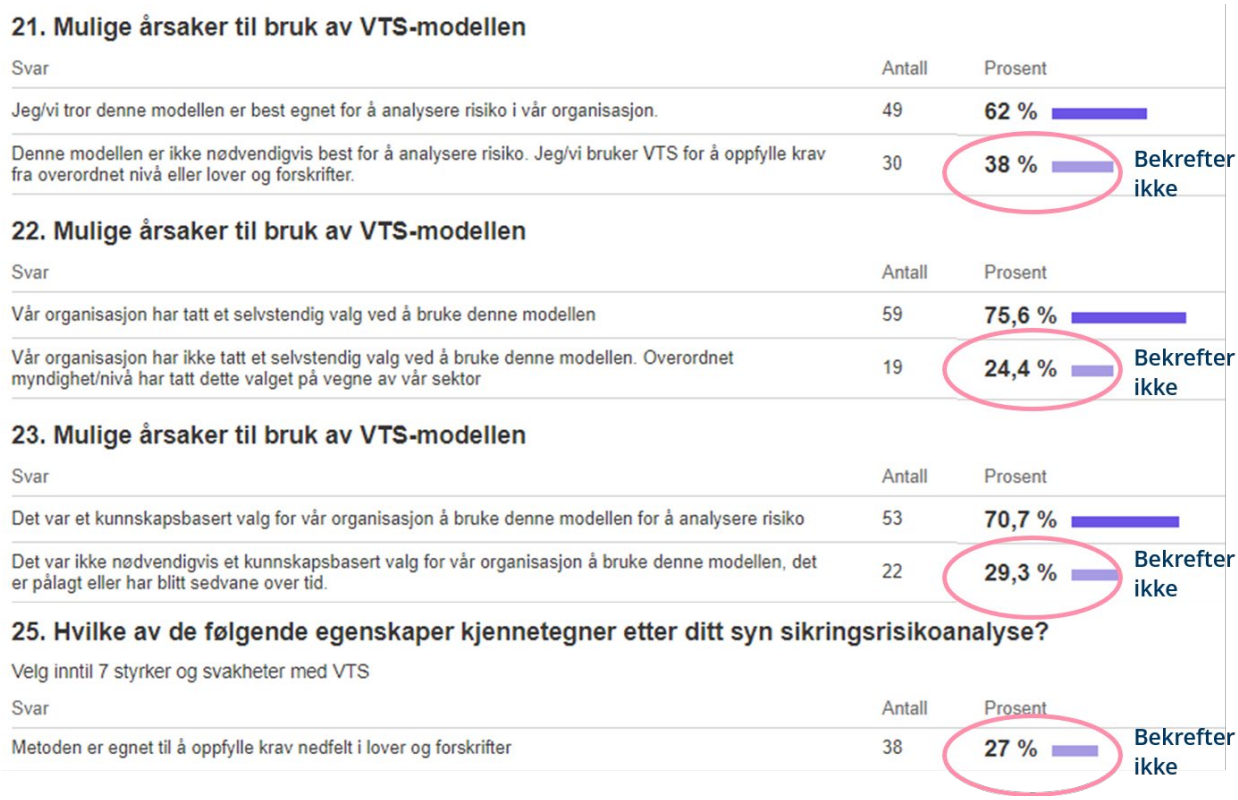
oppfyller. Samtidig er funnet i samsvar med det instrumentelle perspektivet som tar utgangspunkt i at organisasjonen oppfattes som et redskap som utfører oppgaver fra overordnet nivå. Ettersom bruk av ROS-modellen er obligatorisk som følge av sivilbeskyttelsesloven er det også samsvar med pålagt standardisering og dermed et eksempel på tvungen isomorfisme. Til sist kan funnet samsvare med begrenset rasjonalitet eller stratifisering. Det baserer seg på at de som bruker modellen har intensjon om best mulig oppnåelse av hensikten, gitt tilgjengelig informasjon og tid til rådighet.

Analysen viser dermed at antagelsen om at det er overordnet myndighet eller ytre sektorkrav som avgjør valg av ROS-modell i stor grad stemmer. Dette underbygges både av spørreundersøkelsen med fritekstkommentarer, begge intervjuer, bakgrunnsinformasjonen og valgte teorier. ROS-modellen er etablert bransjestandard for en rekke aktører, men det er i hovedsak overordnet nivå eller myndighet som har tatt valget dette på vegne av underliggende organisasjoner.

H_1-hypotesen knyttet til ROS er dermed styrket.

5.1.2 Ytre rammevilkår, instrumentalisme i valg av VTS

Når det gjelder hypotesens antagelse om at det er overordnet myndighet eller ytre sektorkrav som avgjør valg av modell, så gir hverken egne data eller bakgrunnsinformasjon en slik bekreftelse på valget av VTS-modell.



21. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent	
Jeg/vi tror denne modellen er best egnet for å analysere risiko i vår organisasjon.	49	62 %	
Denne modellen er ikke nødvendigvis best for å analysere risiko. Jeg/vi bruker VTS for å oppfylle krav fra overordnet nivå eller lover og forskrifter.	30	38 %	Bekrefter ikke

22. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent	
Vår organisasjon har tatt et selvstendig valg ved å bruke denne modellen	59	75,6 %	
Vår organisasjon har ikke tatt et selvstendig valg ved å bruke denne modellen. Overordnet myndighet/nivå har tatt dette valget på vegne av vår sektor	19	24,4 %	Bekrefter ikke

23. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent	
Det var et kunnskapsbasert valg for vår organisasjon å bruke denne modellen for å analysere risiko	53	70,7 %	
Det var ikke nødvendigvis et kunnskapsbasert valg for vår organisasjon å bruke denne modellen, det er pålagt eller har blitt sedvane over tid.	22	29,3 %	Bekrefter ikke

25. Hvilke av de følgende egenskaper kjennetegner etter ditt syn sikringsrisikoanalyse?

Velg inntil 7 styrker og svakheter med VTS

Svar	Antall	Prosent	
Metoden er egnet til å oppfylle krav nedfelt i lover og forskrifter	38	27 %	Bekrefter ikke

Figur 13. H_1-hypotese mot spørreskjema, instrumentalisme

Spørsmål/påstand nr. 21, 22, 23 og 25 i VTS-delen av spørreundersøkelsen er ellers identiske med 12, 13, 14 og 16 i ROS-delen som peker direkte på denne hypotesen. Til forskjell fra ROS-funnet ser det ikke ut til at hverken top-down instrumentalisme eller tvungen isomorfisme forklarer valg av VTS som analyseform. Funnet gir klare tegn til at bruken av VTS-modell ikke kan skyldes slike ytre krav (Vedlegg I).

VTS-informanten gir følgende forklaring på denne observasjonen:

> "Statssikkerhetssektoren" vokter i større grad (distinkte) enkeltinstitusjoner, mens kommunesektoren har et bredere fokus som dekker hele samfunnet. Dermed institueres statssikkerhet og kommunesektoren på hver sin måte slik at forskjellene mellom disse blir framtredende…. Analytikere og organisasjoner som har tilstrekkelig kunnskap om forskjellen mellom safety hendelser og security handlinger vil ut fra dagens etablerte standarder velge ROS for analyse av safety, og VTS for analyse av security om de kunne velge. (Vedlegg II).

Svaret innebærer implisitt at organisasjoner som bruker VTS-analyse sannsynligvis tilhører "statssikkerhetssektoren" og at disse ikke er "tvunget", men har gjort et selvstendig valg om bruk av VTS siden modellen som anses som best egnet for analyse på *security*, gitt dagens standarder.

ROS-informanten bekreftet at det i hovedsak er "statssikkerhetssektoren", og noen storbykommuner som velger VTS.

> Når det gjelder de securityorienterte aktørene og innenfor statssikkerhetssektoren, vi velger sikringsrisikomodell, altså tre-faktormodell hovedsakelig fordi det kom en ny veileder. Og vi ville prøve den nye veilederen, hva ga den for noe mere. Det er ikke et konstitusjonelt krav, det er det ikke…. Men for vi som er sikkerhetsaktører, det kom en ny modell, det kom en ny metode. Så ble den metoden flagget høyt i veilederperspektivet (fra NSM). Men når det kom en ny sikkerhetslov så ble det tatt ned. Da fikk denne pila et litt annet fortegn. (Vedlegg III).

Fritekstfeltet fra spørreskjemaet har også noen replikker som forklarer krav, eller opplevd krav til bruken av VTS.

> Oppfattes som et krav innen enkelte fagfelt, særlig innen fysisk sikring
> Styrte føringer om metode valg, manglende kjennskap til bruk av risikomodeller.
> Min etat har vedtatt at denne passer best til å vurdere risiko.
> For å tilfredsstille standarder og forskrifter.
> Spesialiserte behov, objekter. (Vedlegg I)

Hypotesen knyttet til VTS støttes heller ikke av sekundærdata. Siden lanseringen av en norsk VTS standard i 2014 ble modellen hyppig diskutert i fagmiljøene og raskt populær. NSM fulgte opp med gjennomarbeidet veiledningsmateriell og metodikken ble etablert som beste praksis for analyse av tilsiktede handlinger i statssikkerhetsmiljøene. Modellen er dermed innført i flere organisasjoner, men i de fleste tilfellene skyldes ikke dette et instrumentelt krav fra en overordnet myndighet.

Som vist i teorikapittelet er denne hypotesen utledet av ulike teorier, men for VTS samsvarer ikke disse med antagelsen om at det er ytre rammefaktorer er av betydning. Funnet bekreftes ikke av det instrumentelle perspektivet med utgangspunkt i at organisasjonen oppfattes som et redskap som utfører oppgaver fra overordnet nivå som en følge av styringsrelasjonen mellom disse. Mye tyder heller på at organisasjoner som benytter VTS i hovedsak har gjort selvstendige valg. Det foreligger pr tid ingen lovkrav, men VTS har likevel vært foretrukken

metode for security i endel miljøer, blant annet NSM, PST og POD (NSM 2015). Funnet samsvarer heller ikke med tvunget isomorfisme, som var tilfellet i analysen av ROS.

Fortsatt bruk av VTS samsvarer i alle tilfeller med begrenset rasjonalitet. All den tid det ikke finnes andre metoder som er optimalisert for analyse av tilsiktede handlinger eller en spesifikk modell som kan ivareta sikkerhetslovens krav, er det rasjonelt å bruke den best egnede modellen, gitt tilgjengelig informasjon.

Analysen viser dermed at antagelsen om at det er overordnet myndighet eller ytre sektorkrav som avgjør valg av modell, ikke samsvarer med valget av VTS. Hverken egne funn eller sekundærdata tilsier at det er tilfelle. Denne modellen er likefremt bransjestandard for endel securityorienterte aktører innenfor statssikkerhetssektoren. Basert på vurderingen av teori er det kun begrenset rasjonalitet og stratifisering som gjenspeiler dagens situasjon.

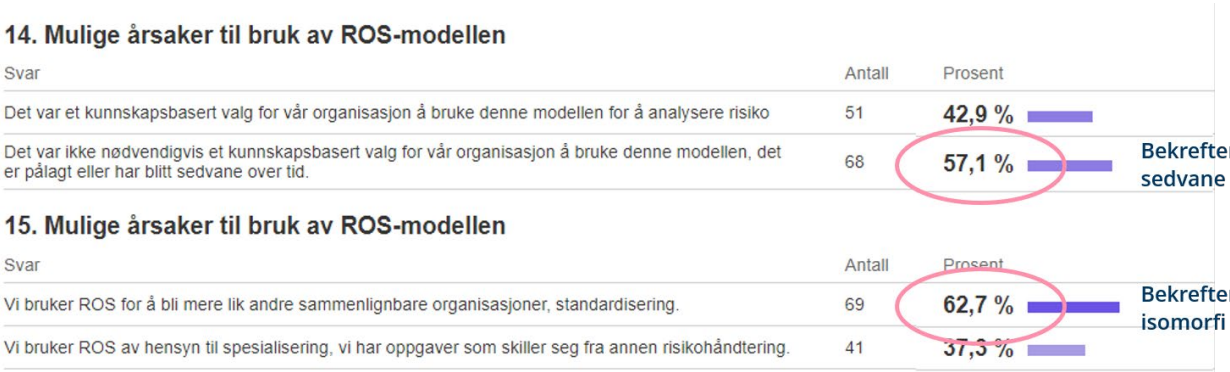
H_1-hypotesen knyttet til VTS er dermed svekket.

5.2 Institusjonalisme og stiavhengighet, kulturperspektivet

Den andre hypotesen som skal undersøkes antar at valget av analysemodell skyldes sedvane eller andre institusjonelle forhold som kan forklares internt i organisasjonen. Denne hypotesen bygger, som tidligere vist på teori fra kulturperspektivet. Egne funn blir analysert i lys av institusjonalisme og stiavhengighet, i tillegg til normativ isomorfisme og begrenset rasjonalitet. Jeg vil her analysere validitetene til denne hypotesen ut fra det datagrunnlaget jeg har samlet inn.

5.2.1 Indre forhold og institusjonalisme i valg av ROS

Basert på spørreundersøkelsen og begge intervjuer er det mye som tyder på at ROS-analysen er institusjonalisert i flere organisasjoner med sedvanetenking og stiavhengighet, i tillegg til normativ standardisering og begrenset rasjonalitet.



Figur 14. H_2-hypotese mot spørreskjema, institusjonalisme

Resultatene fra spørreundersøkelsen viser at spørsmål/påstand 14 og 15 berører denne hypotesen. Spørsmål 14 bekrefter at bruken av ROS-analyse er pålagt eller har blitt sedvane over tid. Det indikerer et trolig samsvar med institusjonell sedvane. Organisasjonene som bruker ROS er fornøyd med etablert løsning og ikke ønsker noen endring. Spørsmål 15 bekrefter at ROS brukes for å bli mer lik andre sammenlignbare organisasjoner, standardisering i samsvar med normativ isomorfisme. Kommentarfeltet gir følgende forklaringer:

> For sånn har vi alltid gjort det.
> Som regel fordi det finnes kompetanse, erfaring og gode standarder for denne metoden

> Velprøvd metode. Finpusset gjennom tiår. Mye god internasjonal litteratur. Standard metode i de fleste modne sikkerhetsmiljøer i forskjellige industrier.
> Gir en enkel og oversiktlig beskrivelse av risiko - forståelig også for ikke-fagpersoner.
> Sedvane
> Fordi det er den modellen man behersker.
> Mange har gjort det før oss, det finnes erfaring og «best practice»
> En etablert standard som man kjenner igjen fra andre forretningsområder som prosjekt og økonomistyring hvor frekvenser og usikkerhet er innarbeidet i et felles risikobilde eller risikoregister. (Vedlegg II).

Intervjuet med ROS-informant bekreftet at denne observasjonen knyttet til institusjonalisme og sedvane er korrekt.

> Dette med tykk institusjonalisme er representativt for norske kommuner. Sånn har vi alltid gjort det, sånn har DSB sagt at vi skal gjøre det, vi har ikke noen grunn til å gjøre det annerledes. Det er dette vi blir målt på. Sitt rolig i båten, gjør det bare ordentlig og vi gjør det på den måten. Ferdig snakka. (Vedlegg III).

Videre gir ROS-informanten støtte til normativ isomorfisme (standardisering) og begrenset rasjonalitet ved at organisasjoner gjør valg som er gode nok til å oppnå hensikten, gitt tilgjengelig informasjon og tid til rådighet.

> Jeg har ikke noen tro på at dette miljøet er så stort at vi klarer å opprettholde to modeller. Jeg tror ikke merverdiene ved å opprettholde to modeller er stor, som det skal drives utvikling på, som det skal drives opplæring på, som det skal drives analyser på, og kommunikasjon av på mange forskjellige nivåer. Nei, det tror jeg egentlig ikke står seg i lengden…. Risikomodellering kommer aldri til å bli noe eksakt vitenskap innenfor dette samfunnsperspektivet (Vedlegg III).

Intervjuet med VTS-informant bekreftet observasjonene knyttet til institusjonalisme og sedvane, og til dels normativ isomorfisme og begrenset rasjonalitet.

> Sedvane, instituert tenkning, osv hos etatstyrer som smitter nedover…. Institusjonalisme og stiavhengighet gir stor forklaringskraft for mange organisasjoners valg (aktivt eller passivt) av analysemodell. For eksempel om en organisasjon har basert det meste av sin portefølje på én type metodikk kan det være tungt å endre tilnærming (Vedlegg II).

Hypotesen støttes godt av sekundærdata, i og med at ROS-modellen bygger på lange tradisjoner i Norge og har bred anvendelse i samfunnet. Det bygger opp under institusjonelle forklaringer som sedvane og stiavhengighet. De som bruker ROS-modellen er fornøyd med etablert løsning og ønsker ingen endring. Ved at ROS-modellen er enklere å gjennomføre uten

spesialisert kompetanse, styrker dette begrenset rasjonalitet ved at en gjør beslutninger og handlinger som oppfyller hensikten.

Som vist i teorikapittelet er hypotesen utledet av forskjellige teorier og funnet viser at ulike forklaringer samsvarer med disse. Webers klassiske byråkratiteori støtter ideen om standardisering av repeterende arbeidsoppgaver, så vel som spesialisering av kompetansen knyttet til kompliserte oppgaver. ROS-analysen er i betydelig grad institusjonalisert i en rekke offentlige så vel som private bedrifter. Metodikken er utviklet og tillært over tid, slik at erfarne fagfolk gjennomfører analysene på en effektiv måte. ROS-modellen eksemplifiserer dermed det institusjonelle perspektivet meget godt, med tanke på både sedvane og stiavhengighet. De som har valgt en bestemt sti ønsker sjelden å gå tilbake og endre kurs.

ROS-modellen gir samtidig forklaringskraft til begrenset rasjonalitet. Så lenge modellen fungerer og oppnår hensiktene, gitt tilgjengelig informasjon og tid til rådighet er dette et rasjonelt valg for de som bruker den. Av de samme årsaker som nevnt gir bruken av ROS også forklaringskraft både til institusjonell og normativ isomorfisme. Når "alle" vet hvordan oppgavene skal løses standardiseres organisasjonene og blir mer kompatible både innad- og ikke minst mellom ulike organisasjoner.

Mye tyder på at bruken av ROS-analyse er institusjonalisert i flere organisasjoner med både sedvanetenking og stiavhengighet. De som bruker modellen er fornøyd med dagens løsning og ønsker ingen endring. ROS-modellen representerer også institusjonell og normativ isomorfisme som gir kompabilitetfordeler for brukerne. Samtidig bekreftes begrenset rasjonalitet, så hvorfor endre noe som fungerer? "If it ain't broke, don't fix it".

Basert på funn fra undersøkelsen, intervjuene, bakgrunnsinformasjonen og teoriene kan vi trekke den slutningen at H_2-hypotesen er styrket når det gjelder ROS-modellen.

5.2.2 Indre forhold og institusjonalisme i valg av VTS

Basert på spørreundersøkelsen og begge intervjuer er det lite som tyder på at VTS-analysen er institusjonalisert med sedvanetenking og stiavhengighet på samme måte som ROS.

Figur 15. H_2-hypotese mot spørreskjema, institusjonalisme

På VTS-delen av undersøkelsen er det spørsmål/påstand 23 og 24 som er identiske med 14 og 15 i ROS-delen, og som vi ser viser tabellen et stikk motsatt resultat. Bruken av VTS-modell samsvarer ikke med sedvane over tid. På spørsmål 24 har en betydelig overvekt av respondentene valgt VTS av hensyn til spesialisering, grunnet oppgaver som skiller seg fra annen risikohåndtering. Siden bare 26,8 % av respondentene har valgt VTS av hensyn til standardisering for å bli mer lik "sammenlignbare organisasjoner" støttes ikke hypotesen eksplisitt, men det er likevel en mulighet for at disse respondentene representerer security-orienterte miljøer innenfor statssikkerhet, hvor VTS-modellen gradvis har blitt instituert standard. En regresjonsanalyse på korrelasjonen mellom spørsmål 23 (kunnskapsbasert), spørsmål 24 (spesialisering) og spørsmål 30 (statlig sektor) ville gitt et langt mer presist svar.

Kommentarfeltet gav følgende tilleggsinformasjon:

> Oppfattes som et krav innen enkelte fagfelt, særlig innen fysisk sikring
> Per nå - beste metodikk for å identifisere risiko knyttet til tilsiktede handlinger (verdier, trusselaktører, kapasitet, sårbarhet). Supplerende verktøy til ROS som gir annen innsikt - kan ikke erstatte hverandre, men kan med fordel kobles mye bedre sammen.
> Min etat har vedtatt at denne passer best til å vurdere risiko.
> Spesialiserte behov, objekter. (Vedlegg I)

Intervjuet med VTS-informant bekreftet antagelsen om at security-orienterte aktører foretrekker VTS-modell:

> Ved safety hendelser utrykkes risiko tradisjonelt som en kombinasjon av sannsynlighet og konsekvens (R = P x C), det vil si ROS-modellen. Utfordringene viser dermed behovet for en egen

> analysemetodikk for villede, ondsinnede handlinger, slik som VTS-modellen representerer…. "Statssikkerhetssektoren" vokter i større grad (distinkte) enkeltinstitusjoner, mens kommunesektoren har et bredere fokus som dekker hele samfunnet. Dermed institueres statssikkerhet og kommunesektoren på hver sin måte slik at forskjellene mellom disse blir framtredende. Det som er normativt best for den ene sektoren er ikke nødvendigvis best for den andre. (Vedlegg II).

Intervjuet med ROS-informant avviser imidlertid at det er safety/security diskusjonen som har ført til valg av analysemodell:

> Jeg tror at denne diskusjonen om safety og security har hatt innvirkning på hvordan vi som analytikere har valgt modell. Men hovedårsakene til valg av metode tror jeg ikke er hvorvidt er det safety eller security. Jeg tror det er andre årsaker som er mer toneangivende når det gjelder hovedårsak til valg av analysemodell. Fordi safetymodellen kan fint brukes på en securityhendelse, ikke noe problem! Og du kommer ut av det med veldig god risikokunnskap og en sårbarhetskunnskap som er godt inne på skiva. Så nei, safety eller security diskusjonen har ikke hatt stor betydning. Det er andre ting som har hatt det. (Vedlegg III).

Sekundærdata indikerer at VTS sannsynligvis er best egnet for analyse av tilsiktede (security) handlinger, men gir ikke noe grunnlag for å si at valget skyldes institusjonelle forhold, som sedvane eller stiavhengighet. Dog så gir dokumentstudien støtte til både normativ isomorfisme (NSM 2015) og rasjonalitet (Barane 2014).

Klassisk organisasjonsteori i lys av både Taylors effektiviseringsteori og Webers byråkratiteori lanserer ideen om standardisering av repeterende arbeidsoppgaver, så vel som spesialisering knyttet til kompliserte oppgaver. Dette skulle tilsi at VTS har et godt potensial for å institusjonaliseres hos miljøer som spesialiserer seg på analyser av risikoen for tilsiktede handlinger. Også kulturperspektivet støtter valget av VTS for spesifikke miljøer, ved at organisasjonene formes og utviklers av stadige prosesser mellom menneskene i- og mellom organisasjonene. Stiavhengighet kan muligens på litt lengre sikt bidra til å forklare bruken av VTS, men ingen av overnevnte antagelser bekreftes av egne datagrunnlaget. Så lenge VTS (reelt eller opplevd) er det beste alternativet for security styrker det i alle tilfeller rasjonelle valg-teorier og begrenset rasjonalitet.

Bruken av VTS-analyse kan tenkes å være institusjonalisert hos endel security-orienterte aktører. I likhet med ROS kan det også tenkes at de som bruker VTS-modellen er fornøyd med

dagens løsning og ikke ønsker noen endring. Til tross for støtte fra bakgrunnsinformasjonen og teorigrunnlaget finner jeg ikke belegg for å forsvare hypotesen ut fra egne primærdata.

H_2-hypotesen knyttet til VTS er dermed svekket.

5.3 Handlefrihet og rasjonelle valg, kunnskap og myter

Den tredje hypotesen som skal undersøkes antar at aktørene fritt velger mellom ROS, VTS eller andre analysemodeller basert på rasjonelle valg, kompetanse og handlefrihet. Videre antas det at oppslutningen om valgt modell kan forklares ut fra myteperspektivet og mimetisk isomorfisme, fordi organisasjoner ønsker å fremstå som moderne og framtidsrettede for å styrke egen legitimitet eller attraktivitet. Jeg vil her analysere validitetene til denne hypotesen ut fra datagrunnlaget.

5.3.1 Rasjonelle valg, kunnskap og myteperspektivet, ROS

Til tross for bakgrunnsinformasjon, teori og et av intervjuene finner jeg ikke grunnlag for å bekrefte at ROS-modellen har vært et rasjonelt og kunnskapsbasert valg i lys av handlefrihet.

Figur 16. H_3-hypotese mot spørreskjema, kunnskap og handlefrihet

Resultatene fra spørreundersøkelsen viser tre spørsmål eller påstander som berører denne hypotesen. Spørsmål 12 og 14 viser at ROS-modellen ikke nødvendigvis er best egnet for å analysere risiko, videre at det at det ikke nødvendigvis var et kunnskapsbasert valg å bruke

denne modellen. Spørsmål 13 gir en marginal indikasjon på at organisasjonen har tatt et selvstendig valg ved å bruke denne modellen. Oppsummert viser funnet at ROS-analyse ikke har vært et kunnskapsbasert valg for disse organisasjonene.

Et utdrag fra fritekstfeltet illustrerer mange kvalitative styrker med ROS-analysen, men få kommentarer indiker at organisasjonen har gjort et selvstendig- eller kunnskapsbasert valg. Kommentarene viser imidlertid tegn på både normativ- og mimetisk isomorfisme.

> Av egen erfaring brukes denne for den er standardisert og "enkel" å benytte i en ellers kompleks oppgave, og gir resultater godt visuelt fremstilt. Den er lett å forholde seg til. Dog kreves erfaring og kompetanse i gjennomføring, for å ikke undertrykke elementer som f.eks. usikkerhet.
> Fordi andre kommuner gjør det
> Mange har gjort det før oss, det finnes erfaring og «best practice»
> Pålegg om å gjøre slik analyse i f.eks. kommuner. Andre velger det kanskje fordi det er den modellen de kjenner til, kopierer kommuner og andre som bruker ROS.
> Kjennskap, Likhet til andre org.
> Velprøvd metode. Finpusset gjennom tiår. Mye god internasjonal litteratur. Standard metode i de fleste modne sikkerhetsmiljøer i forskjellige industrier.
> Velkjent tilnærming med en enkel og kraftig visualisering av risikobilde
> Jeg tror ROS-analyser brukes fordi det er et innarbeidet begrep når sikkerhet skal ivaretas på ulike nivåer. Det foreligger flere modeller/skjemaer som benyttes, men alle jeg har sett forholder seg til trussel multiplisert med konsekvens. Man kunne like gjerne benyttet en annen modell, så lenge den er kjent i hele organisasjonen. (Vedlegg I).

Intervjuet med VTS-informant ga ingen informasjon som indikerer at valg av ROS-modell baserer seg på kunnskapsbasert valg. Men ROS-informanten løftet frem kunnskapsmessige fordeler med ROS-modellen, så vel som normativ og imiterende isomorfi.

> Kunnskap er viktig. Kunnskap og kompetanse om to-faktormodellen er lett tilgjengelig, for den er enklere. Det er noe som man er vant til i mange sammenhenger. Det enkle gjør man mer av enn det som er vanskelig og tungvint. Derfor tror jeg at det er noen subjektive forhold som utdanning, kunnskaper som er styrende for valget…. Alle forsøker nok og å velge den analysemodellen som er mest riktig å bruke ut fra eksisterende kunnskap. Det ligger nok til grunn, men man blir fort fanga av virkeligheten. Enkleste vei til målet som er godt nok, ja takk begge deler…. Kommunene gjør som sagt valg ut i fra at ting er enkelt. Storbykommunene kan gjøre valg fordi de andre gjør det. Sikkerhetsorganisasjoner som har litt ressurser prøver ut nye modeller, setter seg inn i dette og går kurs i dette (Vedlegg III).

Ut fra sekundærdata på ROS kan sikkerhet oppfattes som motsetningen til en eller annen form for negativ hendelse. Dermed forstås høy grad av sikkerhet som et synonymt til en tilstand hvor det er lav sannsynlighet for at en negativ hendelse med alvorlige konsekvenser skal inntreffe. Bruken av både sannsynlighets- og konsekvensbegrepet gir dermed direkte relevans til ROS-modellen som et rasjonelt valg. Sekundærdata viser også at ROS er enklere å gjennomføre uten spesialisert kompetanse. At metodikken er godt utbredt over tiår og anerkjent av de fleste miljøer styrker posisjonen. Disse faktorene gjør at ROS fremstår som et kunnskapsbasert og rasjonelt valg.

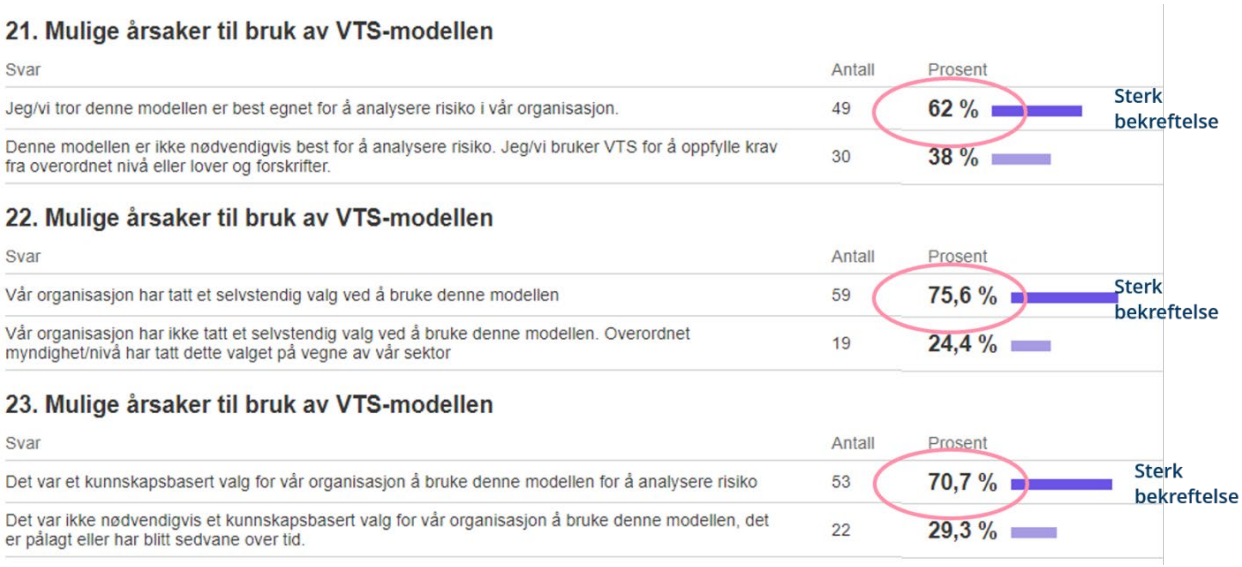
Basert på teoriperspektivene for denne hypotesen er det mye som tyder på at ROS-modellen blir brukt med basis i rasjonelle valg og kompetanse, men ikke handlefrihet, som var et av premissene for denne hypotesen. Videre kan det antas det at også myteperspektivet kan beskrive valget, men det bekreftes ikke gjennomgående. Mimetisk isomorfisme har trolig også vært en faktor, men denne forsvares bare ut fra kommentarfeltene på spørreundersøkelsen.

Til tross for sekundærdata, teori og et av intervjuene finner jeg ikke grunnlag for å forsvare ROS-modellen som et rasjonelt og kunnskapsbasert valg i lys av handlefrihet. ROS-modellen blir brukt fordi den er velkjent og velfungerende, men valget av modell er det, ut fra mine observasjoner i hovedsak andre som har andre stått for.

H_3-hypotesen knyttet til ROS er dermed svekket.

5.3.2 Rasjonelle valg, kunnskap og myteperspektivet, VTS

Basert på spørreundersøkelsen og intervjuer er det mye som tyder på at VTS-modell er et rasjonelt og kunnskapsbasert valg gjort i lys av handlefrihet for security-organisasjoner. Samtidig er myteperspektivet svært beskrivende for den oppslutningen modellen har fått.



21. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent	
Jeg/vi tror denne modellen er best egnet for å analysere risiko i vår organisasjon.	49	62 %	Sterk bekreftelse
Denne modellen er ikke nødvendigvis best for å analysere risiko. Jeg/vi bruker VTS for å oppfylle krav fra overordnet nivå eller lover og forskrifter.	30	38 %	

22. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent	
Vår organisasjon har tatt et selvstendig valg ved å bruke denne modellen	59	75,6 %	Sterk bekreftelse
Vår organisasjon har ikke tatt et selvstendig valg ved å bruke denne modellen. Overordnet myndighet/nivå har tatt dette valget på vegne av vår sektor	19	24,4 %	

23. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent	
Det var et kunnskapsbasert valg for vår organisasjon å bruke denne modellen for å analysere risiko	53	70,7 %	Sterk bekreftelse
Det var ikke nødvendigvis et kunnskapsbasert valg for vår organisasjon å bruke denne modellen, det er pålagt eller har blitt sedvane over tid.	22	29,3 %	

Figur 17. H_3-hypotese mot spørreskjema, kunnskap og handlefrihet

På VTS-delen av undersøkelsen er det spørsmål/påstand 21, 22 og 23 som er identiske med 12, 13 og 14 i ROS-delen. Som vi ser viser tabellen et stikk motsatt resultat. Bruken av VTS skyldes at modellen er best egnet til å analysere risiko i organisasjonen, basert på et kunnskap og selvstendig valg.

Et utdrag fra fritekstdelen av kommentarfeltet gir en utfyllende forklaring. Samtidig bekreftes myte/moteperspektivet fra ny-institusjonell teori.

> Bedre egnet modell mtp analyser av tilsiktede hendelser
> Enkelte virksomheter har behov for å vurdere trusler og scenarioer som det er vanskelig å sette sannsynlighet og frekvens på. Slike scenarioer krever en kvalitativ vurdering. Dette er et bevisst og kvalifisert valg.
> Litt sånn "mote" analyseteknikk
> Per nå - beste metodikk for å identifisere risiko knyttet til tilsiktede handlinger (verdier, trusselaktører, kapasitet, sårbarhet). Supplerende verktøy til ROS som gir annen innsikt - kan ikke erstatte hverandre, men kan med fordel kobles mye bedre sammen.
> Denne modellen er på tur inn og vil nok erstatte ros analysen.
> Populære metode blitt.
> VTS analyse er bedre enn ROS på flere måter. Den er langt mer basert på faktabasert parametere.

> Noen ganger fungerer denne metodikken best. Den krever mer faglig tyngde for å gjennomføres, spesielt når man evaluerer styrken på sikringstiltakene opp mot trusselen, men sammenhengen mellom verdi, trusselaktør, sårbarhet og tiltak kommer frem på en måte som gjør at det er lettere for å få gjennomslag for foreslåtte tiltak. (Vedlegg I).

Intervjuet med VTS-informant gir en tydelig bekreftelse på det bildet som tegner seg ut fra spørreundersøkelsen.

> Ut fra forskjellen på safety-hendelser og security-handlinger så bør valget av analysemodell gjøres på grunnlag av om det er safety-risiko eller security-risiko som skal analyseres. …. Analytikere og organisasjoner som har tilstrekkelig kunnskap om forskjellen mellom safety hendelser og security handlinger vil ut fra dagens modellalternativer velge VTS for risiko som skyldes tilsiktede uønskede handlinger (Vedlegg II).

ROS-informanten nyanserte bildet endel.

> Alle forsøker nok og å velge den analysemodellen som er mest riktig å bruke ut fra eksisterende kunnskap…. Kommunene gjør som sagt valg ut i fra at ting er enkelt. Storbykommunene kan gjøre valg fordi de andre gjør det. Sikkerhetsorganisasjoner som har litt ressurser prøver ut nye modeller, setter seg inn i dette og går kurs i dette…. Nysgjerrighet er en faktor. Hvor nysgjerrige er sikkerhetsmiljøene på bruk av nye metoder? (Vedlegg III).

Ut fra sekundærdataene ble sikringsrisikoanalysen introdusert på et tidspunkt hvor den fikk "drahjelp" av 22. Juli-rapportens kritikk av risikopersepsjonen i samfunnet (NOU 2012: 14). VTS-modellens popularitet kan dermed forstås som en konsekvens av kritikken mot ROS-analysens svakheter knyttet til vurdering av sannsynlighet og usikkerhet (Barane 2014, FFI 2015). VTS har i ettertid blitt stående som den normativt beste modellen for å vurdere risikoen for tilsiktede (villede) handlinger.

Resultatene fra spørreundersøkelsen viser klart at organisasjoner som bruker VTS har tatt et kunnskapsbasert, normativt og selvstendig valg ved å bruke denne modellen. Dette er dermed i tråd med teorien om rasjonelle valg. Samtidig forutsettes det at disse aktørene har endel ressurser og større eller mindre grad av handlingsrom. Uten handlefrihet vil det ikke være mulig å ta et selvstendige valg. Dermed bekreftes også den delen av teorien.

Et nøkkelresonnement for myteperspektivet er at organisasjoner befinner seg i institusjonelle omgivelser under påvirkning av sosialt skapte normer, eller myter som spres som moter

gjennom imitasjon fordi organisasjoner ønsker å fremstå som moderne og framtidsrettede for å styrke egen legitimitet eller attraktivitet.

> Rasjonaliserte myter har to viktige kjennetegn. For det første presenteres de gjerne som svært effektive redskaper som organisasjoner kan bruke for effektiv måloppnåelse. At myten er rasjonalisert innebærer at det ved hjelp av vitenskapslignende argumentasjon er skapt en overbevisning om at den er et effektivt virkemiddel for å oppnå bestemte organisatoriske mål. (Christensen et. al. 2017, s. 76-77).

Her kan vi også ta med utsagnet fra Røvik: "Siden mytene er tidsriktige framstår de gjerne som moter, noe "alle" skal ha inntil de går av moten" (Moren 2011, s. 52). Måten VTS-modellen spredte seg på med eskalerende oppslutning samsvarer fullt ut med forståelsen av myteperspektivet.

Til tross for nyanseringen fra et av intervjuene tegner både primærdata, teori og sekundærdata et tydelig bilde av VTS-modellen som et kunnskapsbasert valg for organisasjoner som analyserer risikoen for tilsiktede handlinger (security). 75,6 % av respondentene i undersøkelsen hevdet at dette var et selvstendig valg, mens 70,7 % hevdet at valget var kunnskapsbasert.

Myteperspektivet er samtidig beskrivende for den oppslutningen modellen har fått i sikkerhetsmiljøene siden 2014. Inntil den eventuelt går av moten som en konsekvens av den nye sikkerhetsloven ser det ut til at VTS-modellen vil beholde sin popularitet.

H_3-hypotesen knyttet til VTS er dermed styrket.

5.4 Kvalitative observasjoner

Som vi har sett hittil så har analysen påvist distinkte forskjeller mellom ROS- og VTS-modellene i lys av organisasjonsteorien. Som forklart i innledningen vil jeg oppsummere analysen med å fremstille noen generelle observasjoner som kjennetegner en god tilnærming til risikoanalyse, uavhengig av modellvalg. Funn som følger baserer seg på kvalitative enkeltkommentarer hentet fra spørreundersøkelsens spørsmål 26: "Hva er etter ditt syn det viktigste suksesskriteriet for å gjennomføre en god risikoanalyse?"

> Det viktigste suksesskriteriet for å gjennomføre en god risikoanalyse er ledelsesforankring, kompetanse hos dem som gjennomfører analysen og at de med eierskap til verdiene deltar i risikoanalyseprosessen. Den største fallgruven er imidlertid oppfølging av risikoanalysen. Hvis ikke ledelsen aktivt bruker risikoanalysen til å akseptere, fjerne, redusere eller overføre identifisert risiko, har analysen liten verdi.
>
> Tilstrekkelig ressurstilgang i selve analysen og ved revisjoner av denne, dette henger sammen med risikoerkjennelse og ledelsesforankring av risikoerkjennelse. Dessverre oppleves lite ressurstilgang i det forebyggende (proaktive) sporet. Ressurser stilles til rådighet når man tvinges til det i form av gjennopprettende tiltak etter en uønsket hendelse.
>
> Jeg mener vi ikke bør se på dette så sort / hvitt som det gjøres i dag. Innenfor begge metodene ser man på verdier (scoping av analysen), trusler eller farer, og sårbarheter. Det kan være nyttig å si noe konkret om hvilke scenarioer som er mer sannsynlig enn andre (sannsynlig basert på den informasjonen vi har om trussel og sårbarhet), og hvilke konsekvenser det vil ha for organisasjonen dersom verdiene rammes slik det fremkommer av det spesifikke scenarioet.
>
> Det er flere enn disse to metodene som kan brukes. I arbeidet må en forstå sin kontekst og sine behov. Deretter må en velge metode som passer basert på dette. En må videre ha kunnskap om styrker og svakheter ved de ulike metodene slik at en tolker resultatene rett. Analyser er ikke eksakt vitenskap og mye av utfordringen er at analytikerne må forstå eget og andres kunnskapsgrunnlag og hvilken usikkerhet som ligger i dataen/informasjonen, og i egen anvendelse av dette.
>
> Man må bruke det verktøyet som passer best i enhver situasjon. Både VTS og ROS er anvendelige for hver sine former for risikovurderinger. Det er viktig å ikke underslå at sannsynlighet kommer med som en betraktning i begge metoder, men at det kan være gunstig å arbeide kvalitativt ved kompliserte og sammensatte risikosituasjoner. VTS lar seg anvende også der sannsynligheten er kjent eller omforent. ROS kan benyttes der sannsynligheten er ukjent. Metode er underordnet. Prosessen med valg av deltakelse, grundighet, bevisstgjøring er viktigere.

> Begge modellene har sine styrker og svakheter, og jeg mener det må være opp til enhver organisasjon å vurdere hvilken som passer best for dem. Ingen modeller klarer fange opp alt, og det er personen som gjennomfører analysene som er avgjørende for om analysen er tilstrekkelig.
>
> Prosessen med involvering av ulik kompetanse for i så stor grad som mulig få kartlagt og "verifisert" dataene i analysen er viktig. Suksesskriteriet er å få presentert resultatet av analysen på en måte som gir beslutningstakere et godt grunnlag for sine beslutninger. (Vedlegg I).

Disse uttalelsene viser dermed at hensikten med analysen, kompetansen til deltakerne og sammensetningen av gruppa kan være viktigere enn valgt modell. Dette samsvarer godt med betraktningene som kom frem i FFIs rapport, vist til tidligere, som framhevet verdien av en strukturert tilnærming, kompetent og bredt sammensatt arbeidsgruppe, helhetlig perspektiv, kommunikasjon av risiko og usikkerhet, og ikke minst gjennomsiktighet, sporbarhet og etterprøvbarhet (Busmundrud et. al. 2015, s. 3). Primærdata fra undersøkelsen og sekundærdata viser dermed at endel kvalitative fellestrekk ved risikoanalyse kan være viktigere enn valgt modell.

Dersom vi tar et tilbakeblikk tilbake til dokumentanalysen så ble det påvist endringer i sikkerhetsloven, som i praksis innebærer at hverken ROS eller VTS tilfredsstiller gjeldende krav til risikovurdering (punkt 4.2.2, figur 11). Dette indikerer at det kan være hensiktsmessig å adressere svakheter ved dagens modeller individuelt, eller ved å satse alt på en sammenslått løsning som ivaretar de nye kravene. Intervjuet med ROS-informanten pekte i retning av en ny fellesmodell:

> Sannsynlighetsbegrepet og den veien det kommer til å ta, jeg tror veien videre blir at vi slår sammen disse to modellene. Og som research foran dette møtet snakket jeg med en dame som sitter i en gruppe som skal se på akkurat det. Vi har i sikkerhetsorganisasjonen i DSB jobbet mye med sikringsrisikometodikk. Og ikke minst verktøy for gjennomføring av risikoanalyser…. Det er verdiene vi skal skjerme og beskytte, uansett hva som skjer med dem, om verdien er et skjermingsverdig objekt etter sikkerhetsloven eller om det er et vannforsyningsanlegg, så er det likevel disse verdiene som vi skal ta vare på. Jeg har ikke noen tro på at dette miljøet er så stort at vi klarer å opprettholde to modeller (Vedlegg III).

VTS-informanten var mer tilbakeholden i forhold til en felles analysemodell, men setter døra på gløtt:

> NS 5814:2008 skal revideres i løpet av 2020. Altså den «gamle» ROS-standarden. Svar på spørsmålet blir dermed at det kommer an på hvor god den nye fellesmodellen blir. Dersom den ikke blir distinktiv nok for begge risikotypene vil det være bedre å rendyrke hver enkelt modell (Vedlegg II).

Begge intervjuene bekrefter dermed at metodikken må forbedres til å ivareta disse kravene som ble fremstilt i dokumentanalysen, (punkt 2.4.2) enten ved en fellesmodell eller ved forbedringer i de eksisterende. Inntil utviklingen av nye modeller er på plass innebærer dette at virksomheter underlagt sikkerhetsloven må ty til improvisasjon for å oppfylle kravene.

Både ROS og VTS har dermed svakheter som bør adresseres, hver for seg eller samlet.

6. Oppsummering, drøfting og konklusjon

I det følgende kommer en oppsummering av de viktigste funnene før vi går over i en drøfting av problemstillingen og konklusjon som besvarer problemstillingen.

6.1 Oppsummering av hovedfunn

Ytre rammefaktorer og instrumentalisme
Både spørreundersøkelsen, intervjuene og sekundærdata bekrefter antagelsen når det gjelder ROS. Modellen er etablert bransjestandard for mange aktører, men ut fra spørreundersøkelsen og intervjuer ble det bekreftet at det i hovedsak var et overordnet nivå, sektormyndighet eller en lovgiver som hadde tatt valget av modell på vegne av underliggende organisasjoner. Observasjonene bekrefter dermed det instrumentelle perspektivet med top-down tilnærming, i tillegg til standardisering ved tvungen isomorfisme.

Når det gjelder VTS så gir hverken primær- eller sekundærdata en lignede bekreftelse. Modellen har blitt etablert som en bransjestandard for endel securityorienterte aktører, men hovedparten av respondentene mente at det var organisasjonen selv som hadde tatt dette valget.

Institusjonalisme, sedvane og stiavhengighet
ROS-analysen er institusjonalisert i flere organisasjoner med preg av både sedvanetenking og stiavhengighet. De fleste som bruker modellen er fornøyd med dagens løsning og ønsker ingen endring. Dermed bekreftes kulturperspektivet fra institusjonell teori, så vel som normativ isomorfisme og begrenset rasjonalitet.

Funnene indikerer i tillegg at også VTS-analysen *kan* være institusjonalisert hos endel aktører. I likhet med ROS er det en mulighet for at de som bruker VTS er fornøyd med dagens løsning og ikke ønsker noen endring. Til tross for endel støtte fra bakgrunnsinformasjonen og teoriene har jeg ingen belegg for å forsvare denne hypotesen ut fra egne data. Det er imidlertid mulighet for at de som velger VTS av hensyn til spesialisering, også standardiserer prosedyren innad i- og mellom organisasjoner i samsvar med prinsippene for mimetisk og normativ isomorfisme.

Handlefrihet og rasjonelle valg, kunnskap og myteperspektivet.
Til tross for bakgrunnsinformasjon, teori og et av intervjuene finner jeg ikke grunnlag for å slå fast at ROS-modellen bekrefter disse perspektivene. ROS-modellen er både rasjonell og

kunnskapsbasert, men ut fra mine data er det for svakt grunnlag til å kunne fastslå at det er gjort et selvstendig valg basert på både rasjonalitet, kunnskap og handlefrihet. I lys av i de fleste tilfellene er det andre aktører enn organisasjonen selv som har stått for valget.

Både bakgrunnsinformasjonen og egne funn tegner et klart bilde av VTS-modellen som et rasjonelt, kunnskapsbasert og selvstendig valg for de fleste organisasjonene som bruker denne modellen. Videre så fremstår myteperspektivet som beskrivende for den oppslutningen modellen har fått i sikringsmiljøene siden 2014.

Kvalitative observasjoner

Bevisstheten omkring hensikten med selve analysen, kompetansen hos deltakerne og sammensetningen av gruppa kan være viktigere enn valg av modell. Observasjonen samsvarer bra med tidligere forskning (Busmundrud et. al. 2015, s. 3).

Dokumentanalysen identifiserte videre at både ROS og VTS har mangler i lys av den nye sikkerhetsloven med forskrift. Begge modellene har dermed svakheter som bør adresseres, hver for seg eller samlet. Intervjuene bekreftet at det arbeides med en ny fellesmodell som vil adressere disse manglene.

6.2 Drøfting

Undersøkelsen av ROS og VTS påviste distinkte forskjeller mellom modellene på hver av de uavhengige variablene ut fra nesten alle teoriperspektivene som inngikk i analysen.

Valget av ROS-modellen kan forklares ut fra to av variablene. For det første samsvarer funnene med top-down instrumentalisme og tvungen isomorfi. For det andre gir ROS forklaring ut fra det institusjonelle kulturperspektivet og stiavhengighet. To av tre uavhengige variabler kan dermed forklare valg av ROS. Instrumenalisme og institusjonalisme kan muligens forstås i en sammenheng. Det har jeg ikke forsket nærmere på.

Valget av VTS-modellen kan forklares som et rasjonelt og kunnskapsbasert valg hos organisasjoner som har ressurser til å ta et selvstendig valg (handlefrihet). I tillegg fremstår modellen som et godt eksempel på myteperspektivet fra ny-institusjonell teori. Det er likevel endel organisasjoner som bruker VTS ut fra et instrumentelt perspektiv, men de utgjør et mindretall i mitt datamateriale. I likhet med ROS er det trolig at også VTS er institusjonalisert noen steder, men datagrunnlaget ga ingen slik bekreftelse.

Begge modellene kan forklares ut fra rasjonelle valg-teorier i form av optimal eller begrenset rasjonalitet. Forskjellene gjøres altså gjeldende ut fra instrumentalisme, institusjonalisme og handlefrihet.

Basert på kvalitative observasjoner finner vi at begge modellene har identifiserte svakheter som burde adresseres, hver for seg eller samlet. Dersom en ny fellesmodell blir god nok til å erstatte dagens ROS og VTS, vil dette kunne gi en samfunnsøkonomisk gevinst med særlig relevans for organisasjoner som analyserer risiko knyttet til både utilsiktede hendelser og tilsiktede handlinger. Samtidig kan forventningene som følger av den nye sikkerhetsloven innfris. Dersom en ny fellesmodell skal oppnå anerkjennelse også hos de security-orienterte aktørene ligger det som en implisitt forutsetning at den blir sensitiv nok til å tilfredsstille deres spesialiserte behov. Hvis ikke kan det være bedre å rendyrke hver enkelt modell.

Observasjonen knyttet til en ny fellesmodell for å imøtekomme kravene fra sikkerhetsloven ligger litt på siden av problemstillingen og blir følgelig utelatt fra konklusjonen. Se ellers punkt 6.4.

6.3 Konklusjon

Jeg vil innlede konklusjonen med et tilbakeblikk på problemstillingen:

> Hva forklarer at vi har to risikomodeller i Norge og hva er bakgrunnen for at sikkerhets- og beredskapsmiljøene så langt ikke har klart å samle seg om en felles og omforent modell for risikoanalyse?

Resultatene av analysen viser gjennomgående forskjeller på ROS og VTS som risikomodeller og det er ulike faktorer som forklarer hvilken modell som blir valgt.

På analysen av *ytre rammefaktorer og instrumentalisme* fikk vi styrket hypotesen om at det instrumentelle perspektivet med top-down tilnærming og standardisering ved tvungen isomorfi er typisk for ROS. Når det gjelder VTS så var resultatet motsatt. Hverken primær- eller sekundærdata ga lignede bekreftelse, så på VTS ble denne hypotesen svekket.

Når det gjelder betydningen av *institusjonalisme, sedvane og stiavhengighet* så viser analysen at hypotesen på ROS ble styrket i lys av kulturperspektivet fra institusjonell teori, normativ isomorfisme og begrenset rasjonalitet. Analysen av VTS ga også noen indikasjoner på institusjonalisme, men ikke tydelig fra primærdataene, så hypotesen på VTS ble svekket.

Videre viser analysen at *handlefrihet og rasjonelle valg, kunnskap og myteperspektivet* hadde stor sammenheng med valget av modell. VTS-modellen representerer alle disse egenskapene på en overbevisende måte og hypotesen ble dermed styrket. ROS-modellen hadde i likhet med VTS et tydelig preg av rasjonalitet og kunnskap, men ikke handlefrihet eller myteperspektivet. Hypotesen på ROS ble dermed svekket.

Basert på *kvalitative observasjoner* ser vi at det til tross for distinksjonen er en rekke likheter mellom de to modellene. En god risikoanalyse bygger på en strukturert tilnærming med et verdifokus, kunnskap om truslene og ledelsesforankring. Gruppen bør bestå av kompetente analytikere som representerer både (teknisk) lokalkunnskap og overblikk, med en kvalitativ tilnærming som har transparens og etterprøvbarhet. Uansett hvilken modell man velger som et utgangspunkt, må risikobildet kunne presenteres for beslutningstakere på en overbevisende måte, med reflektert kommunikasjon av analysens validitet og graden av usikkerhet.

Både spørreundersøkelsen og intervjuene bekreftet at forskjellene mellom ROS og VTS stikker dypere enn de tekniske faktorene som inngår i metodeverktøyet isolert sett.

Forklaringen på at vi har to risikomodeller i Norge skyldes trolig at de er basert på ulike fagtradisjoner fra forskjellige miljø, noe som bekreftes ved å se på det teoretiske grunnlaget for hver av de. At modellene har blitt innført i ulike tidsepoker og i ulik kontekst forsterker skillelinjene.

Samfunnssikkerheten og beredskapen i Norge bygger på en lang tradisjon hvor utøverne stort sett er godt fornøyd med ROS-modellens robusthet og enkelhet. Dette forklares ut fra institusjonalisme, begrenset rasjonalitet og stiavhengighet. I kommuner er det typisk enkeltpersoner som arbeider med risiko, ganske isolert og ofte uten å inngå i et fagmiljø med risikokompetanse. For slike mennesker og deres beslutningstakere er lav brukerterskel en avgjørende faktor. Det er dermed hverken behov eller ønske om en annen modell, og sistnevnte rasjonale gir i lys av policyprosessen legitimitet til instrumentell sektorstyring og tvungen isomorfisme fra overordnede myndigheter.

Miljøer som arbeidet spesielt med beskyttelse av verdier- eller funksjoner mot tilsiktede handlinger observerte svakheter knyttet ROS-modellen, slik de oppfattet den på daværende tidspunkt. Kritikken gjaldt blant annet et uklart verdiperspektiv, overforenkling og underkommunikasjon av usikkerheten. Videre ble ROS kritisert for svakere sensitivitet knyttet til forskjellen mellom utilsiktede hendelser og tilsiktede handlinger hvor en gjerningsperson eller gruppe kan styre utviklingen i hendelsesforløpet. Dette er trolig forklaringen på at organisasjoner som driver med sikring har tatt et kunnskapsbasert og rasjonelt valg om å bruke VTS-modell. Forutsetningen for å kunne utvikle og etablere en ny metode forutsetter ressurser og en viss handlefrihet, noe som er mer typisk hos større organisasjoner.

Bakgrunnen for at sikkerhets- og beredskapsmiljøene så langt ikke har klart å samle seg om en felles og omforent modell bunner altså ut i kulturelle forskjeller, ulik forståelse av hva sikkerhet er for noe, ulik oppfatning om hvordan trusselen skal forstås, ulikt teoretisk utgangspunkt og ulike forutsetninger hos aktørene.

Dette forklarer bakgrunnen for at vi har to risikomodeller i Norge, samt årsakene til at sikkerhets- og beredskapsmiljøene ikke står samlet om en felles og omforent modell for risikoanalyse.

6.4 Forslag til videre forskning

Basert på datagrunnlaget ble det identifisert svakheter ved begge risikomodellene. Innovasjon er dermed å anbefale, og den bør helst springe ut fra miljøene som faktisk praktiserer analyse, og så langt det er mulig bygge på forskningsbasert kunnskap. En arbeidsgruppe er allerede i ferd med å adressere de behovene som er knyttet til overholdelse av sikkerhetslovens krav på i løpet av 2020.

Risikoanalyser og sikringstiltak kjennetegnes ved at så lenge de etablerte tiltakene ikke har blitt *prøvd* eller testet av de reelle påkjenningene de er ment til å tåle, så vil det være usikkerhet knyttet til om dimensjoneringen traff ambisjonsnivået for risikoanalysen. Både overdrevent robuste sikringstiltak og mangelfull sikring med påfølgende verditap er begge deler forhold som kan påføre samfunnet stor økonomisk slagside. Et sterkere søkelys på erfaringslæring fra både vellykkede og mislykkede enkeltcase som har blitt utsatt for de belastninger de reelt var designet for å tåle, kan være fruktbart. Ved å ta læring fra både suksesser og fiaskoer utledes ny kunnskap slik at både analysene og tiltakene kan optimaliseres. I et samfunnsøkonomisk perspektiv kan en slik utvikling bidra til å gjøre oss bedre, og på sikt også medføre økonomiske gevinster.

Litteraturliste

Andersen, E.S. (2005). *Prosjektledelse – et organisasjonsperspektiv.* (1. utg.) OSLO: NKI Forlaget

Andersen, Ø. (2006). *Frykter bilbomber mot regjeringskvartalet*. Hentet fra https://www.dagbladet.no/nyheter/frykter-bilbomber-mot-regjeringskvartalet/66252203

Aven, T. (2015). *Black swans. Improved risk assessment to better reflect the knowledge dimension and surprises*. Hentet fra https://www.uis.no/getfile.php/13263231/SEROS/rapport2015-blackswan-petromaks-28112015-sent.pdf

Baldersheim, H. og Rose, E. (2014). *Det Kommunale laboratorium*. (3. utg.) Bergen: Fagbokforlaget

Barane, J.E. (2014). *Et rasjonelt valg - om trefaktortilnærmingen til sikringsrisiko.* Hentet fra https://www.proakt.no/single-post/2014/12/09/Et-rasjonelt-valg-–-om-trefaktortilnærmingen-til-sikringsrisiko

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

Christensen, T. Egeberg, M. Lægreid, P. Roness, G. og Røvik, K.A. (2017). *Organisasjonsteori for offentlig sektor.* 3. utg. Universitetsforlaget AS, Oslo.

Digitaliseringsdirektoratet (2020). *Offentlige anskaffelser.* Hentet fra https://www.difi.no/fagomrader-og-tjenester/anskaffelser

DiMaggio, P. J. & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48* (2), s. 147-160. Hentet fra https://www.jstor.org/stable/2095101?seq=1

DSB (2014). *Veileder til helhetlig risiko og sårbarhetsanalyse i kommunen.* Hentet fra https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/veileder-til-helhetlig-risiko--og-sarbarhetsanalyse-i-kommunen/

DSB (2018). *Veileder til forskrift om kommunal beredskapsplikt* Hentet fra https://www.dsb.no/veiledere-handboker-og-informasjonsmateriell/veileder-til-forskrift-om-kommunal-beredskapsplikt/

Eriksson-Zetterquist, U., Kalling, T., Styhre, A. & Woll, K. (2014). *Organisasjonsteori*. Oslo: Cappelen Damm akademisk.

Espedal, B. og Kvitastein, O.A. (2012). *Rom for læring: betydningen av handlingsrom for ledelse.* Hentet fra https://www.magma.no/rom-for-laring-betydningen-av-handlingsrom-for-ledelse?tid=213203

Johannessen, A. (2009). *Introduksjon til SPSS*. 4. Utg. Abstrakt forlag AS. Otta.

Hill, M (2013). *The Public Policy Process*, (6. utg). New New York: Published 2014 by Routledge.

Høyer, H.C, Kasa, S. og Tranøy, B.S (2016). *Tillit, Styring, Kontroll*. Oslo: Universitetsforlaget AS.

March, J. og Simon, H. (1993). *Organizations*. 2. Utg. Blackwell Publishers, Cambridge, Massachusetts, USA.

Marsh, D. og Stoker, G. (2002). *Political Analysis. Theory and Methods in Political Science.* 2. Utg. Palegrave Macmillan, New York.

Moren, J. (2011). *Om reformer. En studie av kvalitetsreformen, Politireform 2000 og Kunnskapsløftet.* Hentet fra http://www.diva-portal.org/smash/get/diva2:410820/FULLTEXT01.pdf

Mærli, M.B, (2012). *Risikobasert sikring (security) og risikoreduksjon*. Notat til 22. Juli-kommisjonen. Hentet fra https://docplayer.me/14219493-Notat-8-12-risikobasert-sikring-security-og-morten-bremer-maerli-forsker-det-norske-veritas-risikoreduksjon-08-03-2012-www-22julikommisjonen.html

NKSB (2016). *Sikringshåndboka. Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje, spionasje og annen kriminalitet.* 2. utg. Utgitt av Forsvarsbygg.

NOU 2012: 4 (2012). *Trygg hjemme. Brannsikkerhet for utsatte grupper.* Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2012-4/id670699/sec3

NOU 2012: 14 (2012). *Rapport fra 22. juli-kommisjonen.* Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/

NSD (2020). NSD Personverntjenester. Hentet fra https://nsd.no/personvernombud/.

NSM (2015). *Terrorsikring. En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger.* Utgitt av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste. https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder_terrorsikring_2015_enkelts_final.pdf

NSM (2016). *Håndbok. Risikovurdering for sikring.* Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf

NSR (2017). *Er risikoanalysen din tilpasset dagens kriminalitetsbilde?* Hentet fra https://www.nsr-org.no/aktuelle-saker/er-risikoanalysen-din-tilpasset-dagens-kriminalitetsbilde-article980-110.html

Ringdal, K. (2001). *Enhet og mangfold. Samfunnsvitenskapelig forskning og kvantitativ metode*. Fagbokforlaget Vigmostad & Bjørke AS. 5892 Bergen

Salbu, B. (2019). *Tsjernobyl-ulykken.* Hentet fra https://snl.no/Tsjernobyl-ulykken

Sletten, S. (2018). *Oppdragsbasert risikovurdering i politiet: Hvilken metodikk egner seg best? Masteroppgave fra Universitetet i Stavanger.* Hentet fra https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2508240/Sletten_Stein.pdf?sequence=1&isAllowed=y

Solbakken, M.S. og Dahle, E.A (2019). *Alexander L. Kielland-ulykken*. Hentet fra https://snl.no/Alexander_L._Kielland-ulykken

Standard Norge (2008). *Norsk Standard NS 5814:2008. Krav til risikovurderinger* Kan hentes fra *https://www.standard.no/nyheter/nyhetsarkiv/kvalitet-og-risiko/2013/risikovurderinger---ns-5814/*

Standard Norge (2014). *Norsk Standard NS 5832:2014. Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse.* Kan hentes fra https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=718202

Stranden, R (2019). *Sikring. En innføring i teori og praksis.* Gyldendal Norsk Forlag AS. 1. utgave, 1. opplag 2019.

Söderlund, J (2007). *Projektledning & projektkompetens. Perspektiv på konkurrenskraft.* Liber AB, 205 10 Malmö.

Taleb, N.N (2010). *The Black Swan. The Impact of the Highly Improbable*. The Random House Publishing Group. (Paperback Edition). New York.

Vedleggsoversikt

Rapport fra «Modeller for risikoanalyse i Norge»

Innhentede svar pr. 7. februar 2020 11:02

- Leverte svar: **141**
- Påbegynte svar: **0**
- Antall invitasjoner sendt: **0**

Med fritekstsvar

Innledning

Innenfor sikkerhets- og beredskapsmiljøer i Norge er det spesielt to modeller som brukes for å analysere risiko. Den ene er risiko- og sårbarhetsanalysen (ROS) som fokuserer på sannsynlighet og konsekvens. Den andre er sikringsrisikoanalysen som fokuserer på verdi, trussel og sårbarhet (VTS). Begge har til hensikt å analysere hva slags og hvor mye risiko organisasjonen eller entiteten står ovenfor. Modellene har imidlertid forskjeller av både teoretisk, institusjonell og profesjonsfaglig karakter.

Målgruppen for undersøkelsen er alle som har kjennskap til risikoanalyse, enten du har bakgrunn fra sikkerhet og beredskap, statlig eller kommunal styring, internasjonalt arbeid, næringslivet eller uavhengige organisasjoner. Kjenner du til risikoanalyse er jeg glad for å gi deg muligheten til å bidra med å utvikle ny kunnskap ved Høgskolen i Innlandet. Undersøkelsen består av 34 spørsmål og tar 10-15 minutter.

Kjenner du andre med kompetanse på risikoanalyse? For å nå bredt ut er undersøkelsen satt åpen for alle. Jeg setter stor pris på om du vil bistå mitt arbeid med å videresende lenken til personer som har kompetanse på risikoanalyse i ditt nettverk. Uten deres hjelp når ikke undersøkelsen sitt fulle potensial.

Problemstilling

Hva forklarer at vi har to risikomodeller i Norge og hva er bakgrunnen for at sikkerhets- og beredskapsmiljøene så langt ikke har klart å samle seg om en felles og omforent modell for risikovurderinger?

Jeg vil undersøke om valget av analysemodell (ROS eller VTS) kan skyldes:

- Ytre rammefaktorer eller sektorkrav, lover og regler
- Kultur eller subjektiv identitet hos aktørene, yrkesbakgrunn, kunnskap eller egeninteresser
- Organisasjonsteoretiske forklaringer, som institusjonalisme (studiet av institusjoner) eller isomorfisme (teorier om trender og standardisering)
- Andre årsaker.

Studien gjennomføres uavhengig av ytre premissgivere i sikkerhets- og beredskapssektorene eller interne forhold hos min egen arbeidsgiver som er Departementenes sikkerhets- og serviceorganisasjon (DSS).

Personvern

Nettskjema er en sikker løsning for datainnsamling levert av Universitetet i Oslo. Formatet er anerkjent både av NSD Personvernombudet og Regionale etiske komiteer for helseforskning (REK).

Spørreundersøkelsen er fullstendig anonymisert og ingen innsamlede opplysninger knyttes til deg som person.

Med vennlig hilsen

Bjørn Melandsø Kjelsaas

Masterstudent i offentlig ledelse og styring (MPA)

Høgskolen i Innlandet

Elektronisk samtykke

Trykk "Ja" dersom du blir med på spørreundersøkelsen. Du avgir da elektronisk samtykke til lagring av data (ingen personopplysninger). Lukk nettleseren dersom du vil forlate undersøkelsen uten å etterlate noen spor. Trykk "Nei" dersom du ønsker å levere en blank besvarelse. *

Svar	Antall	Prosent	
Ja	138	**97,9 %**	
Nei (blank besvarelse)	3	**2,1 %**	

Innenfor sikkerhets- og beredskapsmiljøer kan det være ulike oppfatninger om begreper og fagterminologi, alt etter hvor man jobber og hvilken bakgrunn man har. Spørsmål 1-8 handler om terminologi. Obligatoriske spørsmål er merket med stjerne. Velg det svaralternativet du mener er mest riktig, sett fra ditt ståsted.

1. Blant følgende svaralternativer, hva legger du i begrepet sikkerhet? *

Svar	Antall	Prosent
En reell eller opplevd tilstand som innebærer fravær av uønskede hendelser, frykt eller fare	92	65,2 %
Hvor sannsynlig det er at uønskede situasjoner kan oppstå	4	2,8 %
Å være forberedt til innsats for å møte uventede kritiske situasjoner	7	5 %
At man har etablert systemer for å håndtere uønskede hendelser eller ulykker	51	36,2 %

2. Begge de engelske begrepene "safety" og "security" blir ofte oversatt til sikkerhet på norsk. Er du kjent med hvilken forskjellig betydning disse begrepene kan ha? *

Svar	Antall	Prosent
Ja	136	98,6 %
Nei	2	1,4 %

3. Om du svarte ja på forrige spørsmål, hvilket alternativ beskriver best safety?

Svar	Antall	Prosent
En reell eller opplevd tilstand som innebærer fravær av uønskede hendelser, frykt eller fare	22	16,3 %
Sikkerhet mot uønskede utilsiktede hendelser	109	80,7 %
Sikkerhet mot uønskede tilsiktede hendelser	4	3 %

4. Hvilket av svaralternativene beskriver best security?

Svar	Antall	Prosent
En reell eller opplevd tilstand som innebærer fravær av uønskede hendelser, frykt eller fare	5	3,7 %
Sikkerhet mot uønskede utilsiktede hendelser	6	4,4 %
Sikkerhet mot uønskede tilsiktede hendelser	124	91,9 %

5. Blant følgende svaralternativer, hva innebærer beredskap? *

Svar	Antall	Prosent

Svar	Antall	Prosent
En reell eller opplevd tilstand som innebærer fravær av uønskede hendelser, frykt eller fare	0	0 %
Hvor sannsynlig det er at uønskede situasjoner kan oppstå	0	0 %
Å være forberedt til innsats for å møte uventede kritiske situasjoner	73	51,8 %
At man har etablert systemer for å håndtere uønskede hendelser eller ulykker	93	66 %

6. Blant følgende svaralternativer, hva legger du i begrepet risiko? *

Du kan velge inntil 2 alternativer

Svar	Antall	Prosent
Utrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarheter ovenfor den spesifiserte trusselen	63	44,7 %
Utrykk for kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse	99	70,2 %
Begrepet brukes som regel om negative eller farlige hendelser, men kan også innebære positive hendelser/muligheter som kan oppstå	50	35,5 %
Mulig uønsket handling som gir en negativ konsekvens	5	3,5 %
Ethvert forhold eller enhver enhet med potensiale til å forårsake en uønsket hendelse	19	13,5 %

7. Blant følgende svaralternativer, hva legger du i begrepet trussel? *

Du kan velge inntil 2 alternativer

Svar	Antall	Prosent
Utrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarheter ovenfor den spesifiserte trusselen	28	19,9 %
Utrykk for kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse	6	4,3 %
Begrepet brukes som regel om negative eller farlige hendelser, men kan også innebære positive hendelser/muligheter	6	4,3 %
Mulig uønsket handling som gir en negativ konsekvens	71	50,4 %
Ethvert forhold eller enhver enhet med potensiale til å forårsake en uønsket hendelse	85	60,3 %

8. Etter ditt syn, er risiko og trussel omtrent det samme, eller representerer begrepene ulik betydning? *

Svar	Antall	Prosent
Ja, samme betydning	3	2,2 %
Nei, ulik betydning	131	94,9 %
Vet ikke / vil ikke svare	4	2,9 %

Så over til noen spørsmål om risiko- og sårbarhetsanalyse (ROS).

9. Har du, gjennom ditt yrke (eventuelt studier) kjennskap til risiko- og sårbarhetsanalyser (ROS)? *

Svar	Antall	Prosent
JA	137	99,3 %
NEI	1	0,7 %

10. Har du selv utført, eller bidratt til gjennomføring av risiko- og sårbarhetsanalyse i din nåværende eller tidligere stilling?

Svar	Antall	Prosent
JA	124	90,5 %
NEI	13	9,5 %

Du blir nå presentert for noen påstander som angir mulige årsaker til at organisasjoner har valgt eller ikke valgt å gjennomføre risiko- og sårbarhetsanalyser (ROS). Velg det svaralternativet du tror er mest riktig eller hopp over. Dersom du ikke har kjennskap til ROS-modellen kan du gå til bunn av siden og klikk "Neste side" for å hoppe direkte til spørsmål 18.

11. Mulige årsaker til bruk av ROS-modellen

Svar	Antall	Prosent
Vi (vår organisasjon) har kjennskap til bruk av denne modellen	121	95,3 %
Vi (vår organisasjon) har såvidt jeg vet ikke kjennskap til bruk av denne modellen	6	4,7 %

12. Mulige årsaker til bruk av ROS-modellen

Svar	Antall	Prosent
Jeg/vi tror denne modellen er best egnet for å analysere risiko i vår organisasjon	49	39,8 %
Denne modellen er ikke nødvendigvis best for å analysere risiko. Jeg/vi bruker ROS for å oppfylle krav fra overordnet nivå eller lover og forskrifter	74	60,2 %

13. Mulige årsaker til bruk av ROS-modellen

Svar	Antall	Prosent
Vår organisasjon har tatt et selvstendig valg ved å bruke denne modellen.	60	51,7 %
Vår organisasjon har ikke tatt et selvstendig valg ved å bruke denne modellen. Overordnet myndighet/nivå har tatt dette valget på vegne av vår sektor.	56	48,3 %

14. Mulige årsaker til bruk av ROS-modellen

Svar	Antall	Prosent
Det var et kunnskapsbasert valg for vår organisasjon å bruke denne modellen for å analysere risiko	51	42,9 %
Det var ikke nødvendigvis et kunnskapsbasert valg for vår organisasjon å bruke denne modellen, det er pålagt eller har blitt sedvane over tid.	68	57,1 %

15. Mulige årsaker til bruk av ROS-modellen

Svar	Antall	Prosent
Vi bruker ROS for å bli mere lik andre sammenlignbare organisasjoner, standardisering.	69	62,7 %
Vi bruker ROS av hensyn til spesialisering, vi har oppgaver som skiller seg fra annen risikohåndtering.	41	37,3 %

16. Hvilke av de følgende egenskaper mener du kjennetegner Risiko- og sårbarhetsanalyse?

Velg inntil 7 styrker og svakheter med ROS

Svar	Antall	Prosent
Lettfattelig, enkel å gjennomføre	69	48,9 %
Komplisert, krevende å gjennomføre	23	16,3 %
Enkelt å visualisere resultatene i en figur/modell	73	51,8 %

Svar	Antall	Prosent
Krevende å visualisere resultatene i en figur/modell	8	5,7 %
Tar hensyn til sannsynlighet basert på frekvens, kjent historikk eller kvalitativ vurdering.	73	51,8 %
Tar ikke hensyn til sannsynlighet basert på frekvens, historikk eller kvalitativ vurdering.	15	10,6 %
Metoden er forankret i kriminologisk teori som identifiserer faktorer som må være tilstede for at det skal oppstå et sikkerhetsproblem	2	1,4 %
Metoden er anerkjent av både norsk og internasjonal litteratur på området	70	49,6 %
Metoden er egnet for analyse av risiko som skyldes utilsiktede uønskede hendelser	77	54,6 %
Metoden er egnet for analyse av risiko som skyldes tilsiktede uønskede hendelser	33	23,4 %
Metoden er egnet til å oppfylle krav nedfelt i lover og forskrifter	89	63,1 %
Metoden er egnet til å danne et beslutningsgrunnlag ved at risiko identifiseres. Gjør det lettere å ta informerte valg.	97	68,8 %

17. Etter ditt syn, hvorfor velger organisasjoner å bruke ROS-modellen? (Risiko- og sårbarhetsanalyser)

- For sånn har vi alltid gjort det. Prosessen er forholdsvis enkel og man får en grei (om noe overfladisk) oversikt.
- se 16
- Enkelt og godt kjent modell. Tradisjonelt kultur for å risikovurdere utilsiktede hendelser fremfor tilsiktede.
- På grunn av fordelene jeg har krysset av på over. I tillegg kan ROS-analyse gjennomføres også for risiko knyttet til tilsiktede handlinger, men da må sannsynligheten være kunnskapsbasert (ikke frekvensbasert) og den må settes basert på informasjonen vi har om verdi, trussel og sårbarhet.
- Som regel fordi det finnes kompetanse, erfaring og gode standarder for denne metoden
- Lett tilgang på veiledere og ferdige eksempler på akseptkriterier
- Etatstyrer krever det.
- Krav fra PBL, håndterer HMS på byggeplass godt
- Velprøvd metode. Finpusset gjennom tiår. Mye god internasjonal litteratur. Standard metode i de fleste modne sikkerhetsmiljøer i forskjellige industrier.
- Anerkjent risikoanalyse innen risikohåndtering i blant annet oljesektoren og DSB. Forenkler fremstillingen av risiko ved at den visualiseres i en sannsynlighets/konsekvensmatrise. Forenkler ledelsesbeslutninger.
- Den er kjent, lettfattelig og lett å læres opp i.
- fordi andre kommuner gjør det
- Lik praksis på all risikostyring, mindre krav til ulik kompetanse og lik risikommunikasjon.
- For å ha gjort det som overordnet ledelse forventer og for p ha ryggen fri dersom noe skal skje. Skal den ha effekt som ønsket må hele organsiasjonen delta i utarbeidelse

- Per nå - beste metodikk for å kartlegge risiko og sårbarhet som dekker både utilsiktede hendelser og tilsiktede handlinger. Kan tilpasses til alt fra overordnet kartlegging av ROS til detaljerte analyser av spesifikke system/objekt.
- Fordi de er enkle
- Mange har gjort det før oss, det finnes erfaring og «best practice»
- En etablert standard som man kjenner igjen fra andre forretningsområder som prosjekt og økonomistyring hvor frekvenser og usikkerhet er innarbeidet i et felles risikobilde eller risikoregister.
- Nivået over bestemmer
- Mest for å tilfredsstille lovkrav, men forhåpentligvis like mye for å kartlegge og forstå og forberede mulige tiltak mot ulike risiki
- Prioritering av for få ressurser. ROS kan si noe om "restrisiko" og behovet for å vurdere ytterligere tiltak.
- Enkelt og den mest kjente metoden
- Gir en enkel og oversiktlig beskrivelse av risiko - forståelig også for ikke-fagpersoner.
- Det er det kjente og sikre valget. Gjenkjennbart.
- Er et kjent begrep
- De bruker muligens ros på risiko som ikke omfatter tilsiktede uønskede hendelser.
- Dette er det enkleste modellen for å danne seg en ROS på.
- Ukjent med alternativer eller pålagt gjennom rapporteringskrav.
- Lovkrav
- ROS analyser legger grunnlag for beredskapsplaner, som igjen legger grunnlag for øving og evaluering.....jfr. Sivilbeskyttelsesloven.....
- Den er enkel å implementere i organisasjonen blant mennesker som ikke jobber med ROS TIL daglig. Konsekvensverdiene kan tilpasses virksomheten, slik at den gir et relativt oversiktlig bilde av forholdet mellom sannsynlighet og konsekvens.
- Velkjent tilnærming med en enkel og kraftig visualisering av risikobilde
- Den er forholdsvis enkel (men gjøres ofte unødvendig komplisert)
- Sikkert og ikke sikring, pålagt (stat, dsb)
- Dett bestemmer fagmyndighetene
- Jeg mener det er fordi det er den modellen som er mest innarbeidet i organisasjoner her til lands.
- Det er "bransjestandard" og nærmest et krav. Moderne sikkerhetsteori er ikke vår organisasjon spes. moden for
- Anerkjent modell som tilsynelatende er enkel og gir tydelige svar
- Godt innarbeidet metodikk, som også lar seg anvende i forhold til risikoer som ikke er utløst av en trusselaktør
- For å beskrive risiko, ta beslutnikger om risikohåndtering og dimensjonere forebyggende og beredskapsarbeid
- Mangle de kunnskap til alternativer.lav metodisk kompetanse.
- Enkel og god nok
- God kartlegging som opp mot hverandre kan trekke frem dimensjonerende uønskede hendelser
- Enkelt, lovpålagt i offentlig sektor. Gir en lettfattelig visualisering for ledergrupper. Er også blitt standard for formidling av risiko.
- Enkel, mindre komplsert å gjennomføre
- Krav

- Det mangler gode mindre subjektive metoder
- Andre bruker det. Få alternativer. Tilgjengelighet
- anbefalt innen helsevesen og derfor lett å få gehør for
- Av egen erfaring brukes denne for den er standardisert og "enkel" å benytte i en ellers kompleks oppgave, og gir resultater godt visuelt fremstilt. Den er lett å forholde seg til. Dog kreves erfaring og kompetanse i gjennomføring, for å ikke undertrykke elementer som f.eks. usikkerhet.
- Metoden enkelte kjenner til, lett tilgjengelig. Betyr ikke du kan/er god på å bruke den.
- Pålegg om å gjøre slik analyse i f.eks. kommuner. Andre velger det kanskje fordi det er den modellen de kjenner til, kopierer kommuner og andre som bruker ROS.
- Fokus i offentlig sektor har ligget på ROS, mye grunnet at det har kommet som direkte eller indirekte krav innen sektorlovgivning for en del sektorer. Veiledere og annet støttemateriell fokuserer i stor grad kun på ROS-metodikk, selv om andre former for risikovurdering kan være gunstigere.
- Enkel struktur, fremmer refleksjon hos de som deltar i analysen
- Mest kjent
- For å finne fram til svakheter og/eller mangler ved sikkerheten i en virksomhet og implementere tiltak for å oppnå et forsvarlig sikkerhetsnivå sett i forhold til de sikringsmål som er satt for virksomheten.
- Gir en strukturert tilnærming til verdier, trusler og sårbarheter, herunder vurdering av eventuelle sinringstiltak.
- Vår organisasjon bruker både ROS og sikringsrisikoanalyse, avhengig av hvilket type scenario som skal vurdres. Dette er kunnskapsbasert og gir best mulig helhetlig resultat, men er vanskelig å sammenfatte i en overordnet rapport på virksomhetsnmivå.
- Jeg tror ROS-analyser brukes fordi det er et innarbeidet begrep når sikkerhet skal ivaretas på ulike nivåer. Det foreligger flere modeller/skjemaer som benyttes, men alle jeg har sett forholder seg til trussel multiplisert med konsekvens. Man kunne like gjerne benyttet en annen modell, så lenge den er kjent i hele organisasjonen
- Sedvane
- Det er enkelt. Den er det alle er kjent med. Funker helt fint mot utilsiktede hendelser. Ikke egnet til tilsiktede hendelse.
- Gjenkjennbare, og at metoden er fleksibel til å vurdere både utilsiktet og tilsiktede hendelser.
- Den er enkel og kjapp å gjennomføre
- Kjennskap, Likhet til andre org.
- Noen organisasjoner benytter begge metoder for forskjellige vurderinger (sec / safety). For egen organisasjon benyttes begge metoder for forskjellige oppgaver. Spørsmål 12-15 er egentlig begge svaralternativer korrekt.
- Det finnes ikke bare en modell, mange varianter. Hos oss finnes det en variant (som ikke brukes), har vært borti andre verktøy andre steder
- Sedvane
- Ha oversikt over og kunne dokumentere hva organisasjonen har kartlagt av risikofaktorer som kan true måloppnåelse
- .
- Enkel metode for safety, hvor risikoverdien er viktigere enn økonomiske interesser. Mer i offentlig enn i sivile bedrifter. Lett visuelt bilde med risikomatrise.
- Kjent modell
- Utdatert begrep. Vi bruker "Risikovurdering"
- Oslo kommunes valg
- For å kunne lettere håndtere risiko- og sårbarhetssituasjoner.
- for å vurdere SAFETY-risks

- Strukturert og anerkjent metode
- Det er enkelt
- Fordi de er kjent med denne og ikke nødvendigvis 3-faktor modellen (VTS).
- Fordi det er den modellen man behersker.

Så noen spørsmål om sikringsrisikoanalyse (VTS).

18. Har du, gjennom ditt yrke (eller studier) kjennskap til sikringsrisikoanalyser (VTS)? *

Svar	Antall	Prosent
JA	100	**72,5 %**
NEI	38	**27,5 %**

19. Har du selv utført, eller bidratt til gjennomføring av sikringsrisikoanalyse (VTS) i din nåværende eller tidligere stilling?

Svar	Antall	Prosent
JA	72	**52,6 %**
NEI	65	**47,4 %**

Du blir nå presentert for noen påstander som angir mulige årsaker til at organisasjoner har valgt eller ikke valgt å gjennomføre sikringsrisikoanalyser (VTS). Velg det svaralternativet du tror er mest riktig eller hopp over. Dersom du ikke har kjennskap til VTS-modellen kan du gå til bunn av siden og klikk "Neste side" for å hoppe direkte til spørsmål 27.

20. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent
Vi (vår organisasjon) har kjennskap til bruk av denne modellen	77	**72 %**
Vi (vår organisasjon) har såvidt jeg vet ikke kjennskap til bruk av denne modellen	30	**28 %**

21. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent
Jeg/vi tror denne modellen er best egnet for å analysere risiko i vår organisasjon.	49	**62 %**
	30	**38 %**

Svar	Antall	Prosent
Denne modellen er ikke nødvendigvis best for å analysere risiko. Jeg/vi bruker VTS for å oppfylle krav fra overordnet nivå eller lover og forskrifter.		

22. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent
Vår organisasjon har tatt et selvstendig valg ved å bruke denne modellen	59	**75,6 %**
Vår organisasjon har ikke tatt et selvstendig valg ved å bruke denne modellen. Overordnet myndighet/nivå har tatt dette valget på vegne av vår sektor	19	**24,4 %**

23. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent
Det var et kunnskapsbasert valg for vår organisasjon å bruke denne modellen for å analysere risiko	53	**70,7 %**
Det var ikke nødvendigvis et kunnskapsbasert valg for vår organisasjon å bruke denne modellen, det er pålagt eller har blitt sedvane over tid.	22	**29,3 %**

24. Mulige årsaker til bruk av VTS-modellen

Svar	Antall	Prosent
Vi bruker VTS for å bli mere lik andre sammenlignbare organisasjoner, standardisering.	19	**26,8 %**
Vi bruker VTS av hensyn til spesialisering, vi har oppgaver som skiller seg fra annen risikohåndtering.	52	**73,2 %**

25. Hvilke av de følgende egenskaper kjennetegner etter ditt syn sikringsrisikoanalyse?

Velg inntil 7 styrker og svakheter med VTS

Svar	Antall	Prosent
Lettfattelig, enkel å gjennomføre	22	**15,6 %**
Komplisert, krevende å gjennomføre	38	**27 %**
Enkelt å visualisere resultatene i en figur/modell	20	**14,2 %**
Krevende å visualisere resultatene i en figur/modell	35	**24,8 %**

Svar	Antall	Prosent
Tar hensyn til sannsynlighet basert på frekvens, kjent historikk eller kvalitativ vurdering.	30	21,3 %
Tar ikke hensyn til sannsynlighet basert på frekvens, historikk eller kvalitativ vurdering.	29	20,6 %
Metoden er forankret i kriminologisk teori som identifiserer faktorer som må være tilstede for at det skal oppstå et sikkerhetsproblem	40	28,4 %
Metoden er anerkjent av både norsk og internasjonal litteratur på området	36	25,5 %
Metoden er egnet for analyse av risiko som skyldes utilsiktede uønskede hendelser	13	9,2 %
Metoden er egnet for analyse av risiko som skyldes tilsiktede uønskede hendelser	71	50,4 %
Metoden er egnet til å oppfylle krav nedfelt i lover og forskrifter	38	27 %
Metoden er egnet til å danne et beslutningsgrunnlag ved at risiko identifiseres. Gjør det lettere å ta informerte valg.	50	35,5 %
Vet ikke	10	7,1 %

26. Etter ditt syn, hvorfor velger organisasjoner å bruke VTS-modellen? (Sikringsrisikoanalyser)

- Litt sånn "mote" analyseteknikk
- se 25
- Bedre egnet modell mtp analyser av tilsiktede hendelser
- Mange velger nok VTS fordi de mener man ikke kan si noe om sannsynlighet knyttet til risiko for tilsiktede handlinger, jeg mener man kan si noe om sannsynlighet, men at den ikke må være frekvensbasert, den må være kunnskapsbasert. Jeg mener man kan benytte seg av elementer fra både tofaktor og trefaktor når man gjør en risikovurdering. Basert på verdi, trussel og sårbarhet kan man si noe om sannsynlighet (kunnskapsbasert) og konsekvens. Metodene er egentlig ikke så forskjellige i praksis, da ROS-analyse også ser på verdier, trusler (eller farer) og sårbarhet. Den største forskjellen ligger i hvordan risikoen blir presentert.
- Enkelte virksomheter har behov for å vurdere trusler og scenarioer som det er vanskelig å sette sannsynlighet og frekvens på. Slike scenarioer krever en kvalitativ vurdering. Dette er et bevisst og kvalifisert valg
- Kjenner ikke til modellen
- Dekker tilsiktede hendelser og ikke bare HMS på byggeplass
- Oppfattes som et krav innen enkelte fagfelt, særlig innen fysisk sikring
- Det er utfordrende å beskrive sannsynligheten for at en tilsiktet uønsket handling vil inntreffe fordi ofte mangler man et solid datagrunnlag for å kunne gjøre presise prediksjoner. Ved å fokusere på verdiers sårbarheter overfor trusler vil det være enklere å identifisere hvilke sikringstiltak som bør implementeres.
- Vi bruker VTS inn mot aktiviteter med høyere trusselnivå. Alt vurdres etter NS:5814 og aktivitet som ut ifra trusselvurdering gjort av andre aktører (PST) som da har forhøyet trussel for tilsiktede uønskede handlinger vurderes etter NS:5832.
- Styrte føringer om metode valg, manglende kjennskap til bruk av risikomodeller.

- Per nå - beste metodikk for å identifisere risiko knyttet til tilsiktede handlinger (verdier, trusselaktører, kapasitet, sårbarhet). Supplerende verktøy til ROS som gir annen innsikt - kan ikke erstatte hverandre, men kan med fordel kobles mye bedre sammen.
- Denne modellen er på tur inn og vil nok erstatte ros analysen.
- Populære metode blitt, selv om det i utgangspunktet er laget for byggningsbransjen, men er nå også blitt omfavnet av Cyber Nasjonalt, så det er litt møte ute å gå her. Internasjonalt er ISO 31000 fortsatt mest brukt. Internasjonalt benyttes også en trefaktormodell til Risiko bestående av variablene likelihood impact and vulnerability/controllability.
- Egnet til å identifisere risiko for tilsiktede alvorlige uønskede hendelser
- Gir, etter mitt syn, et bedre bilde av risiko. Gjør oss lettere bevisste våre sårbarheter.
- Fordi den godt håndterer tilsiktede uønskede handlinger
- Kunnskap om security og de behov security medfører. Bruk av relevante internasjonale standarder (IRAM2, FEMA, NIST 800-30, etc).
- Tilsiktede hendelser som ikke er like lett å analysere i ROS metodikk
- Vet ikke, er ikke kjent med systemet.
- VTS analyse er bedre enn ROS på flere måter. Den er langt mer basert på faktabasert parametere enn ROS.
- Lite kunnskap om hvordan virksomheten kan forholde seg til sannsynlighet knyttet til tilsiktede hendelser (bayesiansk sannsynlighet)
- VTS er ikke en unik norsk modell, men brukt internasjonalt i mange år. Du antar at risikoforståelsen mellom safety og security er ulik, det er det ulike oppfatninger av. VTS identifiserer de sentrale elementene i et sikringsscenario, selv i ROS ser man på vts.
- Bruker ikke VTS
- Konkret
- Noen ganger fungerer denne metodikken best. Den krever mer faglig tyngde for å gjennomføres, spesielt når man evaluerer styrken på sikringstiltakene opp mot trusselen, men sammenhengen mellom verdi, trusselaktør, sårbarhet og tiltak kommer frem på en måte som gjør at det er lettere for å få gjennomslag for foreslåtte tiltak.
- Min etat har vedtatt at denne passer best til å vurdere risiko.
- Godt egnet der det er viktig å identifiserer verdi. Dette kan eks bidra til å styre hvor sikringstiltakene bør settes inn, og hva som trenger mindre sikring.
- Vi bruker primært ROS.
- For å tilfredsstille standarder og forskrifter
- Egnet til formålet
- Avhengig av virke og kompleksitet, men modellen er logisk og forståelig men kan dog bli kompleks og sier lite om prioritering og sannsynlighet om man ikke har erfaring nok til å tolke det. Modellen kommuniserer godt hvilke faktorer som er inkludert.
- Best egnet til sikringsrisiko
- Denne modellen velges nok ut fra om man arbeider med sikring mot tilsiktede handlinger. Der har det blitt vanlig å følge noen standarder.
- Organisasjoner som primært fokuserer på tilsiktede hendelser finner nok at VTS eller lignende vurderinger er lettere å gjennomføre, da en unngår å måtte tallfeste forventet frekvens for hendelsestyper som er sjeldne, slik som f.eks. terror. Erfaringsmessig har denne problemstillingen vært tilstede i alle ROS-analyser/grovanalyser undertegnede har gjennomført hvor terror/masseskade på grunn av vold o.l. har vært en vurdert hendelse.
- Avhengig av problemstillingen
- Av standariseringshensyn og vedlikehold av analysen over tid og er en del av CIM.
- Som punkt 17.
- VTS er best egnet for den type hendelser vi i hovedsak står overfør, dvs tilsiktede uønskede hendelser.

- Dekker mer enn ROS
- Det er en god standard for tilsiktede hendelser.
- For å avdekke sårbarhetene og tette gapene mer effektivt
- Fordi bruk av kun sannsynlighet ikke er dekkende
- VTS er best egnet for lavfrekvente handlinger med store konsekvenser. VTS metodikken er basert på tanken om samspillet mellom en verdi, en trusselaktør og de sårbarhetene som kan utnyttes for å påvirke verdien i den til enhver tid gitte situasjon. Ergo må endringer i situasjonen vurderes som en faktor i trusselvurderingen. En slik faktor er ikke lett i en ROS metode, da sannsynliggjøring av en eventuell situasjonsendring ikke lar seg beskrive eller tallfeste. Organisasjoner som velger VTS har som oftest kompetanse innen denne form for metodikk.
- VTS-modellen angir en metodikk hvor verdi, trusler og sårbarheter kartlegges og beskrives -og gir grunnlag for mulighetsrommet for at sårbarheter kan utnyttes når gitte faktorer er tilstede. Det vil være usikkerhet knyttet til analyseresultatene i bg. modellene.
- Gir en mer detaljert beskrivelse av forventet/vurdert effekt av tiltak
- Krav til bruk. Mulig denne er best når økonomiske verdier er viktigere enn menneskers sikkerhet. Høy brukerterskel da verdi-begrepet er vanskelig. Mangler en god pedagogisk visuell fremstilling. Så lang ikke møtt andre studenter som har hatt dette gjennom studier, slår deg i trynet når du kommer i arbeidslivet.
- Ikke så kjent i Norge
- Vi bruker både Sannsynlighet/Konsekvens og VTS
- Mangler data for å vurdere sannsynlighet
- For å forhindre sårbarhet
- Fordi det er umulig å anslå sannsynligheten for anslag !
- Bedre egnet for å avdekke spesifikke trusler og realistiske tiltak
- Fordi den hensyntar «hjørnerisko»; hendelser som ikke har skjedd/lav frekvens, med potensielt høy konsekvens. Selv om noe ikke har inntruffet før, vil det skje dersom trusselaktør får intensjon og kapabilitet.
- Spesialiserte behov, objekter.

27. Etter ditt syn, bør sikkerhets- og beredskapsmiljøene i Norge samle seg om en felles modell for risikovurderinger? *

Svar	Antall	Prosent
Sikkerhets- og beredskapsmiljøene bør samle seg om ROS-modellen da denne er best egnet for helhetlig risikostyring	7	**5,1 %**
Sikkerhets- og beredskapsmiljøene bør samle seg om VTS-modellen da denne er best egnet for helhetlig risikostyring	8	**5,8 %**
Begge modellene er nyttige i seg selv, men hverken ROS- eller VTS modellen er fullt ut dekkende for all risikostyring	91	**65,9 %**
Sikkerhets- og beredskapsmiljøene bør samle seg om et tredje alternativ for vurdering av risiko	10	**7,2 %**
Vet ikke	22	**15,9 %**

26. Hva er etter ditt syn det viktigste suksesskriteriet for å gjenomføre en god risikoanalyse?

- 1.en tydelig mandat men som samtidig ikke legger for sterke føringer 2.gode prosessledere 3. Et godt analysemateriell (dette krever at involverte i analysearbeidet leverer pålitelig data som er forankret i fagmiljøet som representeres) 4. Et analytisk rammeverk som er tilpasset oppgaven (det finnes jo et hav av metoder å velge mellom)
- God kjennskap til virksomheten
- Tilstrekkelig ressurstilgang i selve analysen og ved revisjoner av denne, dette henger sammen med risikoerkjennelse og ledelsesforankring av risikoerkjennelse. Dessverre oppleves lite ressurstilgang i det forebyggende (proaktive) sporet. Ressurser stilles til rådighet når man tvinges til det i form av gjennopprettende tiltak etter en uønsket hendelse
- Jeg mener vi ikke bør se på dette så sort / hvitt som det gjøres i dag. Innenfor begge metodene ser man på verdier (scoping av analysen), trusler eller farer, og sårbarheter. Det kan være nyttig å si noe konkret om hvilke scenarioer som er mer sannsynlig enn andre (sannsynlig basert på den informasjonen vi har om trussel og sårbarhet), og hvilke konsekvenser det vil ha for organisasjonen dersom verdiene rammes slik det fremkommer av det spesifikke scenarioet.
- Man må bruke det verktøyet som passer best i enhver situasjon. Både VTS og ROS er anvendelige for hver sine former for risikovurderinger. Det er viktig å ikke underslå at sannsynlighet kommer med som en betraktning i begge metoder, men at det kan være gunstig å arbeide kvalitativt ved kompliserte og sammensatte risikosituasjoner. VTS lar seg anvende også der sannsynligheten er kjent eller omforent. ROS kan benyttes der sannsynligheten er ukjent. Metode er underordnet. Prosessen med valg av deltakelse, grundighet, bevisstgjøring er viktigere
- Kunnskap og samarbeide
- At man kan identifisere risikoer både når det gjelder HMS og tilsiktede hendelser og komme fremt til handlingspunkter og anbefalinger til et prosjekt basert på dette som er fornuftig og kostnadseffektivt.
- Kompetanse, innhenting av informasjon, mangfold og brainstormimg
- Grunnleggende kunnskap og gjeldende fagområde.
- Visshet om at resultatet blir tatt hensyn til i virksomhetens videre prioritering av tiltak
- Det viktigste suksesskriteriet for å gjennomføre en god risikoanalyse er ledelsesforankring, kompetanse hos dem som gjennomfører analysen og at de med eierskap til verdiene deltar i risikoanalyseprosessen. Den største fallgruven er imidlertid oppfølging av risikoanalysen. Hvis ikke ledelsen aktivt bruker risikoanalysen til å akseptere, fjerne, redusere eller overføre identifisert risiko, har analysen liten verdi.
- Forstå hvilket verktøy man skal bruke hvor. Det er mange selgere som står å prøver å selge sitt verktøy fordi det kan brukes til alt. Jeg har ikke et slikt verktøy i min verktøykasse.
- Forberedelser mtp avgrensning av analysen, forståelse av kontekst og bruk av spesialist kompetanse.
- At man er enig om hva som anses som en risiko og som kan være nødvendig for enheten å synliggjøre gjennom en analyse.
- Bred arbeidsgruppe Mandat forankret i ledelse
- Analytisk kompetanse i et tverrsektorielt miljø
- God planlegging Ledelsesforankring Kvalifiserte deltakere (både kjennskap til metodikk og virksomheten/analyseobjektet) Systematisk gjennomgang Kreativ brainstorming Gjennomgang av resultat og oppfølgingsplan med deltakere og ledelsen
- At de aktørene som skal bruke den, er fornøyd, og at den er brukbar og forståelig fir dem, gjennom bredt samarbeid med relevante aktører
- At den forstås av de som skal bruke den til å ta beslutninger.
- Sporbar, gjennomsiktig, gode valg av analyseområder,
- Brei deltagelse, ledelsesforankring, samt en god prosjektleder.
- Informasjon og samarbeid mellom ulike fagmiljøer
- Analyser tar tid, og krever innsats over tid fra ulike miljøer.
- Tilgang til fakta/informasjon.

- Fag- og lokalkunnskap og en god struktur.
- Metodeforståelse, god forståelse av /kjennskap til analyseobjektet, samt inkludering av verdieiere i prosessen.
- Enkel og logisk oppbygging, grafisk fremstilling.
- Gode inn-data, dvs kompetente analytikere
- Et godt situasjonsbilde. Mye bakgrunnstoff og kjennskap til sårbarheter i organisasjonen
- Medvirkning og eierskap fra operatører i den "skarpe enden"
- God modell og gode innsatsfaktorer.
- Kunnskap om begge
- Beskrive usikkerheten
- definere hva man faktisk ønsker å oppnå med analysen. Det er mye god erfaring å hente fra safety og security, men det er prinsipielle forskjellige domener som krever forskjellig fokus.
- Ledelsesforankring, en helhetlig og grundige prosess med bred deltakelse
- Kompetanse hos berørt personell.
- En tradisjonell ROS analyse tar ikke for seg usikkerhetsfaktoren, eller vekting av verdiene i virksomheten. Det blir litt slik at man i tillegg til sansynlighet og konsekvens må regne inn en vekting for å kunne se hvordan ulike risikobilder faktisk rammer virksomheten.
- Godt metode kunnskap, involvering av fagpersonell, kommunisere på et språk og med en modell ledelsen kan forstå.
- Erkjennelse av risiko og vilje til å avsette ressurser til nødvendige konsekvensreduserende tiltak
- Kunnskap, fenomen forståelse, deltakelse og involvering av rett personell
- Det viktigste er at organisasjonen kjenner sine verdier slik at sårbarheter kan tettes enklere
- Erfaring og kunnskap om området
- At alle nivåer i organisasjonen er med på forarbeidet (brainstorming o.l.)
- Kunnskap og håndtering av usikker
- Alle parter i en organisasjon må delta aktivt for å få en god analyse. Analysen blir uansett reaktiv, basert på tidligere hendelser. Jeg ser stort sett alltid at organisasjonen eller prosjektet ikke har definert detaljert nok ned i arbeidsoppgavene eller prosessenen når hendelser er et faktum. Det blir alltid som julekvelden på kejrringa:)
- God og variert erfaring fra arbeidsoppgaven og god nok teoretisk kompetanse til å bruke metoden riktig.
- Kommunikasjon til beslutningstakere. Alt for mange omfattende analyser blir gjennomført uten at de tar inn over seg at hensikten med analysen er beslutningsstøtte og svikter i siste ledd, kommunikasjon til beslutningstakeren.
- At alle relevante parter bidrar med kunnskap knyttet til det man skal risikovurdere - kunnskap er avgjørende for å kunne ta informerte valg.
- At man legger til grunn en definisjon på risiko som samsvarer med det man undersøker. Man må ha riktige akseptkriterier mot det man undersøker. Kan man ta beslutninger ut i fra dataene ? Gir det svar, dvs. Sjekke validiteten.
- Datagrunnlaget
- Forankring, involvering og transparent prosess.
- Det er flere enn disse to metodene som kan brukes. I arbeidet må en forstå sin kontekst og sine behov. Deretter må en velge metode som passer basert på dette. En må videre ha kunnskap om styrker og svakheter ved de ulike metodene slik at en tolker resultatene rett. Analyser er ikke eksakt vitenskap og mye av utfordringen er at analytikerne må forstå eget og andres kunnskapsgrunnlag og hvilken usikkerhet som ligger i dataen/informasjonen, og i egen anvendelse av dette.

- Enkelhet og gode beslutninger/forankringer
- God kjennskap til virksomheten/enheten/forholdet. Åpen for å tilrettelegge realistisk slik at analysen ikke blir utformet kun for dokumentets del.
- Involvering, kommunikasjon, forståelse, sikkerhetskultur. Felles risikoskalaer, da analysene gjerne må benyttes på svært ulike områder og tjenester (eks. Kommunale risikoanalyser som kan omfatte introduksjon av ny teknisk løsning i eksisterende infrastruktur til konsekvenser av overvann i sentrum, til død i helse- og omsorgssektor osv). Hvordan finner man en universal forståelse for konsekvens og sannsynlighet når det er ulike verdier og problemer som analyseres?
- Avdelingen må ha tilgang til god bakgrunnskunnskap/fakta (trusler, sannsynlighet, egne verdier, osv) og kjenne sin egen organisasjon godt for å kunne gjøre en god analyse hvis ikke blir det shit in/shit out - uavhengig av modell.
- Kunnskap og erfaring
- Det eksisterer metoder som slå sammen ROS og VTS. VTS kan benyttes for å drive ROS forståelse
- At analysen anbefaler balanserte sikringstiltak i forhold til verdien av det som skal sikres.
- Forstå kontekst og deretter velge hjelpeverktøy
- Erfaring, kompetanse og gjennomføringsevne. Begge modellene har sine styrker og svakheter, og jeg mener det må være opp til enhver organisasjon å vurdere hvilken som passer best for dem. Ingen modeller klarer fange opp alt, og det er personen som gjennomfører analysene som er avgjørende for om analysen er tilstrekkelig.
- 1. Fagpersoner med kunnskap om metode og prosess. Dvs. kan metoden som brukes på et tilstrekkelig høyt nivå og kan gjennomføre prosjektet på en god måte. 2. Tilgang til tilstrekkelig og korrekt informasjon.
- Faglig bredde i tilnærming og evne til kreativ tenkning sammen med analysekraft.
- Det viktigste suksesskriteriet for å gjennomføre en god risikovurdering er å først definere hva formålet med vurderingen skal være, og deretter bruke den metodikken som passer best til analyseobjektet og formålet (og som passer best med organisasjonens eksisterende kompetanse). Det foreligger et utall forskjellige metodikker, som hver har sine sterke og svake sider.
- At det er kompetente mennesker som gjennomfører analysen, som kan vurdere reelle farer og konsekvenser.
- At risikoanalysen tilpasses de beslutningene risikoanalysen skal understøtte, og at det gjennomføres en god prosess der kunnskap om potensielle fremtidige uønskede hendelser (tilsiktede eller utilsiktede) analyseres med tilhørende konsekvenser og usikkerheter.
- Uavhengig av metode, må analysene forankres i ledelsen. ROS-analyse er fullstendig uegnet mht. tilsiktede uønskede hendelser.
- En god forankring i ledelsen. Åpenhetskultur for egne mangler og svakheter.
- At virksomheten har identifisert og fastsatt verdier som skal beskyttes. At virksomheten har fastsatt sikringsmål som skal oppnås At truslene er identifisert At risikobildet er identifisert At sikringstiltak er anbefalt ift å kunne oppnå sikringsmålene
- God kunnskap om verdiene, kjennskap til eventuelle trusler/ trusselaktører og god metodeforståelse. Være i stand til å gjennomføre analysen metodisk riktig.
- Å sikre bred deltagelse og forankring
- Teoretisk kunnskap og praktisk erfaring slik at man kan være fleksibel i metodevalget. De fleste virksomheter står overfor både utilsiktede og tilsiktede uønskede hendelser, og derfor har både ROS og VTS en plass i sikkerhetsarbeidet. Suksesskriteriet er at man må beherske begge metodene, og man ha kompetanse for å vite når man skal bruke den ene eller den andre.
- Kompetanse om trusselen og evne til objektiv tenking.
- Kunnskap om svakhetene og styrkene i de forskjellige modellene. Kildekritikk og vekting av usikkerhetsmomentet
- Det er viktig at risikoanalyse bygger på reelle hendelser som har skjedd, ikke hver enkelts frykt for at noe skal skje.
- Kunnskap
- god nok forankring i fagmiljøer som er nødvendig i vurderingen av det spesifikke sektorområdet.
- Mandat forankret i toppledelsen. Bare verdivurderingen kan ta opp til ett år i en mellomstor bedrift.

- Tilstrekkelig deltagelse fra personell som kan identifisere og spesifisere ulike trusler.
- At man ikke går for den ene eller andre modellen konsekvent, men at man bruker dem der de fungerer best - ROS på aktiviteter, VTS på sårbarheter og "feilretting"
- Kunnskap og systematikk
- God kjennskap til emnet. Gode kilder å basere vurderingene på., hvis ikke blir det mye «synsing». Fokus på Usikkerhet i tillegg til Sannsynlighet og Konsekvens - Evnen til å erkjenne det vi ikke vet.
- Enhver risikoanalyse, enten ROS eller VTS, er avhengig av ledelsesinvolvering som både vet hva som skal analyseres (og hvorfor), klare ledelsesbeslutninger angående risikoaksept og sikringsmål, og at analytikeren (-e) innehar kompetanse innen vurderingskriteriene, enten det omhandler verdi, trussel og sårbarhet, eller farer og konsekvensen av hendelsene.
- Felles forståelse av verktøy og kriterier, mange vurderer risiko etter at tiltak - uten dermed å ta inn over seg årsak til eksisterende tiltak etc
- Kunnskap
- Prosessen med involvering av ulik kompetanse for i så stor grad som mulig få kartlagt og "verifisert" dataene i analysen er viktig. Suksesskriteriet er å få presentert resultatet av analysen på en måte som gir beslutningstakere et godt grunnlag for sine beslutninger.
- Forståelse av hva du ønsker å oppnå med analysen - det legger premissene for metodevalg, sammensetning, valg av strategi og tiltak
- Bevisst om målet med analysen. Gjør valg av metode ut fra det.
- Kunnskap om området og metode
- Tydelig mål med analysen, godt informasjonsgrunnlag, intervjuobjekter med god kunnskap om analyseobjektet, definerte sikkerhetsmål, kunnskap om trusler og sårbarheter, erfaring med analyser, mm
- Eierskap
- Kompetanse
- Deltagere som forstår formålet
- Vite hva slags risiko som evalueres spørreskjemaet inneholder en vesentlig og gjennomgående feil.....! Security handler om utilsiktede handlinger, som krever VTS-metodikk Safety handler om utilsiktede hendelser, og ROS-metodikk kan benyttes,
- Bidragsyterne til analysen må ha god kunnskap om aktivitet/virksomhet som skal analyseres. Ledelsen av analysen må sørge for at det er "stor takhøyde" for alle mulige innspill som kan ha betydning.
- Verdivurdering og avdelking av reelle trusler
- Å gjøre en god verdivurdering, samt å bruke VTS når det er snakk om tilsiktede hendelser.
- Gode data og god evne til kvalitativ nøytral vurdering.

Til slutt noen demografiske spørsmål om din bakgrunn.

27. Hva er din alder?

Svar	Antall	Prosent
18-33 år	23	**16,3 %**
34-52 år	84	**59,6 %**
53-78 år	29	**20,6 %**

Svar	Antall	Prosent	

28. Hva slags yrkesbakgrunn har du? *

Dersom mer enn to alternativ passer velger du de med størst relevans for din forståelse av risiko- og sikkerhetsfaget.

Svar	Antall	Prosent	
Politi eller forsvar (bachleor / etatsutdanning)	57	**40,4 %**	
Vekter, toller, fengselsbetjent, brannkonstabel eller annen operativ bakgrunn	24	**17 %**	
Ingeniør / teknisk bakgrunn	17	**12,1 %**	
Akademisk / teoretisk bakgrunn	85	**60,3 %**	
Annen yrkesmessig bakgrunn	19	**13,5 %**	

29. Hva slags utdannelse eller kurs har du innenfor risiko, sikkerhet eller beredskap? *

Svar	Antall	Prosent	
Videregående skolenivå	6	**4,3 %**	
Bachelor / ingeniørnivå	43	**30,5 %**	
Mastergradsnivå	68	**48,2 %**	
Doktorgrad / phd	3	**2,1 %**	
Et eller flere fagkurs av kortere varighet	50	**35,5 %**	
Vil ikke svare	2	**1,4 %**	

30. Hvilken sektor eller bransje tilhører du? *

Dersom mer enn to alternativer passer velger du de med størst relevans for din forståelse av risiko- og sikkerhetsfaget.

Svar	Antall	Prosent	
Departement, Stortinget eller Høyesterett	7	**5 %**	
Direktorat eller statlig underliggende etat	63	**44,7 %**	

Svar	Antall	Prosent
Kommune eller fylkeskommune	25	17,7 %
Privat næringsliv	30	21,3 %
Konsulentbransjen eller utdanningsvirksomhet	25	17,7 %
Veldedige organisasjoner, interesseorganisasjoner eller internasjonale organisasjoner	6	4,3 %
Vil ikke svare	4	2,8 %

31. Hvor stor andel av din yrkeserfaring har vært relatert til risiko, sikkerhet eller beredskapsarbeid? *

Svar	Antall	Prosent
6 måneder eller mer	6	4,3 %
2 år eller mer	12	8,5 %
5 år eller mer	27	19,1 %
10 år eller mer	36	25,5 %
20 år eller mer	38	27 %
30 år eller mer	14	9,9 %
Studerer risiko, sikkerhet eller beredskap	13	9,2 %
Bidrar i arbeidsgrupper, vurderer risiko som del av min lederstilling	16	11,3 %
Risikoanalyse er ikke min profesjon akkurat, men jeg er godt kjent med tematikken gjennom arbeid i høyrisikoland	2	1,4 %
Vil ikke svare	4	2,8 %

32. Hva slags type stilling har du i dag? *

Svar	Antall	Prosent
Toppleder eller premissgiver med påvirkningskraft ovenfor egen eller andre organisasjoner	9	6,4 %
Lederstilling	33	23,4 %

Svar	Antall	Prosent
Konsulent, rådgiver, ingeniør, forsker	72	**51,1 %**
Operativ, utfører praktisk risiko, sikkerhets eller beredskapsarbeid (inkludert operativ ledelse/innsatsledelse)	41	**29,1 %**
Student eller utenfor arbeidslivet	5	**3,5 %**
Vil ikke svare	6	**4,3 %**

Avslutning

Dersom du har inngående kunnskaper om risikoanalyse og villig til å dele litt av din innsikt, gjerne send meg en mail på bkjelsaas@gmail.com. Hva du skriver direkte til meg kan ikke knyttes til din besvarelse på spørreskjema.

Som en del av forskningsarbeidet har jeg planlagt å intervjue et mindre antall personer med inngående kjennskap til ROS-analyse eller VTS-analyse på et senere tidspunkt. Dersom du anser deg selv for å være en potensiell intervjukandidat kan du sende en mail hvor du beskriver kort hvilken kompetanse du har og hva du kan bidra med. Ta i såfall med navn og tittel, erfaring og utdannelse.

Tusen takk for ditt bidrag!

Med vennlig hilsen

Bjørn

Vedlegg II

Intervju med Dr. Morten Bremer Mærli, seniorrådgiver v/ Stortingets administrasjon

Intervjuene bygger videre på spørreundersøkelsen "Modeller for risikoanalyse i Norge" som ble gjennomført 6-20. januar 2020 og sees i tett sammenheng med denne.

Det understrekes at synspunktene er Bremer Mærlis egne, og at de ikke har noen ting med Stortinget eller Stortingets administrasjon å gjøre.

1. Sikkerhetsdefinisjonen. *Hvordan vil du forklare forskjellen på safety og security, og har det egentlig noen betydning for oss?*

Safety og security er grunnleggende forskjellig, og denne forskjellen har stor betydning for oss når vi skal analysere risikoen eller sette inn sikkerhetstiltak. Ta en brann som eksempel: Den kan skje ved et uhell (safety) eller ved at den er påsatt (security).

Trygghet/safety definerer *utilsiktede,* uønskede hendelser, mens sikring/security definerer *tilsiktede,* uønskede handlinger.

Sagt enda mer «populært»: Safety handler om *tingenes* iboende faenskap. Security om *menneskenes* iboende faenskap.

Intensjonelle og ikke-intensjonelle hendelser representerer svært forskjellige situasjoner, med ulik dynamikk. Dette fordrer dedikert metodikk, tilpasset de ulike risikosituasjoner. Likevel er det tendenser til en one-size-fits-all-tenkning, hvor hendelsens årsak ignoreres, og det ikke skilles på konsekvensene av høyst ulike scenarier. Med brannscenariet som eksempel; En påsatt (villet) brann kan gi gjerningsmannen et spekter av muligheter til å påvirke utfallet (konsekvensene) på en måte som ikke gjelder rene ulykkesbranner. Tenk bare hvordan hvordan rømningsdører kan blokkeres, responsen kan hindres eller avledes og tidspunkt for ugjerningen velges for å optimalisere ønsket effekt. Intensjon farger med andre ord konsekvenser, og det på måter som gjør intensjonelle handlingers analysemetodikk unik – og veldig annerledes enn (frekvensbasert) metodikk for ulykkesrisiko.

Eksempelet viser at konsekvensene kan bli vesentlig verre dersom dette er gjort med vilje og tiltakene som settes inn kan være vesensforskjellige fra de som velges for å motstå brannuhell.

Forekomsten av henholdsvis villede branner og uhellsbranner er vanligvis forskjellig. I sum, gir dette svært forskjellige risikoestimat for uhell vs villede handlinger.

2. *Kan safety/security diskusjonen ha innvirkning på analytikere og organisasjoners valg av modell (ROS eller VTS) når vi skal gjennomføre risikoanalyser? Forklar i så fall hvordan.*

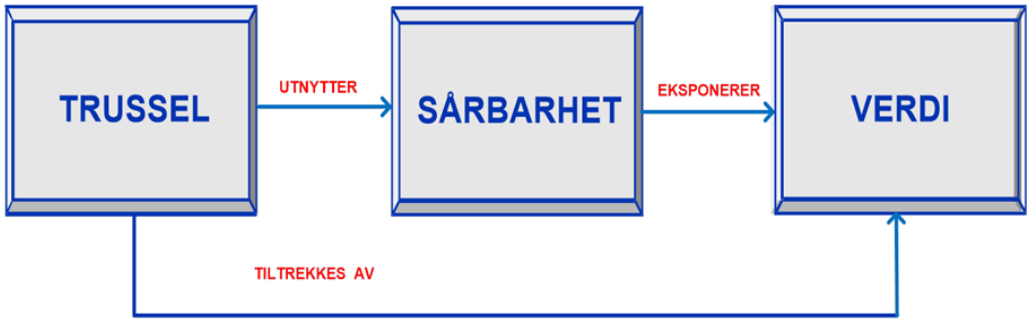
Metodeutfordringene kan oppsummeres med manglende hensyntaking til risikoanalysenes egenart og målsetninger, så vel som forståelse av distinkte aspekter ved de ulike analyseparametere og samspillet mellom disse.
Ut fra forskjellen på safety-hendelser og security-handlinger så bør valget av analysemodell gjøres på grunnlag av om det er safety-risiko eller security-risiko som skal analyseres. Den følgende oversikten illustrerer forskjellene:

	Security risk	**Safety risk**
Trigger	Vinning eller skade	Brudd eller feil
Karakteristikk	Gjort med vilje	Skjer ved uhell
Indikator	Menneske	Menneske eller naturen
Skademaksiminering	Muligens	Nei
Diskriminerende	Muligens	Nei

Oversikten viser distinkte forskjeller på safety risiko og security risiko.

Dersom man tenker at konsekvensen blir det samme eller at tilnærming ikke spiller noen rolle, blir det helt feil! Det er veldig skummelt å kline det sammen til én analyse. Nettopp fordi villede handlinger gir mulighet til å «skreddersy» aksjoner, kan skademaksimering, herunder diskriminerende aksjoner, velges. Konsekvensene kan manipuleres fordi trusselaktøren kan velge tid, sted, eventuelle blokkeringer og så videre. Tenkningen omkring scenarier, analysemodell og mottiltak er dermed vesensforskjellig

Ved safety hendelser utrykkes risiko tradisjonelt som en kombinasjon av sannsynlighet og konsekvens (R = P x C), det vil si ROS-modellen. Utfordringene viser dermed behovet for en egen analysemetodikk for villede, ondsinnede handlinger, slik som VTS-modellen representerer. Figuren under illustrerer en NS 5832 kompatibel praktisk metodikk som søker å belyse, og dermed unngå mulige fallgruver i sikringsrisikovurderinger for beskyttelse mot tilsiktede, uønskede handlinger.



Figur 1. Risiko som en trussel som tiltrekkes av en verdi og som utnytter en sårbarhet for å eksponere verdien. (Gjengitt med tillatelse fra Morten Bremer Mærli).

Analytikere og organisasjoner som har tilstrekkelig kunnskap om forskjellen mellom safety hendelser og security handlinger vil ut fra dagens modellalternativer velge VTS for risiko som skyldes tilsiktede uønskede handlinger.

Sannsynlighet kan ifølge Sikringshåndboka (2017) forstås enten som:
a: En kunnskapsbasert kvalitativ og subjektiv vurdering av hyppigheten for at en hendelse inntreffer.
b: Generelt kan sannsynlighet vurderes ved hjelp av statistiske metoder om relevant statistikk er tilgjengelig, eller som en ikke-statistisk kunnskapsbasert vurdering dersom det ikke finnes egnet statistisk grunnlag. Kombinasjonen av statistisk og ikke-statistisk tilnærming kan også benyttes.

Noen kritikere av ROS-modellen er av den oppfatning at sannsynlighetsbegrepet er uheldig for analyse av scenario med lav hyppighet fordi folk i miljøene tolker sannsynlighet til å være synonymt med *frekvensbasert* sannsynlighet. Om en går tilbake til språkdiskusjonen ser vi også at sannsynlighet enten kan oppfattes som "*probability*" (matematisk sannsynlighet) eller "*likelihood*" (mulighet, trolighet og sjansen for), fra engelsk språk.

3. Sannsynlighetsbegrepet har som vi ser vært en sentral komponent i diskusjonen om ROS og VTS. Sannsynlighet er en essensiell del av ROS-analysen, samtidig som den tilsynelatende er fraværende i VTS-analysen. *Kan du dele noen tanker omkring bruken av sannsynlighetsbegrepet i forbindelse med risikoanalyser, og hvor tror du veien går videre?*

Kunnskapsbasert sannsynlighet er det største selvbedrag siden Titanic! Men sannsynlighet er ikke fraværende i VTS-modellen. Hovedproblemet er at «kunnskapsbasert sannsynlighet» aggregerer to ulike sannsynligheter, som attpåtil «eies» av to forskjellige aktører:

P(A) = sannsynlighet for angrep, eies av trusselaktører
P(B) = sannsynlighet for barrierebrudd, eies av operatør (verdieier)

Jeg vil forklare svakheten med kunnskapsbasert sannsynlighet ut fra figuren under:

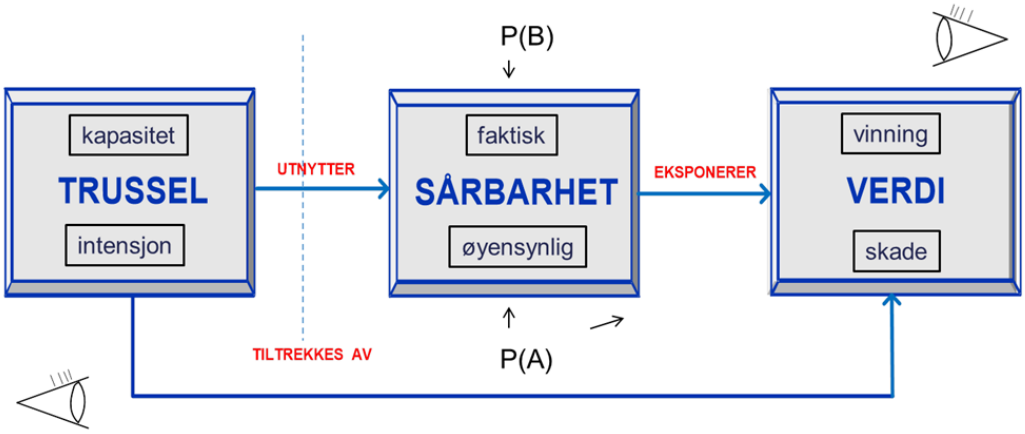


Fig. 2. Endelig modell, med henholdsvis angripers og operatørs perspektiver angitt, samt sannsynligheten for angrep, P(A), og sannsynligheten for barrierebrudd, P(B), gitt et angrep. (Gjengitt med tillatelse fra Morten Bremer Mærli).

P(A), angrepssannsynligheten baserer seg på trusselaktørens kost/nyttevurdering av målet, kombinert med en vurdering av egenkapasitet versus antatt styrke på målet som tenkes angrepet. Det er intensjoner som styrer gjerningsmenns målutvelgelse og taktikk. Det innebærer samtidig at mulige konsekvenser bestemmes av intensjoner. Trusselintensjonen kan holdes opp mot potensialet som ligger i å eksponere verdien (enten som vinning eller påført skade). Sammen med trusselkapasiteten, vil dette definere angrepssannsynligheten, eller

attraktiviteten. Trusselaktøren eier denne sannsynligheten. Det er gjerningsmennene som bestemmer hva som skal angripes, når og hvordan.

Dersom trusselaktøren ikke finner at verdipotensialet er tilstrekkelig, eller at egne kapasiteter er utilstrekkelig til å overvinne sikringen ved anlegget (kost/nyttevurdering) vil han finne et annet mål eller en annen angrepsmetode. Merk også at P(A) dermed er et produkt av den øyensynlige sårbarheten ved anlegget, basert på angriperens subjektive oppfatning. Dette viser viktigheten av «Security apperance», for avskrekking. Dersom angriperne har innsideassistanse, vil den øyensynlige sårbarheten kunne gå mot den faktiske (som det kun er/skal være operatøren som har kunnskap om).

P(A) = 1 eller 0. Enten blir anlegget angrepet, eller så blir det ikke angrepet. Dersom gjerningsmenn finner verdipotensialet høyt nok og/eller antar høy nok sårbarhet hos verdien, gjennomføres angrepet (P(A)=1).

P(B) er sannsynligheten for barrierebrudd ut fra verdieiers bruk og investering i sikkerhetstiltak. Sannsynligheten beskriver muligheten for at en gitt trusselaktør lykkes med å oppnå en gitt konsekvens (barrierebrudd), snarere enn sannsynligheten for at hendelsen (angrepet) finner sted (se tabell). Bruker man ressurser på å styrke barrierene så synker også P(A), fordi øyensynlig sårbarhet blir også mindre ved et høyere sikkerhetsutrykk.

	Lav	Middels	Høy
Sannsynlighet for barriererbrudd (suksess)	Det anses som lite sannsynlig at beskrevet trussel er i stand til å lykkes, gitt eksisterende barrierer og sårbarheter	Det anses som sannsynlig at beskrevet trussel er i stand til å lykkes, gitt eksisterende barrierer og sårbarheter	Det anses som svært sannsynlig at beskrevet trussel er i stand til å lykkes, gitt eksisterende barrierer og sårbarheter

Dette innebærer i praksis at vi har to sannsynligheter. Den ene er sannsynligheten for barrierebrudd, og denne sårbarheten er direkte avhengig av de barrierer og den soliditet som verdien representerer (resiliens eller sikringsnivå som motvirker sårbarheten). Den andre er sannsynligheten for angrep.

BEGGE MÅ VÆRE OPPFYLLT!

Kunnskapsbasert sannsynlighet vil utgjøre en kombinasjon av disse to sannsynlighetene, den ene, P(A), som vi i realiteten ikke kan si noe kvalifisert om, så fremt vi ikke vet om trusselaktørens intensjon, plan og tilnærming der og da. Sannsynligheten eies av ulike og vidt forskjellige aktører og når man smører sammen de to til en sannsynlighet blir det umulig å fastslå den sikkert.

Sikringsrisikoanalyser skiller videre sjelden mellom trusselaktørenes og objekteierenes perspektiver, selv om disse perspektivene kan være svært ulike. Forståelsen av attraktiviteten til mulige angrepsmål, kan bli tilsvarende dårlig, med de implikasjonene dette har for risikoforståelse og behov for sikringstiltak. Mens en tankbil eksempelvis kan utgjøre en marginal verdi for større oljeselskap, kan samme tankbil på veien i urbane områder være et fristende og attraktivt mål for gjerningsmenn med ønske om å påføre skade. Valg av perspektiv styrer altså ikke bare om og hvordan, men også hvorfor, visse mål eventuelt velges – mål som derfor bør sikres.

4. Jeg startet studien med en antagelse om at *safety*-orienterte aktører (f.eks DSB og kommunesektoren) velger ROS, og *security*-orienterte aktører (f.eks NSM, Politi og "statssikkerhetssektoren") velger VTS. *I hvilken grad mener du dette er en korrekt antagelse? Dersom du mener antagelsen bare er delvis korrekt, hvordan kan det fremstilles bedre?*

Ja, det tror jeg er en korrekt antagelse. Kanskje skyldes dette at «statssikkerhetssektoren» i større grad vokter (distinkte) enkeltinstitusjoner, mens kommunesektoren er «bredere».

5. Strukturelle forklaringer: H_1 hypotesen bygger videre på strukturelle eller andre ytre rammefaktorer. Eksempler kan være sektorkrav, bransjestandarder, lover/forskrifter eller tvungen isomorfi (pålagt standardisering).
   I hvilken grad mener du at slike strukturelle forklaringer bidrar til å forklare valget av analysemodell? Gjelder dette i så fall valg av begge modellene eller er det forskjeller?

Alvorlige problemer ift kunnskap. Etatstyrere/premissgivere har ikke alltid kunnskap nok om fenomenet. Derfor blir underliggende organer styrt på metodevalg som kan være basert på feil premisser. Sedvane, instituert tenkning, osv hos etatstyrer som smitter nedover.

6. Indre forklaringer (H_2): *I hvilken grad tror du det medfører riktighet at valg av analysemodell (ROS/VTS) skyldes subjektive forhold hos aktørene, slik som utdanning- og yrkesbakgrunn, kunnskaper, holdninger eller egeninteresser? Mener du at denne forklaringen er dekkende for valg av begge modeller?*

Analytikere og organisasjoner som har tilstrekkelig kunnskap om forskjellen mellom safety hendelser og security handlinger vil ut fra dagens etablerte standarder velge ROS for analyse av safety, og VTS for analyse av security om de kunne velge.

Det er klart at hvis en konsultativ organisasjon har basert det meste av sin portefølje på én type metodikk, kan det være tungt å endre tilnærming. Og så lenge kunden ikke kjenner til trefaktormodellen, består den «gode gamle» måten å gjøre tingene på,

7. Organisasjonsteoretiske forklaringer (H3). Valg av analysemodell kan skyldes;
   - «*Tykk» institusjonalisme,* sånn har vi alltid gjort det her, ingen grunn til å endre.
   - *Stiavhengighet,* Vi har brukt så mye ressurser på dette valget at det er for sent å går tilbake for å velge en annen løsning.
   - *Mimetisk isomorfisme,* Vi bør følge etter/ «etterape» andre sammenlignbare organisasjoner som har valgt en annen (ny) løsning.
   - *Normativ isomorfisme,* vil bør velge den analysemodellen som er mest riktig å bruke, ut fra eksisterende kunnskap.
   - Andre organisasjonsteoretiske forklaringer.
   Beskriv med egne ord hvilke faktorer du mener forklarer organisasjoners eventuelle valg ROS/VTS-analyse? Hva slags organisasjoner gjør hvilke valgbasert på overstående eksempler?

Institusjonalisme og stiavhengighet gir stor forklaringskraft for mange organisasjoners valg (aktivt eller passivt) av analysemodell. For eksempel om en organisasjon har basert det meste av sin portefølje på én type metodikk kan det være tungt å endre tilnærming.

Normativ isomorfisme forklarer at man gjør det beste basert på eksisterende kunnskap.

Som nevnt under spørsmål 4, "statssikkerhetssektoren" vokter i større grad (distinkte) enkeltinstitusjoner, mens kommunesektoren har et bredere fokus som dekker hele samfunnet. Dermed institueres statssikkerhet og kommunesektoren på hver sin måte slik at forskjellene mellom disse blir framtredende. Det som er normativt best for den ene sektoren er ikke nødvendigvis best for den andre.

8. *Hva tror du er årsaken til at sikkerhets- og beredskapsmiljøene ikke har klart å samle seg om en omforent modell for risikovurderinger?*

Fordi det ikke er sikkert at det er det beste. Det er for stor forskjell på safetyrisiko og securityrisko. Videre at det er ulike institusjoner / premissgivere for ulike sektorer.

9. *Burde vi samles om en felles analysemodell som favner alle sikkerhetsaspekter? I så fall hvordan kan dette oppnås? Eller er det bedre å rendyrke ulike verktøy/metoder til forskjellig bruk?*

NS 5814:2008 skal revideres i løpet av 2020. Altså den «gamle» ROS-standarden. Svar på spørsmålet blir dermed at det kommer an på hvor god den nye fellesmodellen blir. Dersom den ikke blir distinktiv nok for begge risikotypene vil det være bedre å rendyrke hver enkelt modell.

10. *Er det etter ditt syn andre faktorer som forklarer valg av analysemodell som jeg ikke har tenkt på?*

Oppfølgingsspørsmål: *Tilbake til den ekspertuttalelsen som du og DNV gav til 22. juli kommisjonen; Er det noen referanser fra denne uttalelsen som det eksplisitt eller implisitt vises til i Gjørvrapporten, eller videre noen "rød tråd" som forbinder ekspertuttalen med Gjørvrapporten i 2012, Standard Norge komite 296 og Norsk standard 583x serien for sikringsrisikoanalyse som lå klar i 2014?*

Svar: *Nei. SN/K 296 gjorde etter mitt syn et selvstendig arbeide.*

Avslutningsvis:
Helt kort, hvilken befatning du selv har hatt med henholdsvis ROS og VTS modellene, hva er din utdannelse /erfaring innenfor fagområdet?

Utdanningsbakgrunn innen kjernefysikk med påfølgende doktorgrad. Yrkesbakgrunn blant annet fra Statens Strålevern og mange år som seniorforsker på Norsk utenrikspolitisk institutt. Betraktes som en ekspert på internasjonal sikkerhetspolitikk med spesielt fokus på atomsikkerhet, ikke-spredning og risiko for radioaktiv/nukleær terrorisme. Senere kompetansestillinger ved Det Norske Veritas og Stortingets administrasjon.

Sted/dato: ***Oslo, 22.1.2020***

Respondent/intervjukandidat

Bjørn Melandsø Kjelsaas
Masterstudent

Vedlegg III

Intervju med Tore Drtina, sikkerhetsleder i DSB

Intervjuene bygger videre på spørreundersøkelsen "Modeller for risikoanalyse i Norge" som ble gjennomført 6-20. januar 2020 og sees i tett sammenheng med denne.

1. Sikkerhetsdefinisjonen. *Hvordan vil du forklare forskjellen på safety og security, og har det egentlig noen betydning for oss?*

Den enkle hovedforskjellen på safety og security er i forhold til villede og ikke-villede handlinger. Det er på en måte det superenkle skillet, mellom villede og ikke-villede handlinger. De har veldig mange forskjellige ting ved seg, men safety og securityperspektivene har også veldig mange likhetstrekk ved seg, og det er kanskje flere likhetstrekk enn det er forskjeller. Og verdien vi skal sikre kan veldig godt være den samme. Det som er kanskje er den store forskjellen er trusselaktøren, slik jeg ser det. Når det gjelder trusselaktører til safetyhendelser så er disse forutsigbare. Bortsett fra det man kaller "acts of god", sorte svaner og sånt noe. Men vær, ras, skred, flom, regnvær, tørke, og alle disse tingene er forutsigbare.

Når det det gjelder villede handlinger så er det en trusselaktør med en intensjon, kapasitet og en historikk, som du ikke kjenner til, som du ikke kan forutsi og vi er inne i det uventede rommet. Veldig mange av disse trusselaktørene slår til når du minst når du minst venter det, eller du kan ikke forutsi at det kommer noe. Og en av de store forskjellene er på trusselsiden. Vi vet endel om trusselaktørene, men vi vet ikke når han vil slå til. Fordi trusselaktørene er blant annet i sikringshåndboken definert som klasse A, B, C og D, hvor klasse D er fremmede makters spesialstyrker, klasse C er organiserte kriminelle og så er det et par andre klasser under der igjen. Så securityperspektivet, der kjenner vi til trusselaktøren, men vet ikke når/om det kommer.

Det er hovedsakelig forskjellen. Verdien er det samme, sårbarheten er det samme, men sårbarheter kan være forskjellige. En ting som er sårbart for en safetyhendelse trenger ikke være det for en securityhendelse. Og vice verca. Men beredskap og forebygging mot safetyhendelser hjelper også mot securitytrusler.

Spørsmålet ditt er veldig godt, jeg studerte denne tematikken på universitetet for halvannet år siden, og akademia er veldig opptatt av at det er en distinkt forskjell mellom safety og security. Mitt inntrykk er det. Jeg er ikke enig, fordi det er ikke så stor forskjell. Det er de samme verdiene vi skal beskytte. Og vi har endel andre parametere i metodikk som er forskjellig. De mener jeg kommer ganske langt ned på lista, som vi vil diskutere flere steder i dette intervjuet. Det er i alle fall hovedforskjellen. Trusselaktørene er forskjellige, enten det er sannsynlighet og konsekvens, eller om det er verdi, trussel og sårbarhet. Konsekvens og sårbarhet er to sider av samme sak, sett veldig grovt overordnet. Sannsynlighet har noe med trusselkomponenten å gjøre, når det gjelder det å vurdere en trusselaktør er det også en historikk komponent i det og det har med sannsynligheten å gjøre. Det er det jeg har av svar på første spørsmål.

Oppfølgingsspørsmål/replikk: *Jeg er enig med deg i at akademia (verbalt) er opptatt av distinksjonen mellom safety og security, men litteraturen på samfunnssikkerhet og beredskap er ikke nødvendigvis det. (Viser bilde av 4 bøker).* Antonsen, Stian, Heldal, Frode, Kvalheim, Sverre A. *Sikkerhet og ledelse*, Lunde, Ivar Konrad, *Praktisk krise- og beredskapsledelse,* Gangdal, Jon, Angeltveit, Gunnar*, Krise,* Beck Ulrich*, Risk Society. Disse bøkene står i sterk kontrast til mer security-spesifikk litteratur som tydeliggjør skillet mellom safety og security, slik som Sikringshåndboka fra Forsvarsbygg som du nevnte, eller Roy Stranden boka "Sikring" som kom ut i fjor. Vi som jobber i fagmiljøene prater veldig distinkt om forskjellen, men det studentene læres opp til, er ikke alltid like distinkt før de er godt inne i faget, eller i alle fall på masternivå.*

Svar: Jeg tror du har rett i det, til en viss utstrekning. Jeg tror dette kommer an på hva slags teorigrunnlag de forskjellige akademiske miljøene legger til grunn for sine studier også. Studiet i Stavanger skiller på det, kanskje litt tydeligere enn det andre utdanninger gjør.

2. *Kan safety/security diskusjonen ha innvirkning på analytikere og organisasjoners valg av modell (ROS eller VTS) når vi skal gjennomføre risikoanalyser? Forklar i så fall hvordan.*

Jeg tror at denne diskusjonen om safety og security har hatt innvirkning på hvordan vi som analytikere har valgt modell. Men hovedårsakene til valg av metode tror jeg ikke er hvorvidt er det safety eller security. Jeg tror det er andre årsaker som er mer toneangivende når det gjelder hovedårsak til valg av analysemodell. Fordi safetymodellen kan fint brukes på en securityhendelse, ikke noe problem! Og du kommer ut av det med veldig god risikokunnskap og en sårbarhetskunnskap som er godt inne på skiva. Så nei, safety eller security diskusjonen har ikke hatt stor betydning. Det er andre ting som har hatt det. Og det kommer vi sikkert tilbake til senere.

Sannsynlighet kan ifølge Sikringshåndboka (2017) forstås enten som:
a: En kunnskapsbasert kvalitativ og subjektiv vurdering av hyppigheten for at en hendelse inntreffer.
b: Generelt kan sannsynlighet vurderes ved hjelp av statistiske metoder om relevant statistikk er tilgjengelig, eller som en ikke-statistisk kunnskapsbasert vurdering dersom det ikke finnes egnet statistisk grunnlag. Kombinasjonen av statistisk og ikke-statistisk tilnærming kan også benyttes.
Noen kritikere av ROS-modellen er av den oppfatning at sannsynlighetsbegrepet er uheldig for analyse av scenario med lav hyppighet fordi folk i miljøene tolker sannsynlighet til å være synonymt med *frekvensbasert* sannsynlighet. Om en går tilbake til språkdiskusjonen ser vi også at sannsynlighet enten kan oppfattes som "*probability*" (matematisk sannsynlighet) eller "*likelihood*" (mulighet, trolighet og sjansen for), fra engelsk språk.

3. Sannsynlighetsbegrepet har som vi ser vært en sentral komponent i diskusjonen om ROS og VTS. Sannsynlighet er en essensiell del av ROS-analysen, samtidig som den tilsynelatende er fraværende i VTS-analysen. *Kan du dele noen tanker omkring bruken av sannsynlighetsbegrepet i forbindelse med risikoanalyser, og hvor tror du veien går videre?*

Når det gjelder sannsynlighetsbegrepet, noen ser det som en sentral komponent og i ROS-analysen så er det det. Og det er en diskusjon med et motsatt fortegn i VTS-analysen hvor sannsynlighet ikke er fremtredende. Den er ikke tydeliggjort som egen faktor og komponent. Jeg er helt på linje med FFI sin rapport (2015/00923) om sannsynlighetsbruk i sikringsrisikoanalyser. Og FFI toner jo problemet ned. Lag ikke et problem av noe som ikke er verdt å lage et problem utav. For det er mange der ute som skal lage analysene, som vil slite.

Når det gjelder sannsynlighet så ble jo VTS-analysen lansert som modell uten eksplisitt sannsynlighetsfaktor eller komponent i seg. Og det var nok noen som så litt rart på det til å begynne med, spesielt akademia synes det var veldig rart. På en annen side så går man da litt i dybden på hva er sannsynlighet, hva sier dette deg? Er det en repetisjonsfrekvens? Hva er faren for at det skal gjenta seg, hvor ofte? Og så videre. Det er egentlig en konsekvens eller sårbarhetsparameter i det. Fordi konsekvensen av en to-faktormodell hvor sannsynligheten er høy og repetisjonsfrekvensen er stor så blir konsekvensen stor. Fordi det skjer ofte kan konsekvensene bli store. Det kan jo dras dit hen at sannsynlighetsbegrepet ikke har så forferdelig mye å si, spesielt i VTS-analysen. I ROS-analysen så er den litt vanskelig å prediktere, den er vanskelig og sette og du må ha stor kjennskap til historiske data. Det er det den baserer seg på.

Det finnes jo modeller for dette, i tekniske systemer er det enklere å modellere sannsynlighet enn det er i samfunnsmodeller. Og også som Ortwin Renn skrev i sin bok om Risk Governance (som jeg forresten anbefaler veldig). Boka sier mye om dette. Det er en veldig interessant bok som sier mye om hvordan vi skal håndtere denne risikoen, enten det er safety eller security på samfunnsnivå.

Sannsynlighetsbegrepet og den veien det kommer til å ta, jeg tror veien videre blir at vi slår sammen disse to modellene. Og som research foran dette møtet snakket jeg med en dame som sitter i en gruppe som skal se på akkurat det. Vi har i sikkerhetsorganisasjonen i DSB jobbet mye med sikringsrisikometodikk. Og ikke minst verktøy for gjennomføring av risikoanalyser. Hvor de som har et krav til seg å beskytte en verdi skal gjennomføre risikoanalyse ned i organisasjonen, ned i de 20 sivilforsvarsdistriktene og ned til et antall eiere av skjermingsverdige objekter og infrastrukturer i DSB. Det er noen som eier disse verdiene, de skal gjennomføre en risikoanalyse, de må ha et verktøy og de må ha en enkel risikoanalyse som er god nok.

Risikomodellering kommer aldri til å bli noe eksakt vitenskap innenfor dette samfunnsperspektivet. Hvis vi dreier mot samlebåndsproduksjon av komponenter og systemer og så videre, så er vi innom en mer eksakt vitenskap, for der tester og sjekker en ut på et utvalg av komponenter med et kvalitetssystem i andre enden. Men når vi driver med risikoanalyse i et samfunnsperspektiv, målingene av hvorvidt risikoanalysene er gode er når analysene treffer hendelsen, eller beredskapsplanen treffer hendelsen, eller hendelsen treffer beredskapsplanen og dette ikke funker. Da var dette for dårlig. Backloopen på det her er vanskelig i samfunnsperspektivet.

Jeg synes sannsynlighetsbegrepet er overdrevet, overfokusert og jeg tror det forsvinner litt når vi slår sammen to- og tre-fakormodellene.

4. Jeg startet studien med en antagelse om at *safety*-orienterte aktører (f.eks DSB og kommunesektoren) velger ROS, og *security*-orienterte aktører (f.eks NSM, Politi og "statssikkerhetssektoren") velger VTS. *I hvilken grad mener du dette er en korrekt antagelse? Dersom du mener antagelsen bare er delvis korrekt, hvordan kan det fremstilles bedre?*

Så er det en påstand du har i spørsmål 4...
(Litt diskusjon og humring mellom intervjuer og respondent i det intervjuer forklarer utgangspunktet for denne påstanden i lys av en hypotese knyttet til problemstillingen).

Jeg tror ikke det er en provoserende påstand. Litt om historikk, DSB og fylkesmennene har ved hjelp av og via kommunene gjennom et laaangt prosjekt, det begynte i 94 så starta vi med risikoanalyser i kommunene. Og DSB sin veileder over risikoanalyser i kommunene osa det to-faktor av. Risiko = sannsynlighet x konsekvens, uansett hvordan du snur og vender opp og ned på det. Det var en gudegave til kommunene, fordi det var enkelt. Og vi lagde gode metodikker på det her med både veiledere, verktøy og slikt. Danskene hadde til og med sin modell som het "Sixty minutes". Hvor de lagde en risikoanalyse for en kommune på en time. Et fantastisk system. Veldig bra med malverk og en veldig diskursbasert tilnærming hvor du satte sammen et rådmannskollegium. I løpet av en time så har du lagd ROS-analysen. Første versjon, kjempebra! Vi fikk i hvert fall identifisert de områdene hvor det var god grunn til å ikke sove godt om natta.

(Litt diskusjon omkring spørsmålet i lys av hvordan det egentlig er i norske kommuner).

Noe av svaret på spørsmål 4 er hva blir disse målt på. Norske kommuner blir målt på ROS-modell fordi det er det som ligger til grunn i Lov om kommunal beredskapsplikt. Punktum! (Compliance). Selv om norske kommuner bryter loven hver dag, så har de innsett det, etter langvarig trykk fra DSB og fylkesmennene, og via storbykommunene ned til bydelene om bruk av ROS. Det er enkelt, det fungerer og de får tid, til og med. DSB brukte flere millioner kroner på å "sukre" denne pillen i kommunene, med gratis kompetansepåfyll, de fikk verktøy, vi kjøpte CIM til kommunene, alle norske kommuner (jeg lagde kontrakten på CIM), og der fikk de ROS-verktøy. Et kvantesprang for at kommunene skal kunne legge inn enkel ROS metodikk i kommunene. Jeg tror ca 80 prosent bruker den (ROS-modulen i CIM), og det er veldig mange.

Når det gjelder de securityorienterte aktørene og innenfor statssikkerhetssektoren, vi velger sikringsrisikomodell, altså tre-faktormodell hovedsakelig fordi det kom en ny veileder. Og vi ville prøve den nye veilederen, hva ga den for noe mere. Det er ikke et konstitusjonelt krav, det er det ikke. Det kom fra Politidirektoratet, PST, Forsvarsbygg ved Nasjonalt kompetansesenter for sikring av bygg som sa at tre-faktormodellen, den er fin. Og så ble den understøttet av et overivrig akademia enkelte steder, som flagga den veldig høyt. Jeg tror i mange henseende har dette vært en tabbe. Det har vært en tabbe og fokusere på securitymodellen, fordi metoden er for kompleks, metoden er for tungvint og for lite tilgjengelig. Og det er ikke nødvendigvis slik at det bare er sikringsrisikoeksperter som lager disse. Ikke sånne som du og jeg som gjør dette og vet hva det er og som gjør dette hver dag. Det er gjerne noen i en 2% stilling skal gjøre dette en gang i året, kanskje lese seg opp på en helt ny metodikk, nei det har jeg ikke noe tru på! Og såpass lite tro på det at jeg mener bestemt det ikke gir noen stor merverdi å gå på den stringente tre-faktormetodikken ut i fra hva en ROS-modell ville gitt. For det er snakk om, hvor langt inn på skiva kommer du. Med en ROS-modell så vil jeg anta at vi skyter en åtter. Ambisjonsnivået for de som lagde tre-

faktormodellen er innertier. Men de som skal skyte har ikke forutsetningene for å rette siktemiddelet godt nok. For de treffer aldri blink, det er for vanskelig å sikte, denne rifla er for tung og ustabil. Metoden er for vanskelig, mener jeg. Slik at vi kommer likevel ikke bedre enn en åtter. Og da har det vært en lang vei fram til en åtter. Kontra en kort og forståelig vei til en åtter. Det betyr noe for de der ute som skal gjøre dette.

Det betyr noe, såpass mye at når DSB legger opp til sikringsrisikoanalyser i sivilforsvarsdistriktene og sånt noe, så legger vi opp til en kombinasjon som fremdeles er verdisentrert. Hele sikringsfaget er verdisentrert. Men det er viktig at risikoanalysen er verdisentrert. Vi skal vite hva det er vi skal sikre. Vi skal ha en bevissthet rundt verdiene våre som er så stor at enten vi er på den ene eller den andre modellen er i stand til å analysere oss, i tilstrekkelig grad frem til hvilke sikringstiltak er nødvendig for å gjøre dette, for å sikre verdien, som grunnsikring og som påbyggingstiltak.

5. Strukturelle forklaringer: H_1 hypotesen bygger videre på strukturelle eller andre ytre rammefaktorer. Eksempler kan være sektorkrav, bransjestandarder, lover/forskrifter eller tvungen isomorfi (pålagt standardisering).
   I hvilken grad mener du at slike strukturelle forklaringer bidrar til å forklare valget av analysemodell? Gjelder dette i så fall valg av begge modellene eller er det forskjeller?

Når det gjelder kommunene så oppleves det som et sektorkrav at to-faktor skal brukes. Lov om kommunal beredskapsplikt peker den retningen, det er et lovkrav og det skal de være compliant med. Jeg tror ikke noen norske kommuner får noe ekstra ros fra fylkesmannen i form av skjønnsmidler eller noe annet dersom de gjør det på en tre-faktormodell. Det tror jeg ikke skjer, jeg tror heller ikke storbykommunene gjør det, de er ganske blanke de også, på sikringsrisikoanalyser.

Men for vi som er sikkerhetsaktører, det kom en ny modell, det kom en ny metode. Så ble den metoden flagget høyt i veilederperspektivet (fra NSM). Men når det kom en ny sikkerhetslov så ble det tatt ned. Da fikk denne pila et litt annet fortegn. For ny sikkerhetslov skal dokumentere det ved hjelp av risikoanalyser. Og ny sikkerhetslov er ikke metodespesifikk, men skal dekke faktorene betydning (verdi), sikkerhetstruende virksomhet (trussel), sannsynlighet, sårbarhet, konsekvens. Det skal vi adressere. Det treffer like mye to- som tre-faktormodellen. Jeg synes det treffer en to-faktor modell bedre som tar opp i seg verdiperspektiv. Det er min påstand.

I styringsdialogen i sektoren, fra departement og nedover så opplever vi ikke krav på metode. Vi skal ha oversikt over risiko, vi skal ha kontroll på risiko, vi skal ha et system for styring av risiko, det er kravene. Og så skal vi dokumentere at vi har et styringssystem for sikkerhet og risiko. Og at sikkerhetsstyringen skal være integrert i virksomhetsstyringen og alt sånt noe. Generelt sett så blir vi ikke målt på dette fra departementet heller. Det er veldig sjeldent i styringsdialogen at sikringsrisikoanalyser er tema. Det dreier seg veldig mye om økonomireglement, om oppdragsstyring, om hvordan departementet utøver regjeringens politikk på enkelte områder, og ikke så veldig mye sikkerhetsstyring.

Dette har også en organisasjonskomponent i seg, at man i styringsdialogen med overordnet myndighet ikke blir målt på metodikken. Det etterspørres ikke metodikk, det stilles ikke noe krav til metodikk, og ting man ikke blir målt på og ikke får penger til, har en tendens til å ikke

bli gjort. Vanskeligere er det ikke. Og som statsansatt så er ikke dette dugnad og hobby, vi har det som en jobb, de færreste har det som et kall.

6. Indre forklaringer (H_2): *I hvilken grad tror du det medfører riktighet at valg av analysemodell (ROS/VTS) skyldes subjektive forhold hos aktørene, slik som utdanning- og yrkesbakgrunn, kunnskaper, holdninger eller egeninteresser? Mener du at denne forklaringen er dekkende for valg av begge modeller?*

Kunnskap! Kunnskap er viktig. Kunnskap og kompetanse om to-faktormodellen er lett tilgjengelig, for den er enklere. Det er noe som man er vant til i mange sammenhenger. Det enkle gjør man mer av enn det som er vanskelig og tungvint. Derfor tror jeg at det er noen subjektive forhold som utdanning, kunnskaper som er styrende for valget. Når det gjelder yrkesbakgrunn og kunnskap, har du en akademisk utdannelse på masternivå, spesielt innenfor sikkerhetsfaget kan du en god del av metodikken. Og for mitt vedkommende da jeg gjennomførte tre-faktor VTS-analyse i hele DSB så var det avgjørende for meg å teste metodikken. Hva gav denne metodikken av merverdi? Bortsett fra et helvetes mye merarbeid som ikke gav noe særlig effekt i andre enden. Jeg fulgte metoden med alle vedleggene slavisk, til punkt og prikke. Jeg syntes jeg brukte uforholdsmessig mye tid på å beskrive usikkerheter i analyseprosessen som forsvant underveis. Det forsvant og ble litt ubrukelig.

7. Organisasjonsteoretiske forklaringer **(**H_3). Valg av analysemodell kan skyldes;
   - «*Tykk» institusjonalisme,* sånn har vi alltid gjort det her, ingen grunn til å endre.
   - *Stiavhengighet,* Vi har brukt så mye ressurser på dette valget at det er for sent å går tilbake for å velge en annen løsning.
   - *Mimetisk isomorfisme,* Vi bør følge etter/ «etterape» andre sammenlignbare organisasjoner som har valgt en annen (ny) løsning.
   - *Normativ isomorfisme,* vil bør velge den analysemodellen som er mest riktig å bruke, ut fra eksisterende kunnskap.
   - Andre organisasjonsteoretiske forklaringer.

   Beskriv med egne ord hvilke faktorer du mener forklarer organisasjoners eventuelle valg ROS/VTS-analyse? Hva slags organisasjoner gjør hvilke valgbasert på overstående eksempler?

Når det gjelder å finne noen knagger å henge dette på, så er det…

Dette med tykk institusjonalisme er representativt for norske kommuner. Sånn har vi alltid gjort det, sånn har DSB sagt at vi skal gjøre det, vi har ikke noen grunn til å gjøre det annerledes. Det er dette vi blir målt på. Sitt rolig i båten, gjør det bare ordentlig og vi gjør det på den måten. Ferdig snakka.

Når det gjelder det å skulle følge opp og etterape andre sammenlignbare institusjoner, så kan det gjelde storbykommunene. Når en storbykommune har gjort dette på en måte og er veldig fornøyd med det, og deler av sin kunnskap og overskuddskompetanse til andre. En storbykommune har omtrent de samme verdiene som andre storbykommuner har. Og så videre.

Jeg foreleser for storbykommunenettverket av og til. Det er et nettverk som DSB holder i. Storbykommunene samles hos DSB to ganger i året, hvor jeg også har snakka om sikringsrisikoanalysemetodikk med de. De store kommunene er de ressurssterke kommunene hvor de har folk på heltid til å gjøre det her, de som har en beredskapsetat som består av mange personer, samtidig som en perifer småkommune kan ha en person i 0.3 prosent stilling. Det henger jo ikke på greip at vi skal sette alle sammen i samme bås, det går ikke an.

Alle forsøker nok og å velge den analysemodellen som er mest riktig å bruke ut fra eksisterende kunnskap. Det ligger nok til grunn, men man blir fort fanga av virkeligheten. Enkleste vei til målet som er godt nok, ja takk begge deler. For vårt vedkommende, da vi gjennomførte sikringsrisikoanalysen i DSB 2018, så brukte jeg modellen fordi jeg var nysgjerrig på den. Men den gav ikke noe særlig og det var grusomt mye jobb. Og jeg hadde ikke verktøystøtte, men nå har vi jo verktøystøtte på den, VTS modul i CIM finnes jo….

Men det fine med ROS modulen i CIM er at den er aggregerbar. Slik at når vi gjennomfører ROS-analyser i CIM så har alle sivilforsvarsdistriktene sine risikoanalyser i samme verktøyet. Jeg kan legge alle risikotabellene oppå hverandre og få det aggregert. Slik at jeg ser hvor og hvordan er det skoen trykker og jeg kan følge med i et overordnet verktøyet. Hvor og hvem og hva er det vi gjør for å redusere denne risikoen og flytte det ned fra de rød kvadranter og mot det gule og grønne. Dette er altså risikostyring på virksomhetsnivå.

Kommunene gjør som sagt valg ut i fra at ting er enkelt. Storbykommunene kan gjøre valg fordi de andre gjør det. Sikkerhetsorganisasjoner som har litt ressurser prøver ut nye modeller, setter seg inn i dette og går kurs i dette. Jeg gikk jo selv et kurs på masternivå ved Universitetet i Stavanger på sikringsanalyser /risikoanalyser ved villede handlinger og terrorisme.

Så det er litt forskjellig hva slags organisasjoner som gjør det, det har mye med å gjøre hva slags organisasjon det er og hvor store de er. Og ikke minst hvor mye ressurser de har til det. for jeg tror ingen har den genuine interessen av å inneha kunnskap om risiko. Kunnskap om risiko i seg sjøl gir ingen mening. Det er hva du gjør med det. For eksempel for en kommune, å sitte på et risikobilde, sitte på en kunnskap om for eksempel avløpssystemet i kommunen. De sitter på en kunnskap om det, men det avgjørende er jo hvordan denne kunnskapen omsettes til handlinger og tiltak. For å redusere sårbarheten, for at innbyggerne skal få en best mulig kommunal tjeneste. Det er det dette dreier seg om, det er et verktøy for å bli bedre. Ja.

8. *Hva tror du er årsaken til at sikkerhets- og beredskapsmiljøene ikke har klart å samle seg om en omforent modell for risikovurderinger?*

Jeg tror hovedårsaken er at sikkerhets- og beredskapsmiljøene er fragmenterte. Det finnes ingen felles nettverk i sikkerhets- og beredskapsmiljøene hvor dette er tatt opp. Det er noe som akademia har gjort. Mye av teoriene rundt risikostyring vedlikeholdes av akademia. Og koblingen mot virksomhetsstyring er dårlig. Vanskelig tilgjengelig kunnskap. Det er jo noe å håpe at man klarer å innse at vi trenger bare en modell for risikostyring. På både villede og ikke-villede handlinger, som passer for alle organisasjoner. Og som gir et resultat hvor du kan dokumentere risikoen. Du lager handlinger ut fra hva du gjør med det. Og en risikoanalyse som bidrar til, i hvert fall i forhold til sikkerhetsloven å dokumentere at du er i

stand til å ivareta forsvarlig sikkerhet, enten det er i forhold til ikke-villede eller villede handlinger. Det har det blitt større og større krav om.

Det er også noe med det at aktørene deler ikke resultater og erfaringer. Nei! Når en kommune gjennomfører en risikoanalyse, så deler de den ikke så veldig mye. Og når virksomheter på direktoratsnivå deler sikringsrisikoanalyser, man er jo så redd for innholdet i de, til dels for at man ikke har plattformer til å dele gradert informasjon på. Men som jeg har sagt, DSB har et nettverk som vi kaller nasjonalt sikkerhetslederforum. Hvor vi samler sikkerhetsledere fra 16 statlige virksomheter på direktoratsnivå. Hvor vi diskuterer dette. Og de ble overrasket når jeg var villig til å dele min sikringsrisikoanalyse. Det satte de stor pris på, men de ville ikke dele sine, fordi det blir for sensitivt. Og det er også en årsak til at man sitter litt på hver sin tue og er misfornøyde.

9. *Burde vi samles om en felles analysemodell som favner alle sikkerhetsaspekter? I så fall hvordan kan dette oppnås? Eller er det bedre å rendyrke ulike verktøy/metoder til forskjellig bruk?*

Det har jeg allerede svart på, en felles modell ja takk! Av årsaker nevnt foran, he he! Det er mange gode argumenter for at vi skal ha en felles modell. Såpass gode at hvis de ikke klarer å enes, så er jeg villig til å skrote tre-faktormodellen.

***Oppfølgingsspørsmål**: Kjenner du den arbeidsgruppen såpass godt at du tror den nye modellen blir så god at både safety- og securityfolk vil slutte seg til den?*

***Svar**: Så godt kjenner jeg ikke til gruppen. Men hvis de ikke har ambisjoner om å klare det, kan de legge seg sjøl ned med en gang. Det må være det altoverskyggende målet å få til det. Hvis ikke de har til målsetning å få til en modell, så kan de kutte arbeidet med en gang. Og så ser vi at, jeg tror at tre-faktormodellen vil miste mer og mer fotfestet. Fordi den er for kompleks, den er for vanskelig tilgjengelig.*

***Oppfølgingsspørsmål**: Utgangspunktet for arbeidet med den nye modellen er vel slik jeg har forstått det NS 5814, altså ROS-standarden fra 2008. Den har implisitt noen svakheter ved seg som må rettes opp for at securityfolk skal kunne ta den tilstrekkelig på alvor. Men om man tar til seg noen av de positive kvalitetene som kom med securitystandarden i 2014, og putter det tilbake inn i ROS-modellen?*

***Svar:** Jeg tror ROS-modellen, men med et megatydelig verdiperspektiv. For det kommer vi ikke unna, at dette faget er verdisentrert. Det er verdiene vi skal skjerme og beskytte, uansett hva som skjer med de, om verdien er et skjermingsverdig objekt etter sikkerhetsloven eller om det er et vannforsyningsanlegg, så er det likevel disse verdiene som vi skal ta vare på. Jeg har ikke noen tro på at dette miljøet er så stort at vi klarer å opprettholde to modeller. Jeg tror ikke merverdiene ved å opprettholde to modeller er stor, som det skal drives utvikling på, som det skal drives opplæring på, som det skal drives analyser på, og kommunikasjon av på mange forskjellige nivåer. Nei, det tror jeg egentlig ikke står seg i lengden.*

Jeg har også stilt spørsmål til amerikanske myndigheter, både FEMA, DHS og FBI, hvordan gjør de det i USA? Og videre slags modeller bruker de i europeiske land som det det er naturlig å sammenligne oss med? Jeg har spurt vår internasjonale avdeling i DSB og de sier;

Nei, sånn tre-faktormodell etter norsk standard 5832 har ikke noe stort feste i Europa. Den har kanskje godt feste i USA. Hvorfor skal vi drive med dette her, her på berget, for vi er så små! Det er bare tøys! Det er kanskje å banne i kirka, med det er det jeg virkelig mener. Fordi det gir ikke stor merverdi.

Så svar på 9, nei vi skal ikke ha to, vi skal ha en modell som dekker begge deler og som er god nok, ferdig snakka.

10. *Er det etter ditt syn andre faktorer som forklarer valg av analysemodell som jeg ikke har tenkt på?*

I forhold til offentlig styring, hva er det i styringssignalene, altså virksomhetsstyringen som indikerer metodevalg? Der kan det være noe. Og det kan være avhengigheter til metodevalg i forhold til annen virksomheter som utvikler beredskapsplanverk, som neste steg etter en risikoanalyse. Hvis det kommer noen komponenter i virksomhetsstyringen? Hvis lovverket sier noe? Forhåpentligvis er lovverket såpass utydelig at det ikke går på metodevalg. Metodevalgene er mer dynamiske enn det loven er, endrer seg fortere.

Nysgjerrighet er en faktor. Hvor nysgjerrige er sikkerhetsmiljøene på bruk av nye metoder? Så nysgjerrighet er en faktor, og det var en faktor for mitt vedkommende, for DSB når vi valgte tre-faktor var vi nysgjerrige på den nye modellen, men vi ble litt skuffa.

***Oppfølgingsspørsmål**: Hva med kommunikasjon av usikkerhet? Usikkerhet vs sannsynlighet på det som vi ikke vet?*

Svar: Usikkerheter. Usikkerheter i et sannsynlighet og konsekvens perspektiv er knyttet til sannsynlighetsbegrepet, der er det størst usikkerheter. Eksempelvis for en kommune. Hvis usikkerhetene er enkle å forholde seg til. Det man ikke vet har man et relativt godt empirisk grunnlag for å anta noe om. Og i en kommune så analyserer man ganske nære ting.

Usikkerheter i tre-faktormodell er mer omfattende, fordi modellen og metoden legger opp til at usikkerheter skal eksplisitt beskrives i hvert eneste ledd, i hvert eneste scenario som trusselaktøren kan utnytte for å utnytte sårbarhetene, får å nå verdiene. Det er på en måte litt sånn sjølmål, med overdreven bruk av usikkerhetsdokumentasjon snakke metoden ned. Min erfaring med å gjennomføre tre-faktormodellen er at usikkerhetsbeskrivelsen ikke gav noe merverdi. Og usikkerhetene gav ingen merverdi når vi kom til beslutningstakers vurdering heller. Det gav meg ingen ting. Der hadde usikkerhetsfantastene på det metodekurset fått full score, jeg synes ikke noe om det. Ja, vi skal ha usikkerheter beskrevet i dette her, men på riktig nivå. Hvis usikkerheten tar så stor overhånd, så blir det dårlige beslutninger når leder skal, tross alt vi bruker risikoanalyser for å gå til våre ledere for å be om penger til å sikre, jeg synes det blir feil.

Og i VTS-analysen i forhold til usikkerhet; Det er usikkerhet på trusselaktørene. På hva slags kapabiliteter de har. Det er så mye usikkerhet rundt det. Hvis man tar inn over seg usikkerhetene, hvis vi skal etablere grunnsikringen rundt et objekt i forhold til en trusselaktør. Dersom trusselen øker, eller at trusselaktørene endrer seg, eks fra organiserte kriminelle til fremmede staters spesialstyrker, så øker vi usikkerheten samtidig som konsekvenspotensialet øker. Og vi vet mindre om fremmede lands spesialstyrker enn vi vet om organiserte

kriminelle. Så her er altså metoden litt inkonsistent ved bruken av usikkerhet, og vi skal beskrive usikkerhet i alle disse momentene. Og hvordan adderer vi usikkerheter? Nei, dette tror jeg ikke i sum fører noe godt ved seg. Men vi må ha med usikkerheter, vi må forklare for beslutningstakere hvor ligger usikkerhetene og hva slags forhold har vi til dem, for vi må håndtere usikkerhetene. Og beslutninger i situasjoner med stor grad av usikkerhet er også en kunst. Det må gjøres, men vi skal vekte de usikkerhetene vi har, og vi må for all del ikke legge de sammen.

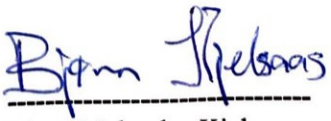
Jeg tror heller ikke at dyptgående studier, et usikkerhetsstudium. Er ikke sikkert at det fører noe godt ved seg? Jeg er ikke overbevist om at det bringer risiko-Norge nevneverdig mer i riktig retning at man starter en stor diskurs om usikkerhetsperspektivet. Men vi må ha et forhold til det, og ta det med inn i beslutningen når vi skal foreslå noe til en sjef som sitter med pengene. Det er vel det jeg mener om usikkerheter.

Avslutningsvis*:*
Helt kort, hvilken befatning du selv har hatt med henholdsvis ROS og VTS modellene, hva er din utdannelse /erfaring innenfor fagområdet?

Har gjennomført risikoanalyser på kommunalt nivå, har vært fylkesberedskapssjef i noen år med metodeveileder og prosessansvar ansvar for norske kommuner.
Master i risikostyring, har nå ansvar for risikoanalyser og risikostyring i hele DSB inkludert Nødnett, på et overordnet nivå. Har gjennomført og oppdaterer DSB sin egen analyse. Til sist oppfølging alle sivilforsvarsdistriktene og de skal gjøre to-faktor (ROS), med et hovedfokus å beskrive betydningen av verdien, herunder konsekvenser ved bortfall av den.

Sted/dato: ***Nydalen, 29.1.2020***

Respondent/intervjukandidat



Bjørn Melandsø Kjelsaas
Masterstudent
Høgskolen i Innlandet

Vil du delta i forskningsprosjektet

" Modeller for risikoanalyse i Norge"?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å forklare årsaker til at organisasjoner velger ROS-analyse, VTS-analyse eller begge disse modellene for å analysere hva slags og hvor mye risiko organisasjonen eller entiteten står ovenfor.

Formål
Formålet med undersøkelsen er å undersøke om valget av analysemodell (ROS eller VTS) kan skyldes:

- Ytre rammefaktorer eller sektorkrav, lover og regler
- Subjektiv identitet, kultur, kompetanse og bakgrunn hos aktørene.
- Institusjonalisme med institusjonalisert sedvane vs. mimetisk eller normativ isomorfisme.

I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Intervjuene bygger videre på spørreundersøkelsen "Modeller for risikoanalyse i Norge" som du allerede er kjent med. https://nettskjema.no/a/134183

Opplysningene skal primært benyttes til en master i offentlig ledelse og styring (MPA) ved Høgskolen i Innlandet. Masteroppgaven vil være offentlig. Innsamlede opplysninger kan sekundært bli brukt til eventuelle artikler, undervisning eller andre forskningsprosjekter som har til hensikt å løfte frem ny kunnskap om risikoanalyse, samfunnssikkerhet eller organisasjonsstudier.

Hvem er ansvarlig for forskningsprosjektet?
Høgskolen i Innlandet v/ Fakultet for økonomi og samfunnsvitenskap,

Hvorfor får du spørsmål om å delta?
Du er spurt om å delta basert på din kunnskap om risikoanalyse ved bruk av ROS- eller VTS-modellen. Du har enten sendt meg en henvendelse på mail om din villighet, eller jeg har fått dine kontaktopplysninger oppgitt av andre ressurser innenfor fagområdet med anbefaling om å spørre deg.

Hva innebærer det for deg å delta?
Deltagelsen innebærer et kvalitativt intervju på inntil 60 minutters varighet hvor samtlige spørsmål handler om de to modellene for risikoanalyse og tilhørende terminologi i lys av organisasjonsstudier. Jeg vil også intervjue 1-2 andre personer over samme tematikk.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Du har også sagt deg villig til å stå fram med fullt navn og tittel i min masteroppgave som vil bli publisert som et offentlig dokument. Eventuelt øvrige personopplysninger om deg vil bli permanent slettet eller anonymisert ved prosjektslutt.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Dersom du på et senere tidspunkt ønsker å trekke tilbake ditt samtykke er det kun student (Bjørn Kjelsaas) og veileder (Pernille Rieker) som vil ha tilgang. I så henseende vil ditt navn, posisjon og eventuelt andre identifiserbare opplysninger bli permanent slettet fra digitale plattformer, papirutskrifter og eller håndskrevne notater. Gjenværende opplysninger fra intervjuet vil da være anonymisert.
- Deltakerne vil kunne gjenkjennes i masteroppgaven, eventuelle artikler eller i undervisningssammenheng dersom samtykket fortsatt er tilstede.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Prosjektet skal etter planen avsluttes 29. februar 2020 ved at masteroppgaven innleveres for sensur. Masteroppgaven vil senere bli publisert av Høgskolen I Innlandet ved at den gjøres søkbar sammen med andre oppgaver, samt av undertegnede.

Formålet med at datamaterialet ikke skal anonymiseres ved prosjektslutt er etterprøvbarhet, eventuelle oppfølgingsstudier og arkivering for senere forskning. Det er kun navn og stilling på intervjutidspunktet som vil bli lagret offentlig på ubestemt tid.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Høgskolen i Innlandet har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
- *Handelshøgskolen i Innlandet* ved Bjørn Melandsø Kjelsaas på bkjelsaas@gmail.com (student) eller Pernille Rieker pernille.rieker@inn.no (professor II og veileder).
- Vårt personvernombud: Hans Petter Nyberg, hans.ryberg@inn.no, Høgskolen i Innlandet.
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Pernille Rieker	Bjørn Melandsø Kjelsaas
Prosjektansvarlig (Professor II/ veileder)	Student Master i offentlig ledelse og styring (MPA)

Samtykkeerklæring

Samtykke innhentes skriftlig ved intervjuets oppstart.

Jeg har mottatt og forstått informasjon om prosjektet "Modeller for risikoanalyse i Norge og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☑ å delta i *intervju på inntil 60 minutters varighet*
- ☒ *at opplysninger om meg publiseres slik at jeg kan gjenkjennes i masteroppgaven "Modeller for risikoanalyse i Norge" ved Høgskolen i Innlandet*
- ☑ *at opplysninger om meg også kan publiseres i eventuelle artikler eller undervisning/foredrag over samme tematikk, med henvisning til overstående masteroppgave.*

22/01/20

(Signert av prosjektdeltaker, dato)

Samtykkeerklæring

Samtykke innhentes skriftlig ved intervjuets oppstart.

Jeg har mottatt og forstått informasjon om prosjektet "Modeller for risikoanalyse i Norge og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☒ å delta i *intervju på inntil 60 minutters varighet*
- ☐ *at opplysninger om meg publiseres slik at jeg kan gjenkjennes i masteroppgaven "Modeller for risikoanalyse i Norge" ved Høgskolen i Innlandet*
- ☒ *at opplysninger om meg også kan publiseres i eventuelle artikler eller undervisning/foredrag over samme tematikk, med henvisning til overstående masteroppgave.*

Tore Pettersen

(Signert av prosjektdeltaker, dato)

NSD NORSK SENTER FOR FORSKNINGSDATA

NSD sin vurdering

Prosjekttittel

Modeller for risikoanalyse i Norge

Referansenummer

437887

Registrert

13.01.2020 av Bjørn Kjelsaas - 181509@stud.inn.no

Behandlingsansvarlig institusjon

Høgskolen i Innlandet / Handelshøgskolen Innlandet - Fakultet for økonomi og samfunnsvitenskap / Institutt for organisasjon, ledelse og styring

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Pernille Rieker , pernille.rieker@inn.no, tlf: 91729804

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Bjørn Melandsø Kjelsaas, bkjelsaas@gmail.com, tlf: 95800374

Prosjektperiode

13.01.2020 - 29.02.2020

Status

17.01.2020 - Vurdert

Vurdering (1)

17.01.2020 - Vurdert

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet den 17.01.2020 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte. MELD VESENTLIGE ENDRINGER Dersom det skjer vesentlige endringer i

behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html Du må vente på svar fra NSD før endringen gjennomføres. TYPE OPPLYSNINGER OG VARIGHET Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 29.02.2020. LOVLIG GRUNNLAG Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a. PERSONVERNPRINSIPPER NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:
- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål - dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet - lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet DE REGISTRERTES RETTIGHETER Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20). NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13. Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned. FØLG DIN INSTITUSJONS RETNINGSLINJER NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32). For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon. OPPFØLGING AV PROSJEKTET NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet. Lykke til med prosjektet! Kontaktperson hos NSD: Simon Gogl Tlf. Personverntjenester: 55 58 21 17 (tast 1)